

חישוביות וסיבוכיות

טבלה של רדוקציות

רדוקציה	עמוד
$L_{\text{HALT}} \leq L_{\text{acc}}$	דוגמה 7.6 עמוד 72
$\bar{L}_{\text{acc}} \leq L_{\text{NOTREG}}$	דוגמה 7.11 עמוד 76
$L_{\text{acc}} \leq L_{\text{NOTREG}}$	דוגמה 7.12 עמוד 77
$L_{\text{HALT}} \leq L_{\text{NOTREG}}$	דוגמה 7.13 עמוד 78
$L_{\text{acc}} \leq L_{\text{REG}}$	דוגמה 7.15 עמוד 80
$\bar{L}_{\text{acc}} \leq L_{\text{REG}}$	דוגמה 7.14 עמוד 79
$\bar{L}_{\text{acc}} \leq L_{M_1 \neg M_2}$ כאשר $L_{M_1 \neg M_2} = \{ \langle M_1, M_2, w \rangle \mid w \in L(M_1) \wedge w \notin L(M_2) \}$	דוגמה 7.16 עמוד 81
$\bar{L}_{\text{acc}} \leq L_{M_1 \subset M_2}$ כאשר $L_{M_1 \subset M_2} = \{ \langle M_1, M_2 \rangle \mid L(M_1) \subset L(M_2) \}$	דוגמה 7.17 עמוד 81

תוכן העניינים

4	1 מכונות טיורינג
4	הגדרה היוריסטית של מכונת טיורינג
8	הגדרה פורמלית של מכונת טיורינג
21	טבלת המעברים
25	חישוב פונקציות
29	2 מודלים חישוביים שקולית
32	3 מכונות טיורינג מרובות סרטים
32	מכונת טיורינג מרובת סרטים: הגדרה היוריסטית
32	מכונת טיורינג מרובת סרטים: הגדרה פורמלית
33	קונפיגורציה של מטמ"ס
35	שקילות בין מטמ"ס למ"ט עם סרט יחיד
41	4 מכונת טיורינג אי דטרמיניסטית
41	הגדרה של מכונת טיורינג אי-דטרמיניסטית
43	עץ החישוב של מ"ט א"ד
44	שקילות בין מ"ט א"ד למ"ט דטרמיניסטית

48	5	תכונות סגירות של R ו- RE
48		הגדרה של השפות R ו- RE
54		קידוד של מ"ט דטרמיניסטית
54		מ"ט אוניברסלית U
57	6	אי-כריעות
57		השפות L_d, L_{halt}, L_{acc} לא כריעות
61		השפה L_E לא כריעה
63		השפה L_{EQ} לא כריעה
66		סיכום: כריעות וקבילות של שפות
67	7	רדוקציה
67		טבלה של רדוקציות
67		מ"ט המחשבת את פונקציה
69		רדוקציות
76		דוגמאות בשימוש של משפט הרדוקציה בין שפות משלימות (משפט 7.2)
76		דוגמאות בשימוש של משפט הרדוקציה (משפט 7.1)
83	8	מבוא לסיבוכיות
83		הגדרה של סיבוכיות
85		יחס בין הסיבוכיות של מ"ט סרט יחיד ומטמ"ס
86		יחס בין הסיבוכיות של מ"ט דטרמיניסטית ומ"ט א"ד
88		המחלקה P
88		בעיית PATH
90		בעיית RELPRIME
93	9	המחלקה P והמחלקה NP
93		המחלקה P
93		דוגמאות לבעיות ב- P
93		בעיית המסלול ההמילטוני HAMPATH
94		אלגוריתם אימות
94		המחלקה NP
97		הקשר בין NP למ"ט א"ד
98		הקשר בין המחלקה P ו-NP
101	10	NP שלמות
101		המחלקות NPC ו- NPH
102		בעיית הספיקות
102		בעיית SAT
103		משפט קוק לויין
103		גרסאות של $kSAT$
103		בעיית 3SAT
105		הוכחת משפט קוק לויין*
111	11	רדוקציות פולינומיאליות
111		$CLIQUE$ היא NP-שלמה
113		בעיית הקבוצה הבלתי תלויה
115		בעיית הכיסוי בקודקודים
116		הבעייה VC
117		PARTITION
117		רדוקציות פולינומיאליות

שיעור 1

מכונות טיורינג

1.1 הגדרה היוריסטית של מכונת טיורינג

הגדרה 1.1 מכונת טיורינג (הגדרה היוריסטית)

הקלט והסרט

מכונת טיורינג (מ"ט) קורא קלט. הקלט נמצא על סרט אינסופי. התווים של הקלט נמצאים במשבצות של הסרט. במכונת טיורינג אנחנו מניחים שהסרט אינסופי לשני הכיוונים. משמאל לתחילת הקלט לא כתוב כלום, ומימין לסוף הקלט לא כתוב כלום. אנחנו מניחים שיש תו הרווח $_$ שנמצא בכל משבצות שאינן משבצות קלט, משמאל לקלט ומימין לקלט.

...	_	_	a	b	b	b	a	a	_	_	_	...
-----	---	---	---	---	---	---	---	---	---	---	---	-----

הראש

במצב ההתחלתי הראש בקצה השמאלי של הקלט.

...	_	_	a	b	b	b	a	a	_	_	_	...
-----	---	---	---	---	---	---	---	---	---	---	---	-----



הראש יכול לזוז ימינה על הסרט וגם שמאלה על הסרט. הראש יכול לקרוא את התוכן שנמצא במשבצת הסרט שבה הוא נמצא. הראש יכול לכתוב על המשבצת הסרט שבה הוא נמצא. הכתיבה נעשית תמיד במיקום הראש.

המצבים

בהתחלה הראש בקצה השמאלי של הקלט והמ"ט במצב התחלתי q_0 . הראש קורא את התו במשבצת הראשונה וכותב עליה לפי הפונקציית המעברים (שנגדיר בהגדרה 1.2). כעת המ"ט במצב חדש q_1 . הראש קורא את התו במשבצת השניה וכותב עליה לפי הפונקציית המעברים ואז המ"ט במצב חדש q_2 . התהליך ממשיך עד שהראש מגיע לקצה הימני של הקלט, ואז הוא ממשיך לקרוא ולכתוב על כל משבצת בכיוון שמאלה, עד שהוא מגיע לקצה השמאלי. במ"ט ניתן לטייל על הקלט שוב ושוב לשני הכיוונים. התהליך מסתיים כאשר המ"ט מגיע למצב מקבל q_{acc} או מצב דוחה q_{rej} .

דוגמה 1.1

נבנה מכונת טיורינג אשר מקבלת מילה אם היא בשפה

$$L = \{w \in \{a, b\}^* \mid \#a_w = \#b_w\}.$$

ז"א השפה המורכבת מכל המילים עם מספר שווה אותיות a ו b .

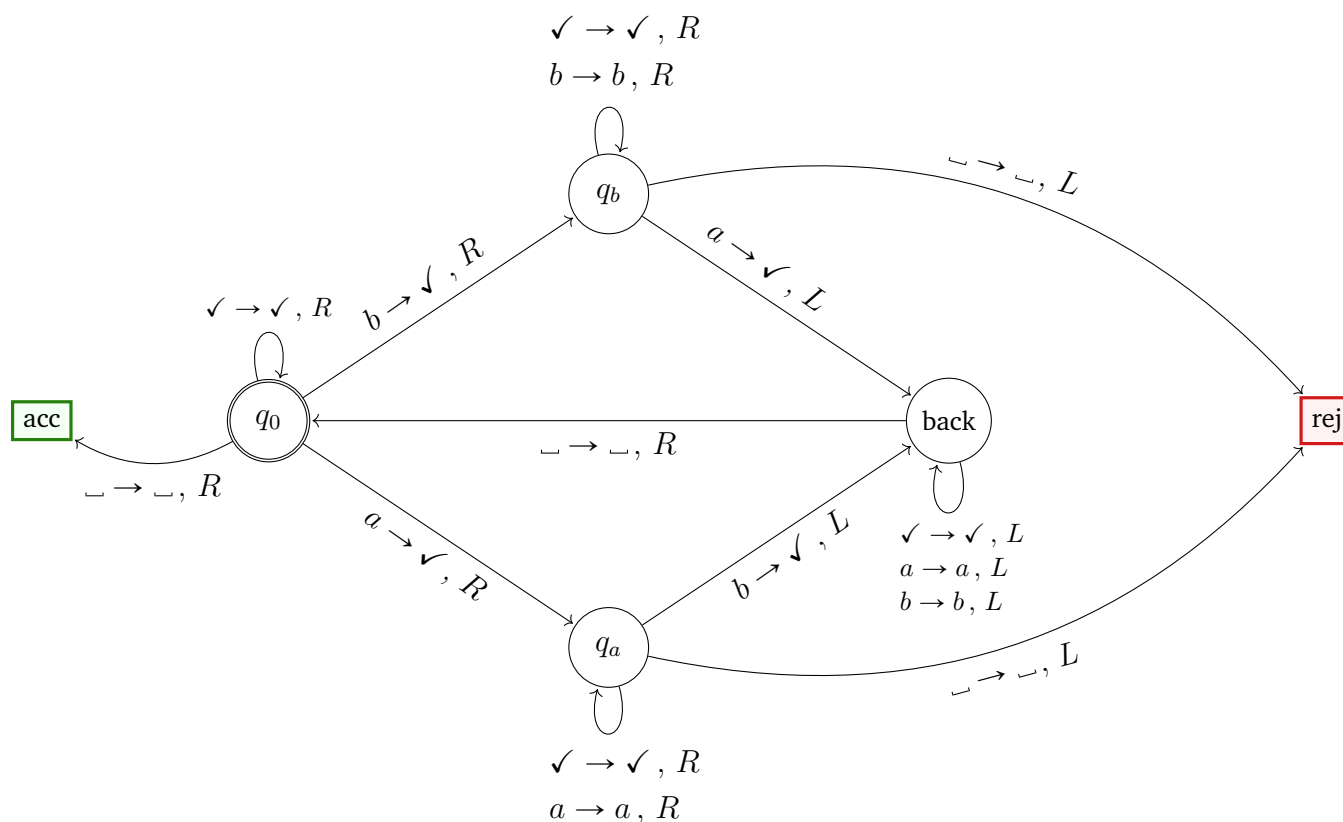
תיאור מילולי

- נסרוק את הקלט משמאל לימין ולכל a נחשפ b תואם.
 - נניח שראינו במשבצת הראשונה a , נסמן עליה \checkmark .
 - עכשיו נסרוק את יתרת הקלט ונחפש אות b מתאימה ל a שכבר ראינו.
 - אם לא מצאנו, המילה לא בשפה.
 - אם מצאנו, נסמן את ה- b התואם ב- \checkmark .
 - נחזור לתחילת הקלט ונעשה סריקה נוספת משמאל לימין.
 - במשבצת הראשונה יש \checkmark מסיבוב הראשון. הראש פשוט כותב עליה \checkmark , כלומר משבצת ראשונה נשארת ללא שינוי.
 - הראש z שמאלה למשבצת הבאה. נניח שמצאנו b . נסמן במשבצת \checkmark .
 - נסרוק את יתרת הקלט ונחפש אות a מתאימה ל b שכבר ראינו.
 - אם לא מצאנו, המילה לא בשפה.
 - אם מצאנו, נסמן את ה- a התואם ב- \checkmark .
 - בכל משבצת שיש \checkmark כותבים עליה \checkmark וממשיכים למשבצת הבאה הימני.
 - נחזור לתחילת הקלט ונעשה סריקה נוספת משמאל לימין.
 - חוזרים על התהליך שוב ושוב.
 - אם היה מעבר שבו לא מצאנו אות תואמת, המילה לא בשפה.
 - אם כולן היו תואמות ועשינו מעבר שבו הגכנו מקצה לקצה, מרווח לרווח, בלי לראות שום אות, אז המילה בשפה.
- כעת נתאר את המ"ט באמצעות המצבי המכונה והפונקציית המעברים.

מצבי המכונה

q_0	המצב ההתחלתי. אליו נחזור אחרי כל סבב התאמה של זוג אותיות.
q_a	מצב שבו ראינו a ומחפשים b תואם.
q_b	מצב שבו ראינו b ומחפשים a תואם.
back	מצב שנשתמש בו כדי לחזור לקצה השמאלי של הקלט ולהתחיל את הסריקה הבאה (סבב ההתאמה הבא).
acc	מצב מקבל.
rej	מצב דוחה.

- כאשר המכונה מגיעה למצב acc היא עוצרת.
עצירה במצב acc משמעותה קבלה.
- כאשר המכונה מגיעה למצב rej היא עוצרת.
עצירה במצב rej משמעותה דחייה.
- רק בשני מצבים אלו המכונה מפסיקה.
בכל מצב אחר המכונה בהכרח ממשיכה.

תרשים מצבים

- בכל צעד המכונה מבצעת שתי פעולות:

1. כותבת אות במיקום הראש
2. זזה צעד אחד שמאלה או צעד אחד ימינה.

- בכל צעד המכונה יכולה לעבור למצב אחר או להישאר באותו מצב.

דוגמה 1.2

בדקו אם המכונת טיורינג של הדוגמה 1.1 מקבלת את המילה .abbbbaa

פתרון:

— q_0 a b b b a a —

␣	✓	q_a	b	b	b	a	a	␣
␣	back	✓	✓	b	b	a	a	␣
back	␣	✓	✓	b	b	a	a	␣
␣	q_0	✓	✓	b	b	a	a	␣
␣	✓	q_0	✓	b	b	a	a	␣
␣	✓	✓	q_0	b	b	a	a	␣
␣	✓	✓	✓	q_b	b	a	a	␣
␣	✓	✓	✓	b	q_b	a	a	␣
␣	✓	✓	✓	back	b	✓	a	␣
␣	✓	✓	back	✓	b	✓	a	␣
␣	✓	back	✓	✓	b	✓	a	␣
␣	back	✓	✓	✓	b	✓	a	␣
back	␣	✓	✓	✓	b	✓	a	␣
␣	q_0	✓	✓	✓	b	✓	a	␣
␣	✓	q_0	✓	✓	b	✓	a	␣
␣	✓	✓	q_0	✓	b	✓	a	␣
␣	✓	✓	✓	q_0	b	✓	a	␣
␣	✓	✓	✓	✓	q_b	✓	a	␣
␣	✓	✓	✓	✓	✓	q_b	a	␣
␣	✓	✓	✓	✓	back	✓	✓	␣
␣	✓	✓	✓	back	✓	✓	✓	␣
␣	✓	✓	back	✓	✓	✓	✓	␣
␣	✓	back	✓	✓	✓	✓	✓	␣
back	␣	✓	✓	✓	✓	✓	✓	␣
␣	q_0	✓	✓	✓	✓	✓	✓	␣
␣	✓	q_0	✓	✓	✓	✓	✓	␣
␣	✓	✓	q_0	✓	✓	✓	✓	␣
␣	✓	✓	✓	q_0	✓	✓	✓	␣
␣	✓	✓	✓	✓	q_0	✓	✓	␣
␣	✓	✓	✓	✓	✓	q_0	✓	␣
␣	✓	✓	✓	✓	✓	✓	q_0	␣
␣	✓	✓	✓	✓	✓	✓	␣	acc

דוגמה 1.3

בדקו אם המכונת טיורינג של הדוגמה 1.1 מקבלת את המילה aab.

פתרון:

␣	q_0	a	a	b	␣
␣	✓	q_a	a	b	␣
␣	✓	a	q_a	b	␣
␣	✓	back	a	✓	␣
␣	back	✓	a	✓	␣
back	␣	✓	a	✓	␣
␣	q_0	✓	a	✓	␣
␣	✓	q_0	a	✓	␣
␣	✓	✓	q_a	✓	␣
␣	✓	✓	✓	q_a	␣
␣	✓	✓	rej	✓	␣

1.2 הגדרה פורמלית של מכונת טיורינג

הגדרה 1.2 מכונת טיורינג

מכונת טיורינג (מ"ט) היא שביעיה

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$$

כאשר:

Q	קבוצת מצבים סופית ולא ריקה
Σ	א"ב הקלט
Γ	א"ב הסרט
δ	פונקציית המעברים
q_0	מצב התחלתי
q_{acc}	מצב מקבל יחיד
q_{rej}	מצב דוחה יחיד

$$\perp \notin \Sigma$$

$$\Sigma \subseteq \Gamma, \perp \in \Gamma \text{ ref}$$

$$\delta : (Q \setminus \{q_{rej}, q_{acc}\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$$

דוגמה 1.4 (המשך דוגמה 1.1)

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$$

$$Q = \{q_0, q_a, q_b, \text{back}, q_{rej}, q_{acc}\}.$$

$$\Sigma = \{a, b\}, \quad \Gamma = \{a, b, \sqcup, \checkmark\}$$

$$\delta(q_0, a) = (q_a, \checkmark, R),$$

$$\delta(q_0, b) = (q_b, \checkmark, R),$$

$$\delta(q_0, \sqcup) = (q_{acc}, \sqcup, R),$$

$$\delta(q_a, \checkmark) = (q_a, \checkmark, R),$$

$$\delta(q_a, a) = (q_a, a, R),$$

$$\delta(q_a, b) = (\text{back}, \checkmark, L),$$

$$\delta(q_b, \checkmark) = (q_b, \checkmark, R),$$

$$\delta(q_b, b) = (q_a, b, R),$$

$$\delta(q_b, a) = (\text{back}, \checkmark, L),$$

קל יותר לרשום את פונקציית המעברים δ כטבלה:

$Q \backslash \Gamma$	a	b	\sqcup	\checkmark
q_0	(q_a, \checkmark, R)	(q_b, \checkmark, R)	(q_{acc}, \sqcup, R)	(q_0, \checkmark, R)
q_a	(q_a, a, R)	$(\text{back}, \checkmark, L)$	(q_{rej}, \sqcup, L)	(q_a, \checkmark, R)
q_b	$(\text{back}, \checkmark, L)$	(q_b, b, R)	(q_{rej}, \sqcup, L)	(q_b, \checkmark, R)
back	(back, a, L)	(back, b, L)	(q_0, \sqcup, R)	$(\text{back}, \checkmark, L)$

הגדרה 1.3 קונפיגורציה

תהי $M = (Q, q_0, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$ מכונת טיורינג. קונפיגורציה של M הינה מחרוזת

$$uq\sigma v$$

כאשר משמעות:

$$u, v \in \Gamma^*, \quad \sigma \in \Gamma, \quad q \in Q.$$

q מצב המכונה,

σ הסימון במיקום הראש

u תוכן הסרט משמאל לראש,

v תוכן הסרט מימין לראש.

דוגמה 1.5 (המשך של דוגמה 1.3)

u	q	σ	v
␣	q_0	a	a b ␣
␣✓	q_a	a	b ␣
␣✓ a	q_a	b	␣
␣✓	back	a	✓ ␣
␣	back	✓	a ✓ ␣
␣	back	␣	✓ a ✓ ␣
␣	q_0	✓	a ✓ ␣
␣✓	q_0	a	✓ ␣
␣✓✓	q_a	✓	␣
␣✓✓✓	q_a	␣	␣
␣✓✓	rej	✓	␣

דוגמה 1.6

בנו מכונת טיורינג אשר מקבלת כל מילה בשפה

$$L = \{a^n \mid n = 2^k, k \in \mathbb{N}\}$$

ז"א מילים בעלי מספר אותיות a אשר חזקה של 2.

פתרון:

ראשית נשים לב:

$$\frac{n}{2^k} = 1 \text{ כלומר } k \text{ פעמים, כלומר } n = 2^k.$$

לאור המשפט הזה נבנה אלגוריתם אשר מחלק את מספר האותיות במילה ב-2 בצורה איטרטיבית. אם אחרי סבב מסויים נקבל מספר אי-זוגי גדול מ-1 אז מספר האותיות a במילה לא יכול להיות חזקה של 2. אם אחרי כל הסבבים לא קיבלנו מספר אי-זוגי גדול מ-1 אז מובטח לנו שיש מספר אותיות a אשר חזקה של 2.

• נתון הקלט

␣	␣	a	a	a	a	a	a	a	a	␣	␣
---	---	---	---	---	---	---	---	---	---	---	---

↑

נעבור על סרט הקלט. משמאל לימין.

• מבצעים מחקיה לסירוגין של האות a כלומר אות אחת נמחק ואות נשאר וכן הלאה.

␣	␣	✓	a	✓	a	✓	a	✓	a	␣	␣
---	---	---	---	---	---	---	---	---	---	---	---

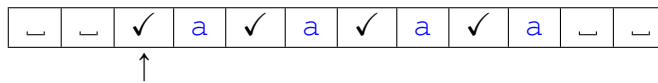
↑

אם אחרי סבב הראשון

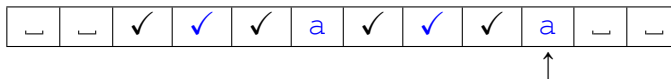
* יש ✓ בתו האחרון \Leftarrow קיבלנו מספר אי-זוגי של אותיות a אחרי חילוק ב-2 \Leftarrow אין חזקה של 2 אותיות a במילה.

* יש a בתו האחרון \Leftarrow קיבלנו מספר זוגי של אותיות a אחרי חילוק ב-2 ונמשיך לסבב הבא.

- הראש חוזר לתו הראשון של הקלט



- בסבב הבא חוזרים על התהליך של מחיקה לסירוגין של האות a (אות אחת נמחק ואות אחת נשאיר)

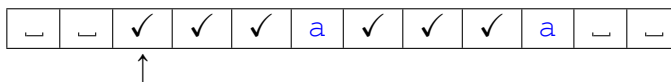


אם אחרי סבב השני

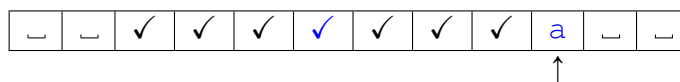
* יש ✓ בתו האחרון \Leftarrow קיבלנו מספר אי-זוגי של אותיות a אחרי חילוק ב-2 \Leftarrow אין חזקה של 2 אותיות a במילה.

* יש a בתו האחרון \Leftarrow קיבלנו מספר זוגי של אותיות a אחרי חילוק ב-2 ונמשיך לסבב הבא.

- הראש חוזר לתו הראשון של הקלט



- בסבב הבא חוזרים על התהליך של מחיקה לסירוגין של האות a (אות אחת נמחק ואות אחת נשאיר)



אם אחרי סבב השלישי

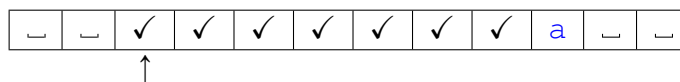
* יש ✓ בתו האחרון \Leftarrow קיבלנו מספר אי-זוגי של אותיות a אחרי חילוק ב-2 \Leftarrow אין חזקה של 2 אותיות a במילה.

* יש a בתו האחרון \Leftarrow קיבלנו מספר זוגי של אותיות a אחרי חילוק ב-2 ונמשיך לסבב הבא.

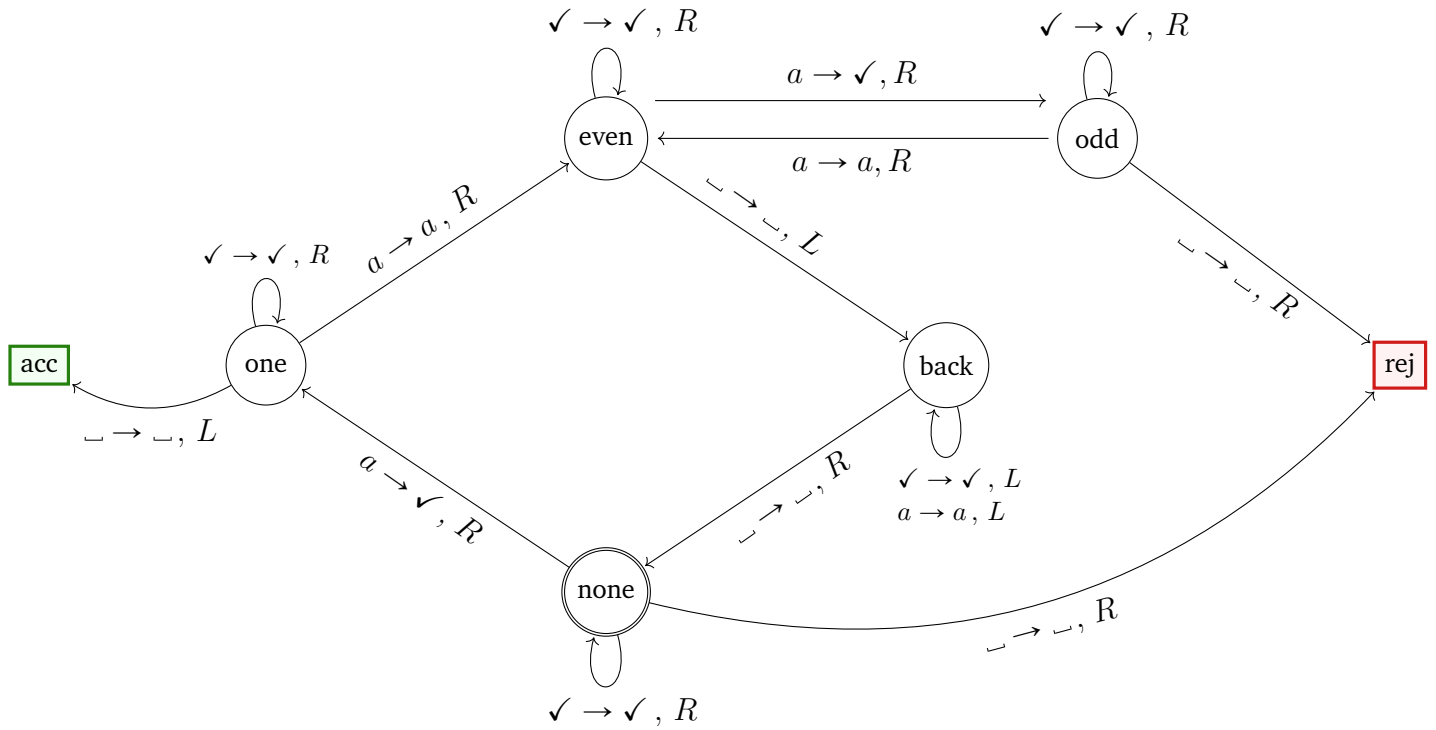
- הראש חוזר לתו הראשון של הקלט.

בסבב האחרון נשאיר רק אות a אחת.

לכן לפי המשפט למעלה מובטח לנו כי המילה מורכבת ממספר אותיות a אשר חזקה של 2.



המכונת טיורינג אשר מקבלת מילים בשפה שעובדת לפי האלגוריתם המתואר למעלה מתואר בתרשים למטה.



המצבים:

- מצב none: מצב התחלתי. עדיין לא קראנו a בסבב סריקה זה.
- מצב one: קראנו a בודד.
- מצב even: קראנו מספר זוגי של a.
- מצב odd: קראנו מספר אי-זוגי של a.
- מצב back: חזרה שלמאלה.

דוגמה 1.7

בדקו אם המילה

aaaa

מתקבלת על ידי המכונת טיורינג בדוגמה 1.6.

פתרון:

␣	none	a	a	a	a	␣
␣	✓	one	a	a	a	␣
␣	✓	a	even	a	a	␣
␣	✓	a	✓	odd	a	␣
␣	✓	a	✓	a	even	␣
␣	✓	a	✓	back	a	␣
␣	✓	a	back	✓	a	␣
␣	✓	back	a	✓	a	␣
␣	back	✓	a	✓	a	␣
␣	back	␣	✓	a	✓	␣
␣	none	✓	a	✓	a	␣
␣	✓	none	a	✓	a	␣

␣	✓	✓	one	✓	a	␣
␣	✓	✓	✓	one	a	␣
␣	✓	✓	✓	a	even	␣
␣	✓	✓	✓	back	a	␣
␣	✓	✓	back	✓	a	␣
␣	✓	back	✓	✓	a	␣
␣	back	✓	✓	✓	a	␣
back	␣	✓	✓	✓	a	␣
␣	none	✓	✓	✓	a	␣
␣	✓	none	✓	✓	a	␣
␣	✓	✓	none	✓	a	␣
␣	✓	✓	✓	none	a	␣
␣	✓	✓	✓	✓	one	␣
␣	✓	✓	✓	acc	✓	␣

u	q	σ	v
␣	none	a	aaa ␣
␣ ✓	one	a	aa ␣
␣ ✓ a	even	a	a ␣
␣ ✓ a ✓	odd	a	␣
␣ ✓ a ✓ a	even	␣	␣
␣ ✓ a ✓	back	a	␣
␣ ✓ a	back	✓	a ␣
␣ ✓	back	a	✓ a ␣
␣	back	✓	a ✓ a ␣
␣	back	␣	✓ a ✓ a ␣
␣	none	✓	a ✓ a ␣
␣ ✓	none	a	✓ a ␣
␣ ✓ ✓	one	✓	a ␣
␣ ✓ ✓ ✓	one	a	␣
␣ ✓ ✓ ✓ a	even	␣	␣
␣ ✓ ✓ ✓	back	a	␣
␣ ✓ ✓	back	✓ a	␣
␣ ✓	back	✓	✓ a ␣
␣	back	✓	✓ ✓ a ␣
␣	back	␣	✓ ✓ ✓ a ␣
␣	none	✓	✓ ✓ a ␣
␣ ✓	none	✓	✓ a ␣
␣ ✓ ✓	none	✓	a ␣
␣ ✓ ✓ ✓	none	a	␣
␣ ✓ ✓ ✓ ✓	one	␣	␣
␣ ✓ ✓ ✓	acc	✓	␣

דוגמה 1.8

בדקו אם המילה

aaa

מתקבלת על ידי המכונת טיורינג בדוגמה 1.6.

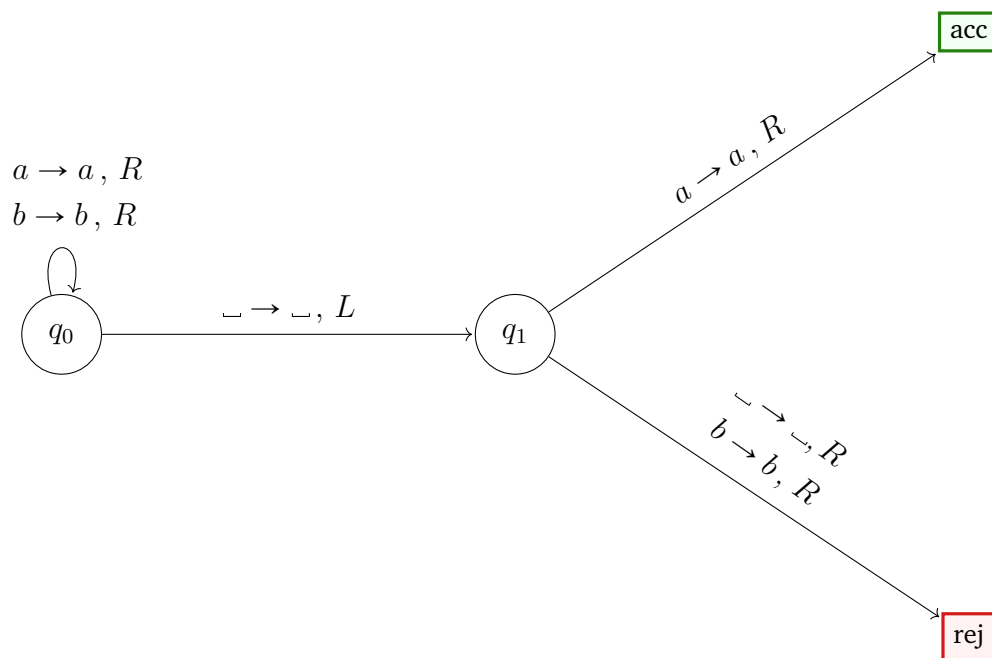
פתרון:

␣	none	a	a	a	␣
␣	✓	one	a	a	␣
␣	✓	a	even	a	␣
␣	✓	a	✓	odd	␣
␣	✓	a	✓	␣	rej

u	q	σ	v
␣	none	a	aa ␣
␣ ✓	one	a	a ␣
␣ ✓ a	even	a	␣
␣ ✓ a ✓	odd	␣	␣
␣ ✓ a ✓ ␣	rej	␣	␣

דוגמה 1.9

מהי שפת המכונה:



פתרון:

תיאור מילולי:

- במצב התחלתי q_0 :

* אם אנחנו רואים a , עוברים למשבצת הבאה לימין הראש.

* אם אנחנו רואים b , עוברים למשבצת הבהאה לשמאל הראש.

- ממשיכים כך עד שנגיע לתו רווח, כלומר לסוף המילה, ואז עוברים למשבצת לשמאל הראש, כלומר לתו האחרון של המילה.

* אם אנחנו רואים a, המילה מתקבלת. (ז"א התו האחרון הינו a.)

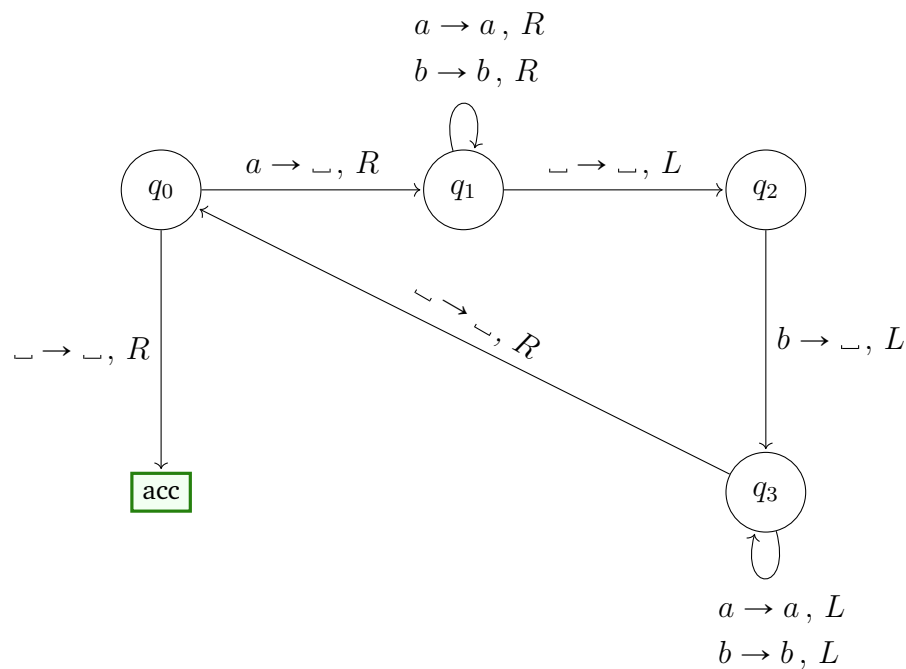
* אם אנחנו רואים b, המילה נדחית. (ז"א התו האחרון הינו b.)

* אם אנחנו רואים תו-רווח המילה נדחית. (ז"א המילה הינה ריקה.)

תשובה סופית: המכונה מקבלת שפת המילים המסתיימות באות a.

דוגמה 1.10

מהי שפת המכונה:



פתרון:

תיאור מילולי:

- במצב התחלתי q_0 :
 - * אם אנחנו רואים b , המילה נדחית.
 - * אם אנחנו רואים a , המילה מתקבלת.
 - * אם אנחנו רואים a , כותבים עליה a ועוברים למשבצת הבאה לימין הראש, והמ"ט עוברת למצב q_1 .
- במצב q_1 אנחנו ראינו a וכתבנו עליה a .
 - * אם אנחנו רואים במשבצת הבאה a או b , ממשיכים למשבצת הבאה לימין והמ"ט נשארת במצב q_1 .
 - * אם אנחנו רואים תו רווח (כלומר הגענו לסוף המילה) הראש a למשבצת השמאלי, כלומר לאות האחרונה של המילה והמ"ט עוברת למצב q_2 .
- במצב q_2 ראינו a בתו הראשון, כתבנו עליה a והראש קורא התו האחרון.
 - * אם אנחנו רואים a המילה נדחית.
 - * אם אנחנו רואים a , המילה נדחית.
 - * אם אנחנו רואים b כותבים עליה b והמ"ט עוברת למצב q_3 .
- במצב q_3 קראנו a בתו הראשון ומחקנו אותה, קראנו b ומחקנו אותה.
 - * הראש a משבצת אחת שמאלה עד שיגיע לתו הראשון ומ"ט חוזרת למצב התחלתי q_0 .

- המ"ט באופן איטרטיבי, עוברת על הקלט ובכל מעבר:
 * אם יש a בתחילת המילה מורידה אותה ומחליפה אותה עם $_$, אחרת המילה נדחית,
 * אם יש b בסופה של המילה מורידה אותה ומחליפה אותה עם $_$, אחרת המילה נדחית.
- אם לאחר מספר מעברים כאלו הסרט ריק, המ"ט מקבלת, וזה יתקיים לכל מילה ורק למילים בשפה

$$\{a^n b^n \mid n \geq 0\}.$$

תשובה סופית: המכונה מקבלת שפת המילים

$$\{a^n b^n \mid n \geq 0\}.$$

דוגמה 1.11

פתרון:

μ	q	σ	ν
$_ _$	q_0	a	aaabbbb $_ _$
$_ _ _$	q_1	a	aabbbb $_ _$
$_ _ _ a$	q_1	a	abbbb $_ _$
$_ _ _ aa$	q_1	a	bbbb $_ _$
$_ _ _ aaa$	q_1	b	bbb $_ _$
$_ _ _ aaab$	q_1	b	bb $_ _$
$_ _ _ aaabb$	q_1	b	b $_ _$
$_ _ _ aaabbb$	q_1	b	$_ _$
$_ _ _ aaabbbb$	q_1	$_$	$_$
$_ _ _ aaabbb$	q_2	b	$_ _$
$_ _ _ aaabb$	q_3	b	$_ _ _$
$_ _ _ aaab$	q_3	b	b $_ _ _$
$_ _ _ aaa$	q_3	b	bb $_ _ _$
$_ _ _ aa$	q_3	a	bbb $_ _ _$
$_ _ _ a$	q_3	a	abbb $_ _ _$
$_ _ _$	q_3	a	aabbb $_ _ _$
$_ _$	q_3	$_$	aaabbb $_ _ _$
$_ _ _$	q_0	a	aabbb $_ _ _$
$_ _ _ _$	q_1	a	abbb $_ _ _$
$_ _ _ _ a$	q_1	a	bbb $_ _ _$
$_ _ _ _ aa$	q_1	b	bb $_ _ _$
$_ _ _ _ aab$	q_1	b	b $_ _ _$
$_ _ _ _ aabb$	q_1	b	$_ _ _$
$_ _ _ _ aabbb$	q_1	$_$	$_ _$
$_ _ _ _ aabb$	q_2	b	$_ _ _$
$_ _ _ _ aab$	q_3	b	$_ _ _ _$
$_ _ _ _ aa$	q_3	b	b $_ _ _ _$
$_ _ _ _ a$	q_3	a	bb $_ _ _ _$
$_ _ _ _$	q_3	a	abb $_ _ _ _$

_____	q_3	—	aabb_____
_____	q_0	a	abb_____
_____	q_1	a	bb_____
_____a	q_1	b	b_____
_____ab	q_1	b	_____
_____abb	q_1	—	_____
_____ab	q_2	b	_____
_____a	q_3	b	_____
_____	q_3	a	b_____
_____	q_3	—	ab_____
_____	q_0	a	b_____
_____	q_1	b	_____
_____b	q_1	—	_____
_____	q_2	b	_____
_____	q_3	—	_____
_____	q_0	—	_____

הגדרה 1.4 גרירה בצעד אחד

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$ מכונת טיורינג, ותהי c_1 ו- c_2 קונפיגורציות של M .
נסמן

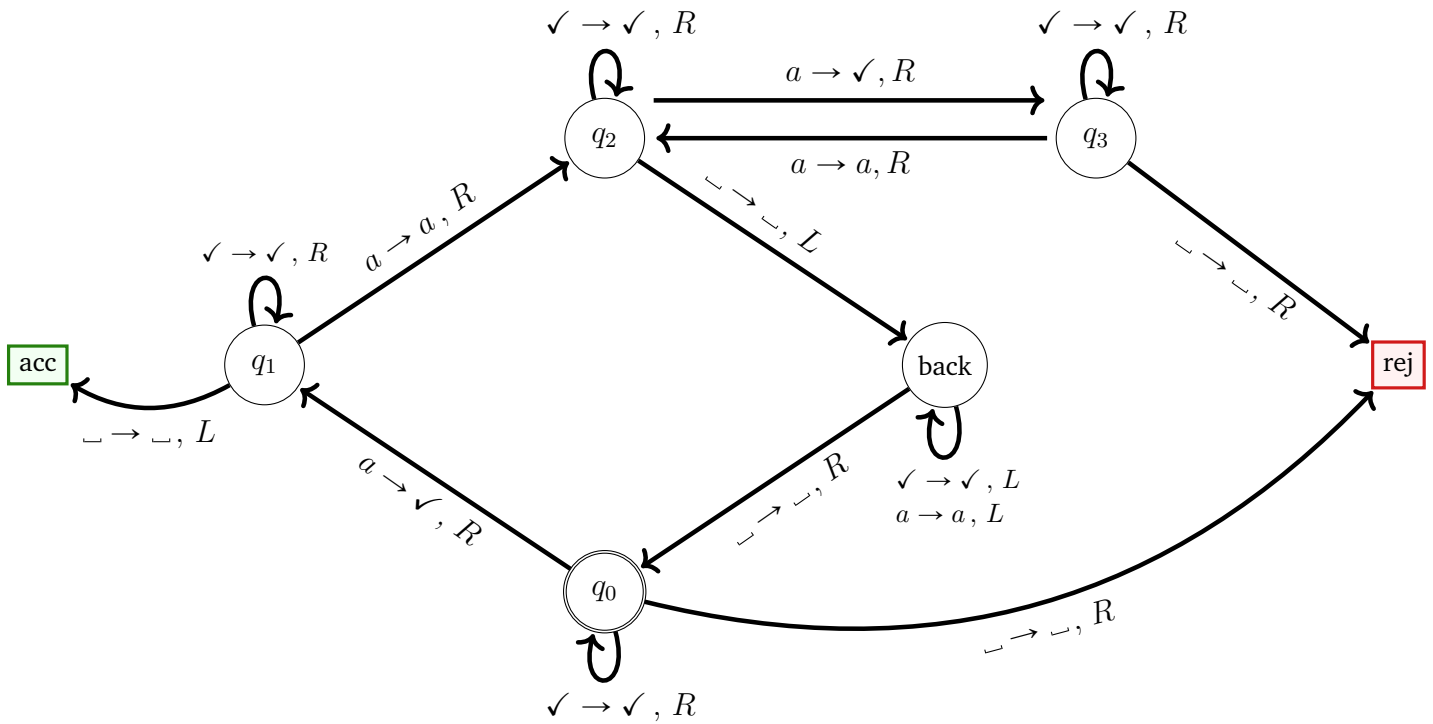
$$c_1 \vdash_M c_2$$

(במילים, c_1 גורר את c_2) אם כשנמצאים ב- c_1 עוברים ל- c_2 בצעד בודד.

דוגמה 1.12 (המשך של דוגמה 1.6)

במכונת טיורינג שמתואר בתרשים דמטה (אשר שווה למ"ט בדוגמה 1.6 רק עם סימנים שונים למצבים) מתקיים

$$\checkmark q_0 a \checkmark a \vdash_M \checkmark \checkmark q_1 \checkmark a$$



הגדרה 1.5 גרירה בכללי

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$ מכונת טיורינג, ותהי c_1 ו- c_2 קונפיגורציות של M .
נסמן

$$c_1 \vdash_M^* c_2$$

(במילים, c_1 גורר את c_2) אם ניתן לעבור מ- c_1 ל- c_2 ב-0 או יותר צעדים.

דוגמה 1.13 (המשך של דוגמה 1.6)

במכונת טיורינג שמתואר בתרשים דמטה (אשר שווה למ"ט בדוגמה 1.6 רק עם סימנוים שונים למצבים) מתקיים

$$\checkmark q_0 a \checkmark a \vdash_M^* \checkmark \checkmark \checkmark q_4 a$$

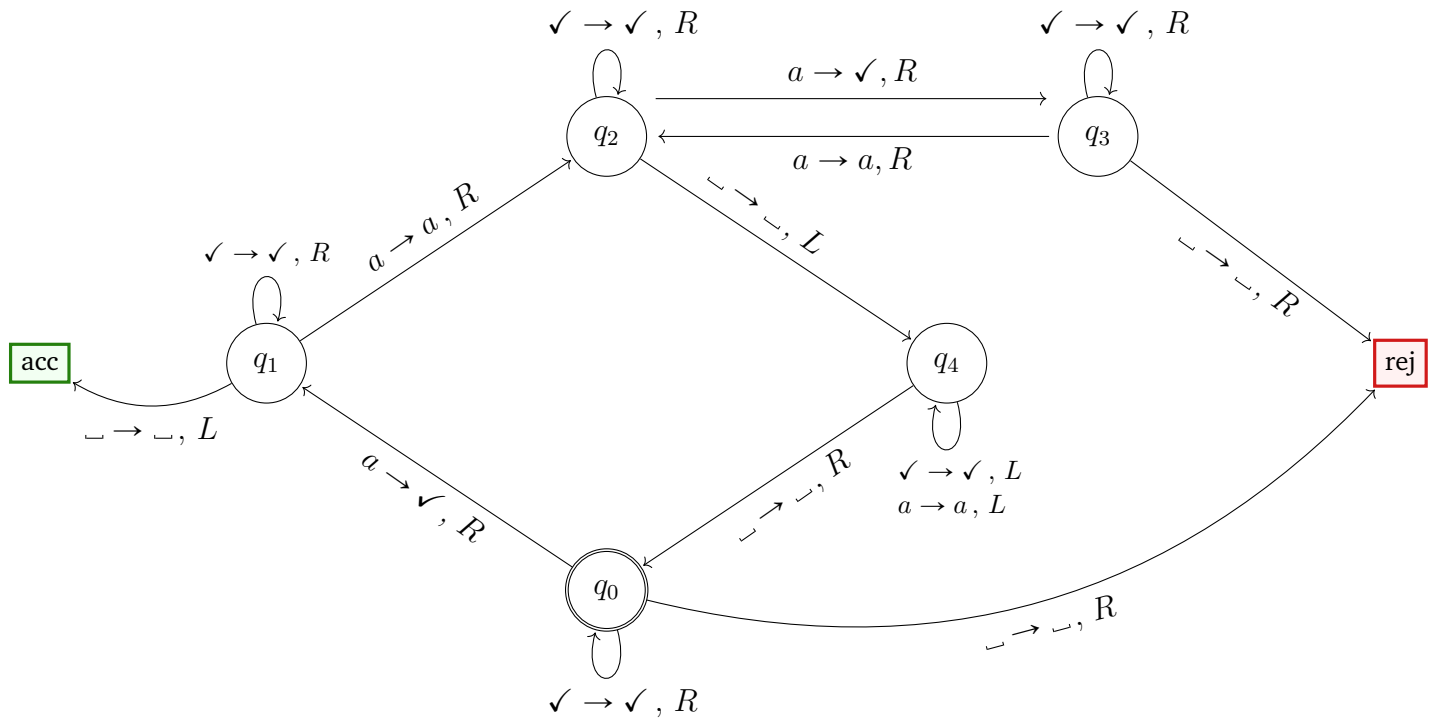
כי

$$\checkmark q_0 a \checkmark a \vdash_M \checkmark \checkmark q_1 \checkmark a$$

$$\vdash_M \checkmark \checkmark \checkmark q_1 a$$

$$\vdash_M \checkmark \checkmark \checkmark a q_2 _$$

$$\vdash_M \checkmark \checkmark \checkmark q_4 a .$$



הגדרה 1.6 קבלה ודחייה של מחרוזת

תהי

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$$

מכונת טיורינג, ו-

$$w \in \Sigma^*$$

מחרוזת. אומרים כי

• M מקבלת את w אם

$$q_0 w \vdash_M^* u \ q_{acc} \sigma v$$

עבור $v, u \in \Gamma^*, \sigma \in \Gamma$ כלשהם,

• M דוחה את w אם

$$q_0 w \vdash_M^* u \ q_{rej} \sigma v$$

עבור $v, u \in \Gamma^*, \sigma \in \Gamma$ כלשהם.

הגדרה 1.7 הכרעה של שפה

תהי

$$M = (Q, \Sigma, \Gamma, \delta, q_0, acc, q_{rej})$$

מכונת טיורינג, ו-

$$L \subseteq \Sigma^*$$

שפה. אומרים כי M מכריעה את L אם לכל $w \in \Sigma^*$ מתקיים

• $M \Leftarrow w \in L$ מקבלת את w .

• $M \Leftarrow w \notin L$ דוחה את w .

הגדרה 1.8 קבלה של שפה

תהי

$$M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$$

מכונת טיורינג, ו-

$$L \subseteq \Sigma^*$$

שפה. אומרים כי M מקבלת את L אם לכל $w \in \Sigma^*$ מתקיים• אם $w \in L$ אז M מקבלת את w .• אם $w \notin L$ אז M לא מקבלת את w .

במקרה כזה נכתוב ש-

$$L(M) = L.$$

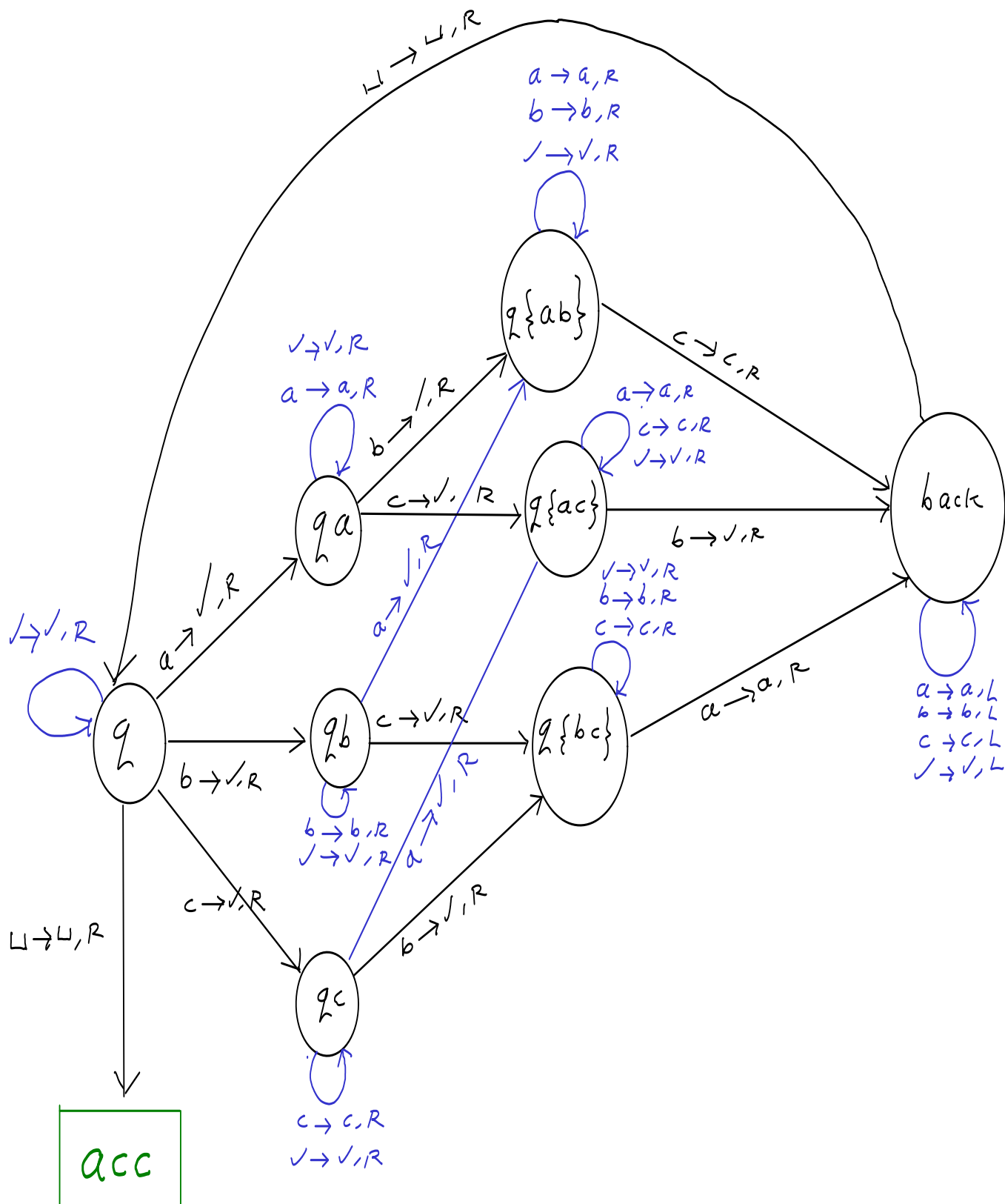
1.3 טבלת המעברים

דוגמה 1.14

בנו מכונת טיורינג שמכריעה את השפה

$$L = \{w = \{a, b, c\}^* \mid \#a_w = \#b_w = \#c_w\}$$

פתרון:



מצב	סימון בסרט	מצב חדש	כתיבה	תזוזה	תנאי
$q.S$	σ	$q.(S \cup \{\sigma\})$	\checkmark	R	$\sigma \notin S$
$q.S$	σ	$q.S$		R	$\sigma \in S$
$q/\{a, b, c\}$	a, b, c, \checkmark	back		L	
$q.\emptyset$	\perp	acc		R	
back	a, b, c, \checkmark	back		L	
back	\perp	$q.\emptyset$		R	

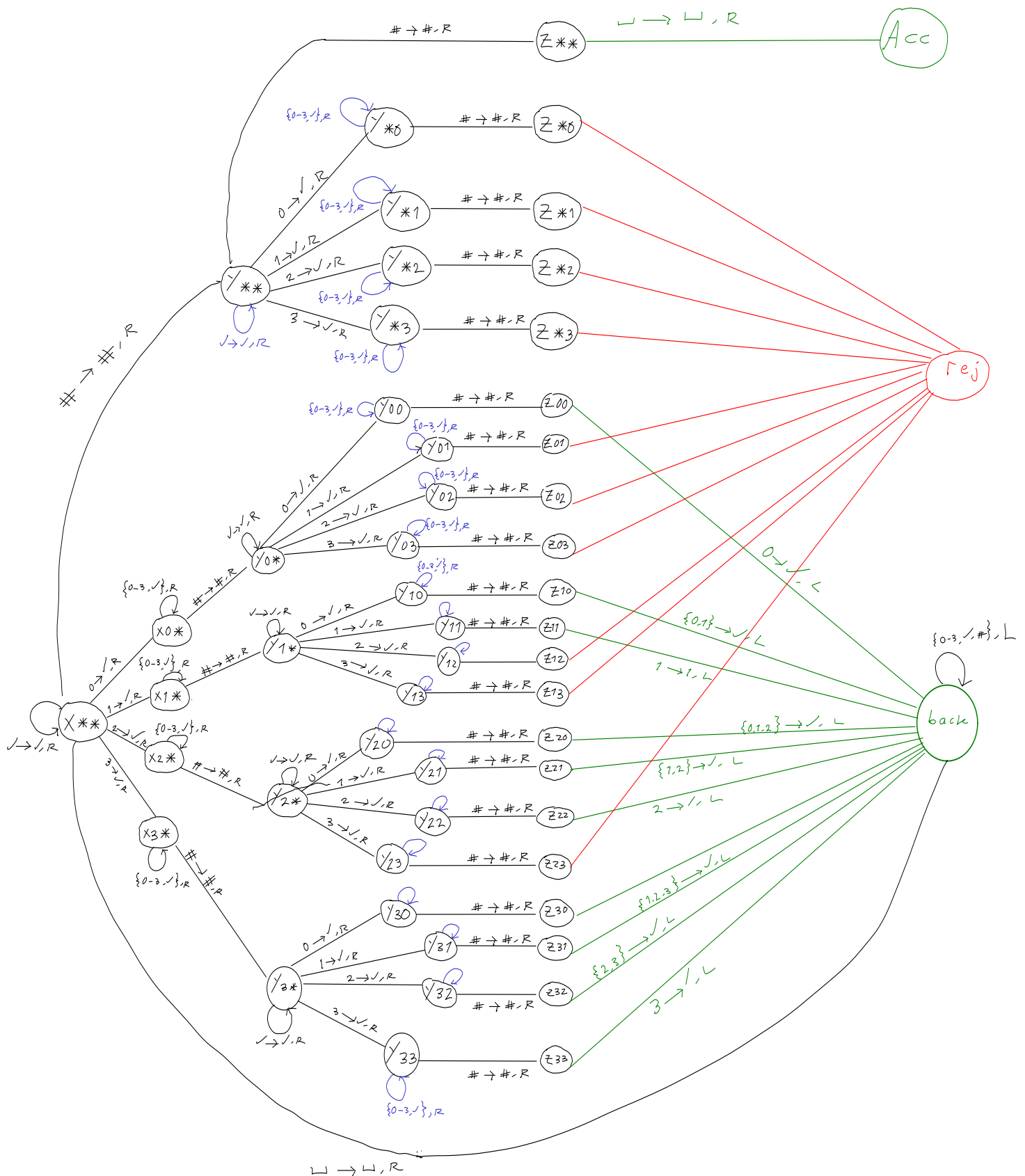
דוגמה 1.15

בנו מכונת טיורינג שמכריעה את השפה

$$\{x_1 \dots x_k \# y_1 \dots y_k \# z_1 \dots z_k \mid x_i, y_i, z_i \in \{0, \dots, 3\}, \forall i, x_i \geq z_i \geq y_i\}$$

פתרון:

$$L = \{X_1 X_2 \# Y_1 Y_2 \# Z_1 Z_2 \mid X_i, Y_i, Z_i \in \{0,1,2,3\} \forall i, X_1 \geq X_2, Y_1 \geq Y_2\}$$



תנאי	תזוזה	כתיבה	מצב חדש	סימון בסרט	מצב
	R	✓	$X\sigma^*$	σ	X^{**}
	R	✓	X^{**}	✓	X^{**}
	R		$X\sigma^*$	$0, 1, \dots, 9, \checkmark$	$X\sigma^*$
	R		$Y\tau^*$	#	$X\tau^*$
	R		$Y\tau\sigma$	σ	$Y\tau^*$
	R		$Y\tau^*$	✓	$Y\tau^*$
	R		$Y\tau\sigma$	$0, 1, \dots, 9, \checkmark$	$Y\tau\sigma$
	R		$Z\tau_1\tau_2$	#	$Y\tau_1\tau_2$
	R		$Z\tau_1\tau_2$	✓	$Z\tau_1\tau_2$
	L	✓	back	σ	$Z\tau_1\tau_2$
	R		acc	\sqsubset	Z^{**}
	L		back	$0, 1, \dots, 9, \checkmark$	back
	R		X^{**}	\sqsubset	back

1.4 חישוב פונקציות

הגדרה 1.9 מכונת טיורינג שמחשבת פונקציה f

תהי $f : \Sigma_1^* \rightarrow \Sigma_2^*$ ותהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$ מכונת טיורינג. אומרים כי M מחשבת את f אם:

- $\Sigma = \Sigma_1$ ו- $\Sigma_2 \subset \Gamma$.
- לכל $w \in \Sigma_1^*$ מתקיים $q_0 w \vdash q_{acc} f(w)$.

דוגמה 1.16 חיבור אונרי

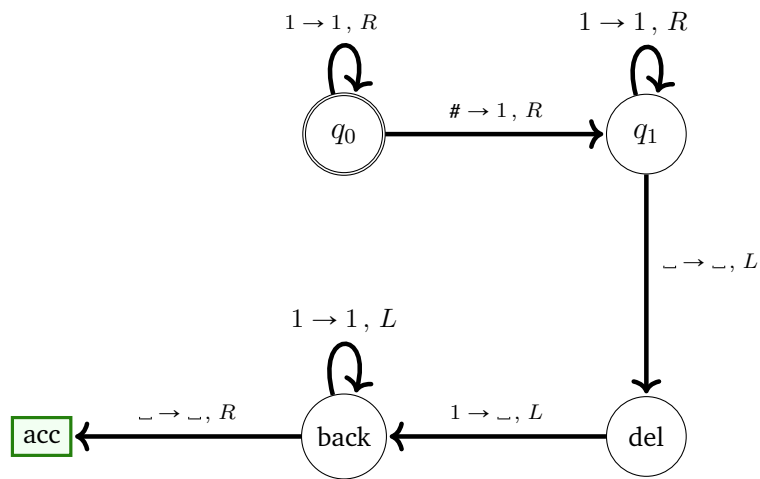
בנו מכונת טיורינג אשר מקבלת את הקלט

$$1^i \# 1^j$$

ומחזירה את פלט

$$1^{i+j}.$$

פתרון:



דוגמה 1.17 כפל אונרי

בנו מכונת טיורינג אשר מקבלת את הקלט

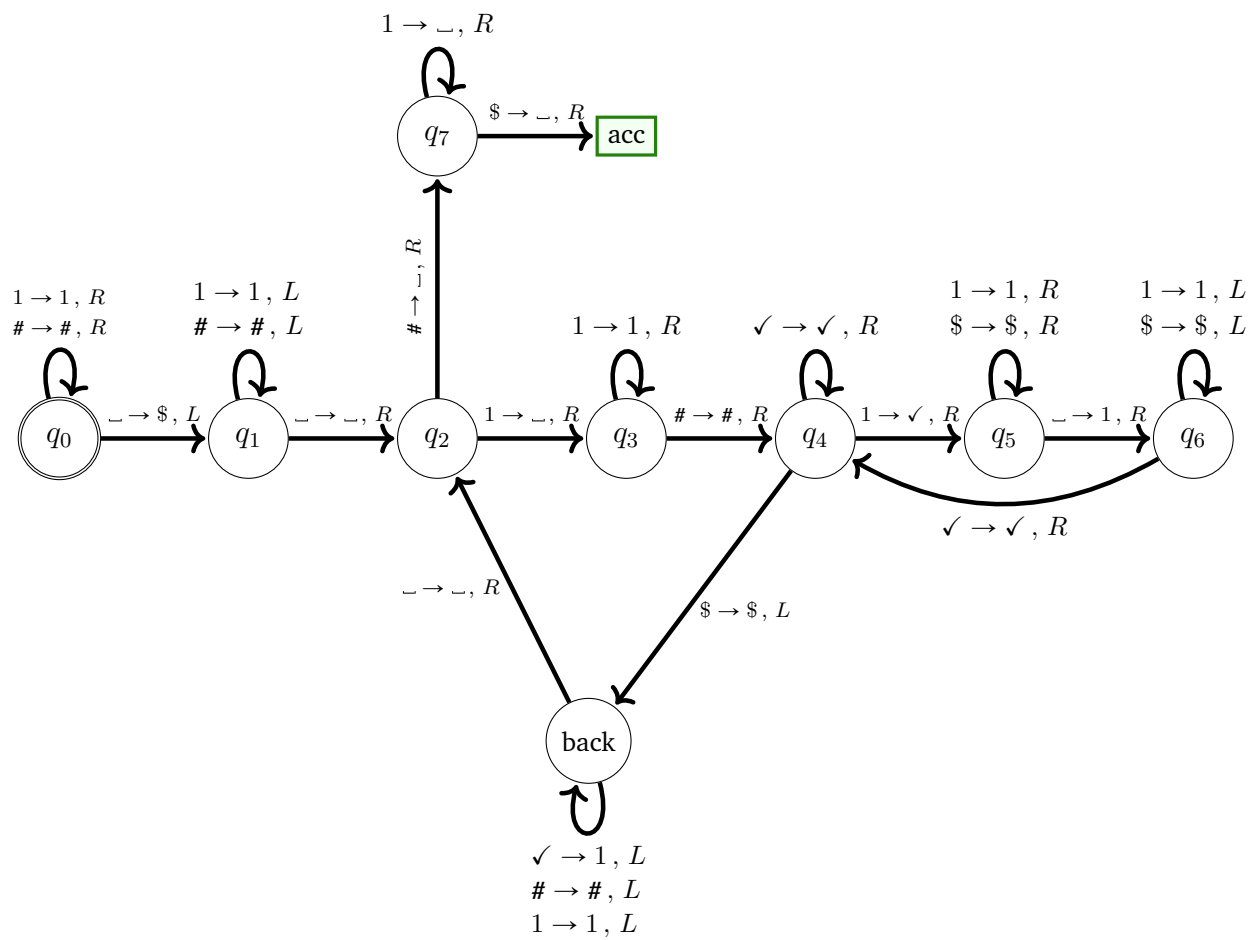
$$1^i \# 1^j$$

ומחזירה את פלט

$$1^{i \cdot j}.$$

פתרון:

- לדוגמה, נניח שהקלט הוא 2 כפול 2. הקלט הוא 11#11.
- נרצה להבדיל בין הקלט לבין הפלט. לכן בתחילת הריצה, נתקדם ימינה עד סוף הקלט ונוסיף שם את התו \$.
- לאחר מכן נחזור לתחילת הקלט. על כל אות 1 במילה השמאלית נעתיק את המילה הימינית לאחר סימן ה-\$.
- לאחר מכן נשאיר רק את התווים שלאחר סימן ה-\$.
- כלומר, נמחק את כל מה שאינו פלט.



μ	q	σ	ν
$_$	q_0	1	1#11 $_$
$_11\#11$	q_1	$_$	$_$
$_11\#11$	q_1	\$	$_$
$_$	q_1	$_$	11#11\$
$_$	q_2	1	1#11\$
$_ _$	q_3	1	#11\$
$_ _1\#$	q_4	1	1\$
$_ _1\#\checkmark$	q_5	1	\$
$_ _1\#\checkmark 1\$$	q_5	$_$	$_$
$_ _1\#\checkmark 1\$1$	q_6	$_$	$_$
$_ _1\#$	q_6	\checkmark	1\$1 $_$
$_ _1\#\checkmark$	q_4	1	\$1 $_$
$_ _1\#\checkmark\checkmark$	q_5	\$	1 $_$
$_ _1\#\checkmark\checkmark \1	q_5	$_$	$_$
$_ _1\#\checkmark\checkmark \11	q_6	$_$	$_$
$_ _1\#\checkmark$	q_6	\checkmark	\$11 $_$
$_ _1\#\checkmark\checkmark$	q_4	\$	11 $_$
$_ _1\#\checkmark$	back	\checkmark	\$11 $_$
$_$	back	$_$	1#11\$11 $_$
$_ _$	q_2	1	#11\$11 $_$
$_ _ _$	q_3	#	11\$11 $_$
$_ _ _ \#$	q_4	1	1\$11 $_$

_ _ _#✓	q_5	1	\$11_
_ _ _#✓1\$11	q_5	_	_
_ _ _#✓1\$111	q_6	_	_
_ _ _#	q_6	✓	1\$111_
_ _ _#✓	q_4	1	\$111_
_ _ _#✓✓	q_5	\$	111_
_ _ _#✓✓\$111	q_5	_	_
_ _ _#✓✓\$1111	q_6	_	_
_ _ _#✓	q_4	✓	\$1111
_ _ _#✓✓	q_4	\$	1111
_ _ _#✓	back	✓\$	1111
_ _	back	_	#11\$1111
_ _ _	q_2	#	11\$1111
_ _ _ _	q_7	1	1\$1111
_ _ _ _ _	q_7	\$	1111
_ _ _ _ _	acc	1	111

שיעור 2

מודלים חשובים שקולית

הגדרה 2.1 מודל חשובי

מודל חשובי הוא אוסף של מכונות טיורינג שעבורן מוגדרים המושגים של הכרעה וקבלה של שפות.

הגדרה 2.2 מודלים שקולים חשובית

יהיו A ו- B מודלים חשוביים. אומרים כי A ו- B שקולים אם לכל שפה L התנאים הבאים מתקיימים:

(1) קיימת מ"ט במודל A שמכריעה את L אם"ם קיימת מ"ט במודל B שמכריעה את L .

(2) קיימת מ"ט במודל A שמקבלת את L אם"ם קיימת מ"ט במודל B שמקבלת את L .

דוגמה 2.1

נסמן ב- T את מודל מכונת הטיורינג הבסיסי.

במודל זה בכל צעד ניתן לזוז ימינה או שמאלה. אך לא ניתן להישאר במקום, באותה המשבצת בסרט. במודל זה, הסרט הוא אינסופי לשני הכיוונים. בתחילת החישוב הראש נמצא בתחילת הקלט.

נסמן ב- O את מודל מכונת הטיורינג עם סרט ימינה בלבד.

במודל זה בכל צעד ניתן לזוז ימינה או שמאלה. אך לא ניתן להישאר במקום, באותה המשבצת בסרט. במודל זה, הסרט הוא אינסופי לכיוון אחד בלבד - ימינה. בתחילת החישוב, הקלט ממוקם בקצה השמאלי של הסרט והראש נמצא בתחילת הקלט. החישוב מתנהל כמו במכונה במודל T , למעט כאשר הראש נמצא במשבצת השמאלית ביותר בסרט וצריך לזוז ש מאלה - במקרה כזה הראש נשאר במקום ולא זז.

הוכיחו כי המודל T והמודל O שקולים חשובית.

פתרון:

יש להוכיח ש:

- לכל מ"ט במודל O קיימת מ"ט שקולה במודל T .
- לכל מ"ט במודל T קיימת מ"ט שקולה במודל O .

כיוון ראשון

נוכיח כי לכל מ"ט במודל O קיימת מ"ט שקולה במודל T . כלומר:

נתונה $M^O = (Q^O, \Sigma^O, \Gamma^O, \delta^O, q_0^O, acc^O, rej^O)$ במודל O .

נבנה, $M^T = (Q^T, \Sigma^T, \Gamma^T, \delta^T, q_0^T, acc^T, rej^T)$ שקולה במודל T .

נעבוד רק עם צד ימין של הסרט האינסופי של M^T ואז M^T תהיה שקולה ל- M^O .

רכיבי המ"ט M^T זהים לאלו של המ"ט M^O , מלבד מהתכונה שהראש של M^O לא זז מעבר לקצה השמאלי של הקלט.

לכן כדי ש- M^T תהיה שקולה ל- M^O נוסיף מעברים לפונקצית המעברים של M^T כדי שהראש של M^T לא יז מעבר לקצה השמאולי של הקלט.

הרעיון הוא לסמן את המשבצת שמשמאל לתחילת הקלט עם סימן מיוחד \$, ואז להוסיף מעברים לפונקצית המעברים של M^T שמבטיחים שאם הראש נמצא למשבצת שמסומנת \$ אז הוא מיד חוזר ו- M^T חוזרת למצב ההתחתי של המ"ט M^O . זה מתבצע על ידי הוספת השורות הבאות לטבלת המעברים של M^T :

תנאי	תזוזה	כתיבה	מצב חדש	סימון	מצב
	L	Ω	$q_\$$	σ	q_0^T
	R	$\$$	q_0^O	\perp	$q_\$$
$\forall q \in Q^O$	R	$\$$	q	$\$$	q

$$Q^T = Q^O \cup \{q_0^T, q_\$\}, \quad \Sigma^T = \Sigma^O, \quad \Gamma^T = \Gamma^O \cup \{\$\}, \quad \text{acc}^T = \text{acc}^O, \quad \text{rej}^T = \text{rej}^O.$$

כיוון שני

נוכיח כי לכל מ"ט במודל T קיימת מ"ט שקולה במודל O . כלומר:

$$\text{נתונה } M^T = (Q^T, \Sigma^T, \Gamma^T, \delta^T, q_0^T, \text{acc}^T, \text{rej}^T) \text{ במודל } T.$$

$$\text{נבנה } M^O = (Q^O, \Sigma^O, \Gamma^O, \delta^O, q_0^O, \text{acc}^O, \text{rej}^O) \text{ שקולה במודל } O.$$

הרעיון הוא לסמן קו על הסרט במשבצת באמצע הקלט, ואז לקפל את הסרט בקו הזה. באופן הזה נקבל סרט עם קצה שמאולי ואינסופי ימינה. במשבצות של הסרט החדש המקופל יש שני תווים, אחד למעלה (U) ואחד למטה (D), מלבד מנקודת הקיפול שבו יש משבצת אחת שמסומנת \$.

באופן הזה אפשר לסמלץ את המכונה M^O במכונה M^T על ידי הוספת המעברים הבאים לטבלת המעברים של M^T . לכל $\tau, \sigma, \pi \in \Gamma^T$:

תנאי	תזוזה	כתיבה	מצב חדש	סימון	מצב
תזוזה שמאלה: $(q, \sigma) \xrightarrow{M^T} (p, \tau, L)$	L	π τ	$p.D$	π σ	$q.D$
	R	τ π	$p.U$	σ π	$q.U$
תזוזה שמאלה: $(q, _) \xrightarrow{M^T} (p, \tau, L)$	L	$_$ τ	$p.D$	$_$	$q.D$
	R	τ $_$	$p.U$	$_$	$q.U$
תזוזה ימינה: $(q, \sigma) \xrightarrow{M^T} (p, \tau, R)$	R	π τ	$p.D$	π σ	$q.D$
	L	τ π	$p.U$	σ π	$q.U$
תזוזה ימינה: $(q, _) \xrightarrow{M^T} (p, \tau, R)$	R	$_$ τ	$p.D$	$_$	$q.D$
	L	τ $_$	$p.U$	$_$	$q.U$
	R	\curvearrowright	$q.U$	\$	$q.D$
	R	\curvearrowright	$q.D$	\$	$q.U$
אתחול					
$\tau \in \Sigma \cup \{ _ \}$ $\sigma \in \Sigma$	R	\$	$q.\tau$	τ	q_0^O
	R	$_$ σ	$q.\tau$	τ	$q.\sigma$
	L	$_$ $_$	back	$_$	$q._$
	L	\curvearrowright	back	$_$ τ	back
	R	\curvearrowright	$q_0^T.D$	\$	back
סיום					
			acc^O	הכל	$acc^T.D$
			acc^O	הכל	$acc^T.U$
			rej^O	הכל	$rej^T.D$
			rej^O	הכל	$rej^T.U$
כל השאר עובריסל-rej					

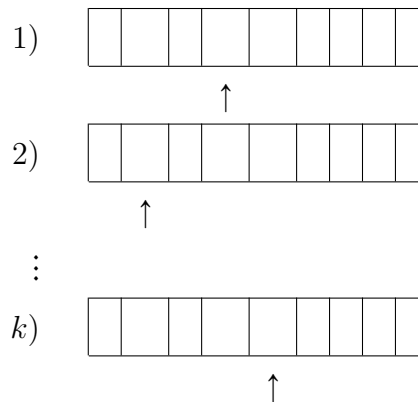
$$\Gamma^O \supseteq (\Gamma^T \times \Gamma^T) \cup \{\$ \} .$$

שיעור 3

מכונות טיורינג מרובות סרטים

3.1 מכונת טיורינג מרובת סרטים: הגדרה היוריסטית

מכונת טיורינג מרובת סרטים (מטמ"ס) היא הכללה של מ"ט עם סרט יחיד. ההבדל הוא שלמטמ"ס ישנו מספר סופי של סרטים, נניח $k > 1$ סרטים.



- לכל סרט יש ראש שלו.

- בתחילת העבודה הקלט w כתוב בתחילת הסרט הראשון וכל שאר הסרטים ריקים. הראשים בכל סרט מצביעים על התא הראשון בסרט, והמכונה נמצאת במצב התחלתי q_0 .

- בכל צעד חישוב, לפי המצב הנוכחי ול- k התווים שמתחת ל- k הראשים, המכונה מחליטה לאיזה מצב לעבור, מה לכתוב מתחת לכל אחד מ- k הראשים ולכן להזיז את הראש בכל אחד מ- k סרטים.

- הראשים של הסרטים יכולים לזוז באופן בלתי-תלוי בהתאם לפונקצית המעברים של המטמ"ס.

3.2 מכונת טיורינג מרובת סרטים: הגדרה פורמלית

הגדרה 3.1 מכונת טיורינג מרובת סרטים

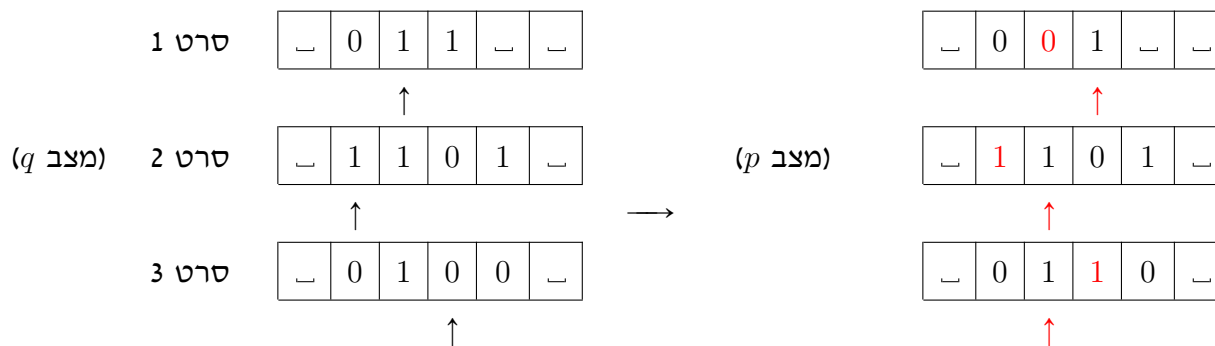
מכונת טיורינג מרובת סרטים היא שביעיה:

$$M = (Q, \Sigma, \Gamma, \delta_k, q_0, q_{acc}, q_{rej})$$

כאשר $Q, \Sigma, \Gamma, q_0, q_{acc}, q_{rej}$ מוגדרים כמו מ"ט עם סרט יחיד (ראו הגדרה 1.2). ההבדל היחיד בין מ"ט עם סרט יחיד לבין מטב"ס הוא הפונקצית המעברים. עבור מטמ"ס הפונקצית המעברים היא מצורה הבאה:

$$\delta_k : (Q \setminus \{q_{acc}, q_{rej}\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, R, S\}^k$$

3.1 דוגמה



$$\delta_k \left(q, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right) = \left(p, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} R \\ R \\ L \end{pmatrix} \right).$$

3.3 קונפיגורציה של מטמ"ס

הכללה של קונפיגורציה של מטמ"ס עם סרט יחיד:

$$\begin{pmatrix} u_1 q & v_1 \\ u_2 q & v_2 \\ \vdots \\ u_k q & v_k \end{pmatrix}$$

3.2 דוגמה

בנו מטמ"ס שמכריעה את השפה:

$$L_{w^R} = \{ w = \{a, b\}^* \mid w = w^R \}.$$

כלומר שפת הפלינדרומים.

פתרון:

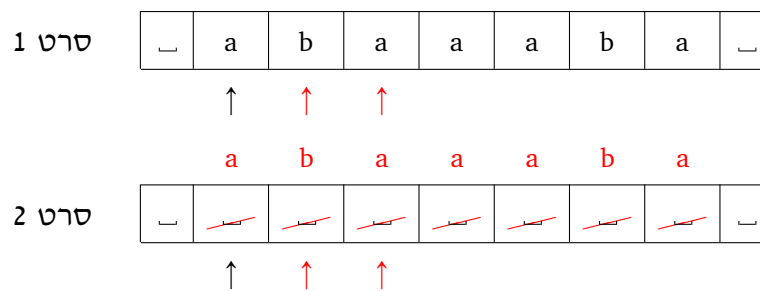
נבנה מטמ"ס עם שני סרטים:

תאור המכונה:

נסמן M_2 המ"ט עם 2 סרטים שמכריעה את השפה L_{w^R} .

$M_2 =$ על הקלט w :

(1) מעתיקה את w לסרט 2.



(2) מזיזה את הראש בסרט 1 לתו הראשון ב- w ואת הראש בסרט 2 לתו האחרון ב- w .

(3) משווה בין התווים שמתחת לראשים:

- אם התו שמתחת לראש בסרט 1 הוא \perp אז $\text{acc} \leftarrow \perp$.
- אם התווים שמתחת לראשים שונים אז $\text{rej} \leftarrow \text{rej}$.
- אחרת מזיזה את הראש בסרט 1 ימינה ואת הראש בסרט 2 שמאלה, וחוזרת לשלב (3).

הפונקציה המעברים של M_2 היא:

$$\delta \left(q_0, \begin{pmatrix} a \\ \perp \end{pmatrix} \right) = \left(q_0, \begin{pmatrix} a \\ a \end{pmatrix}, \begin{pmatrix} R \\ R \end{pmatrix} \right),$$

$$\delta \left(q_0, \begin{pmatrix} b \\ \perp \end{pmatrix} \right) = \left(q_0, \begin{pmatrix} b \\ b \end{pmatrix}, \begin{pmatrix} R \\ R \end{pmatrix} \right),$$

$$\delta \left(q_0, \begin{pmatrix} \perp \\ \perp \end{pmatrix} \right) = \left(q_{\text{back}}, \begin{pmatrix} \perp \\ \perp \end{pmatrix}, \begin{pmatrix} L \\ L \end{pmatrix} \right).$$

נשים לב כי הסיבוכיות זמן של המכונה עם שני סרטים, M_2 היא $O(|w|)$, כאשר w האורך של המילה.

כעת נבנה מ"ט עם סרט יחיד שמכריעה את השפה L_{WR} .

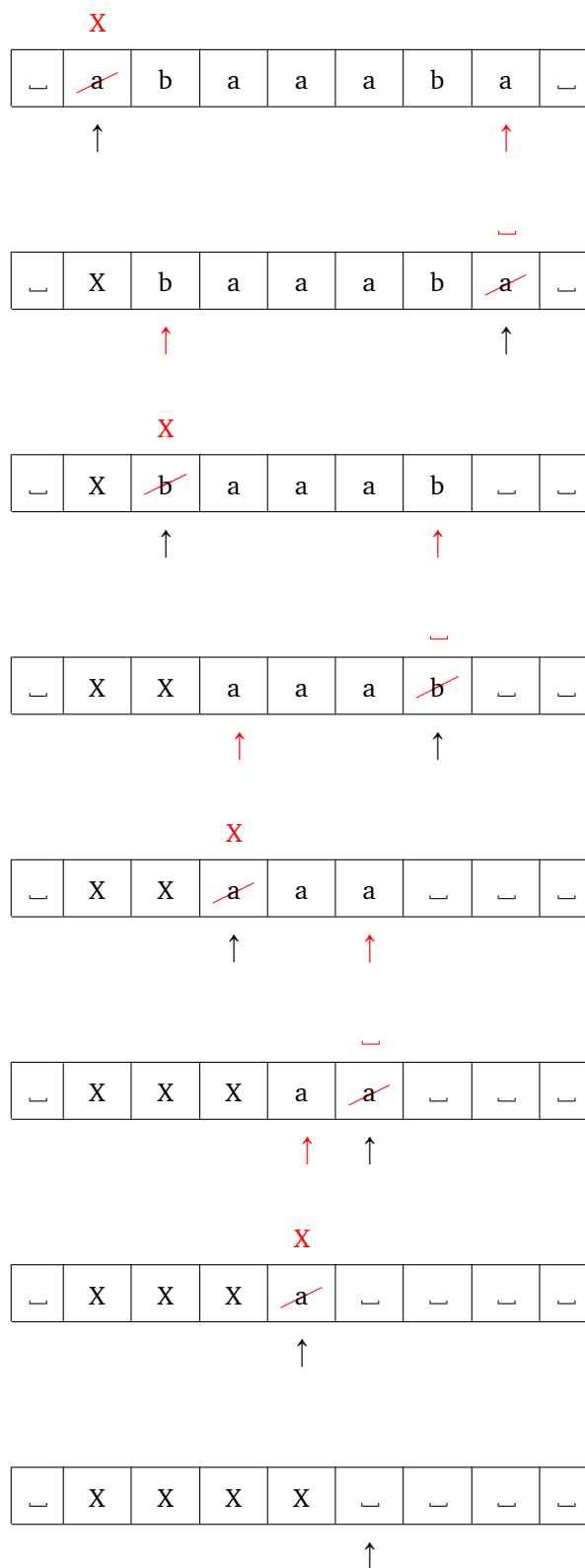
תאור המכונה:

נסמן M_1 המכונה עם סרט יחיד שמכריעה את השפה L_{wR} .

$M_1 =$ על הקלט w :

- (1) אם התו שמתחת לראש הוא \perp אז $\text{acc} \leftarrow M_1$.
- (2) זוכרת את התו שמתחת לראש ומוחקת אותו ע"י X .
- (3) מזיזה את הראש ימינה עד התו הראשון משמאל ל- \perp .

- אם התו שמתחת לראש הוא X אז $\text{acc} \leftarrow X$.
- אם התו שונה מהתו שזכרנו אז $\text{rej} \leftarrow \text{rej}$.
- מוחקת את התו שמתחת לראש ע"י \perp , מזיזה את הראש שמאלה עד התו הראשון מימין ל- X וחוזרת לשלב (1).



3.4 שקילות בין מטמ"ס למ"ט עם סרט יחיד

מ"ט עם סרט יחיד היא מקרה פרטי של מטמ"ס.

משפט 3.1 שקילות בין מטמ"ס למ"ט עם סרט יחיד

לכל מטמ"ס M קיימת מ"ט עם סרט יחיד M' השקולה ל- M .

כלומר, לכל קלט $w \in \Sigma^*$:

- אם M מקבלת את $w \iff M'$ מקבלת את w .
- אם M דוחה את $w \iff M'$ דוחה את w .
- אם M לא עוצרת על $w \iff M'$ לא עוצרת על w .

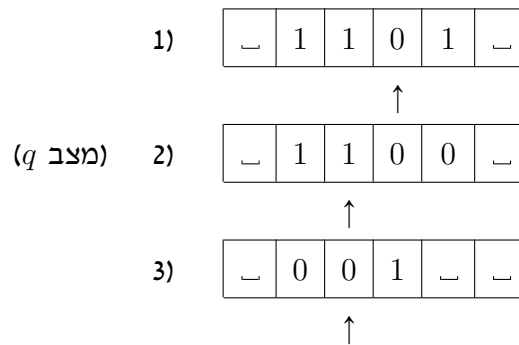
הוכחה:

בהינתן מטמ"ס $M = (Q, \Sigma, \Gamma, \delta_k, q_0, q_{acc}, q_{rej})$ עם k סרטים, נבנה מ"ט עם סרט יחיד $M' = (Q', \Sigma, \Gamma', \delta', q'_0, q'_{acc}, q'_{rej})$ השקולה ל- M באופן הבא:

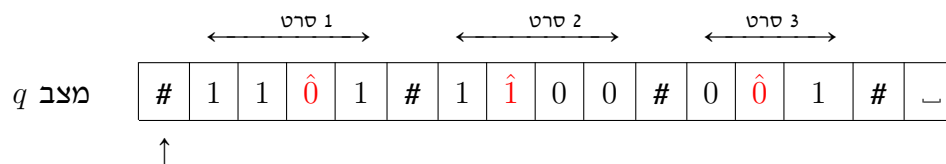
רעיון הבנייה:

בהינתן קלט $w \in \Sigma^*$, M' תבצע "סימולציה" של ריצה M על w .

ב- M



ב- M'



• M' תשמור את התוכן של k הסרטים של M על הסרט, רק שהתוכן של סרט i יופיע בין $\#_i$ ל- $\#_{i+1}$.

• M' תשמור את המיקום של הראשים של M ע"י הכפלת הא"ב Γ .

כלומר, לכל אות $\alpha \in \Gamma$, M' תשמור שתי אותיות α ו- $\hat{\alpha}$ ב- Γ , כך ש- $\hat{\alpha}$ תסמן את התו שמתחת לראש בכל סרט.

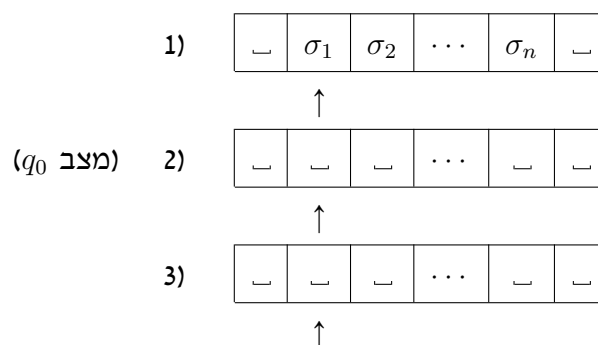
- בכל צעד חישוב, M' סורקת את הסרט שלה משמאל לימין כדי ללמוד מהם התווים שמתחת לראשים (התווים שמסומנים ב- $\hat{\alpha}$).
- M' משתמשת בפונקצית המעברים δ_k של M כדי לחשב את המעבר הבא.
- M' סורקת את הסרט שלה משמאל לימין כדי לעדכן את הסרטים ואת המיקום הראשים בהם.

תאור הבנייה של M' :

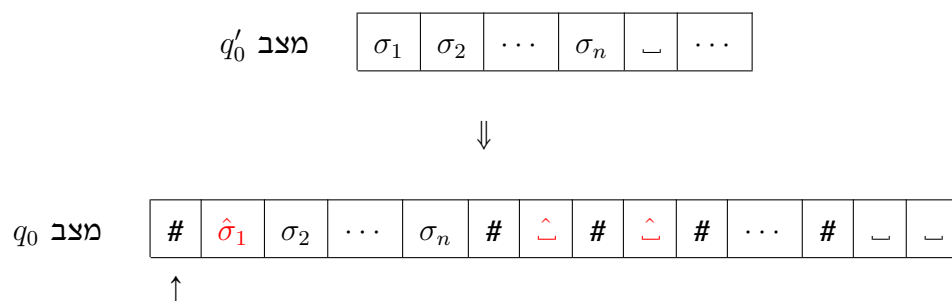
(1) שלב האיתחול

בהינתן קלט $w = \sigma_1 \sigma_2 \cdots \sigma_n$, מאתחלת את הקונפיגורציה ההתחלתית של M על הסרט שלה.

ב- M

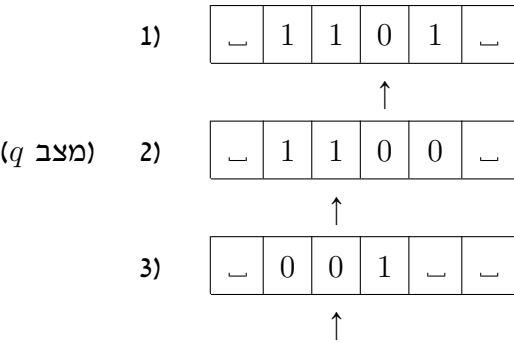


ב- M'

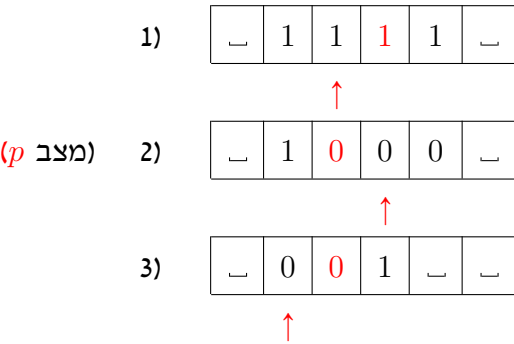


(2) תאור צעד חישוב של M

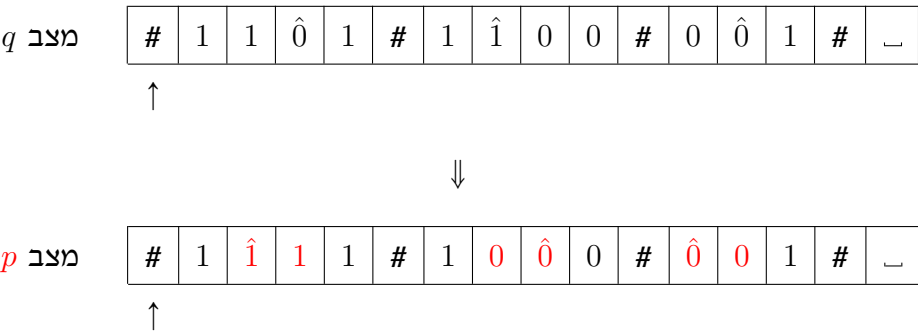
ב- M



$$\delta_k \left(q, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right) = \left(p, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} L \\ R \\ L \end{pmatrix} \right)$$

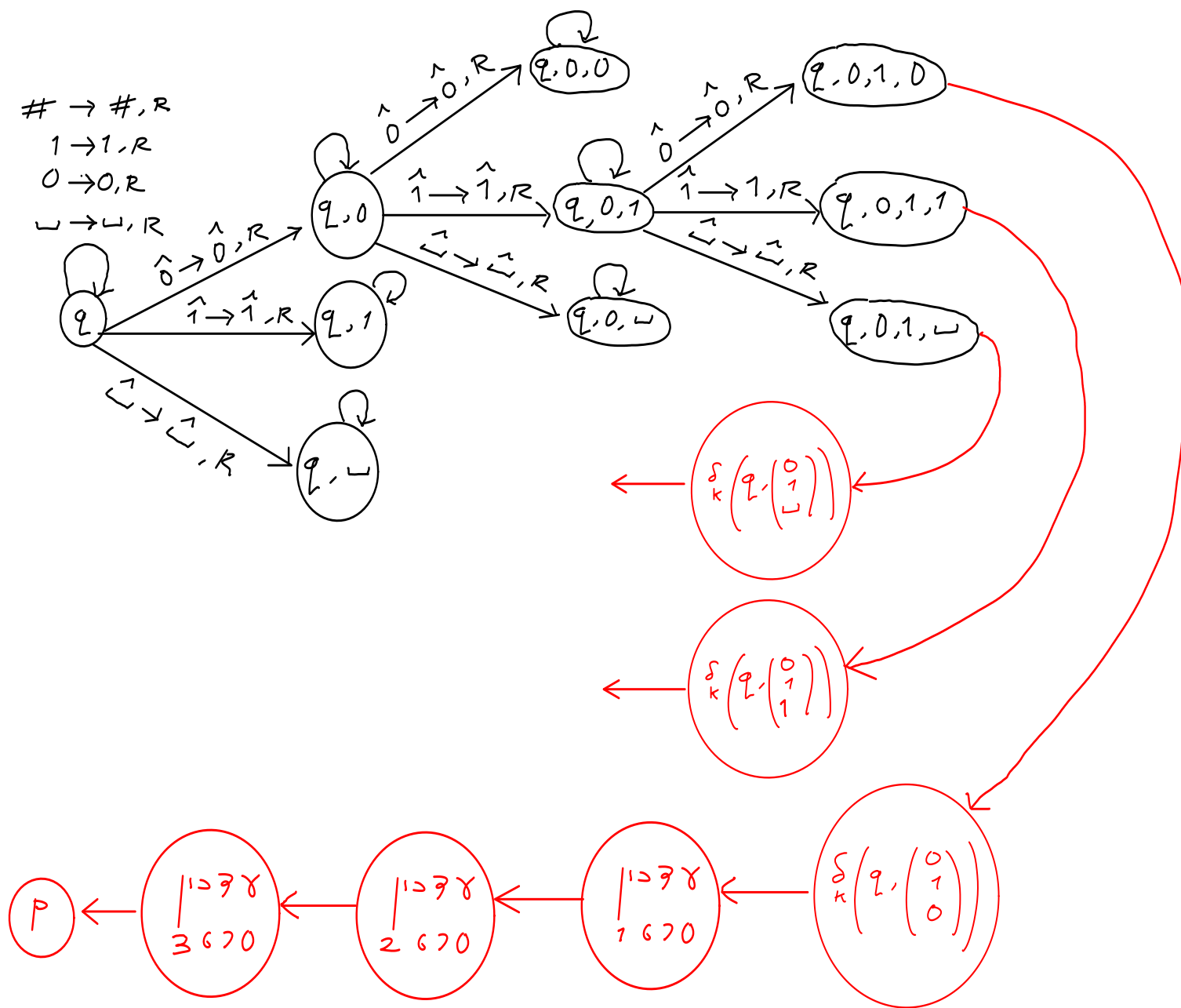


ב- M'



- איסוף מידע
- M' סורקת את הסרט שלה משמאל לימין ומזהה את התווים שמסומנים ב- $\hat{\alpha}$. מידע זה ניתן לשמור במצבים. לדוגמה:

$$q, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$



p מצב

#	1	$\hat{1}$	1	1	#	1	0	$\hat{0}$	0	#	$\hat{0}$	0	1	#	_
---	---	-----------	---	---	---	---	---	-----------	---	---	-----------	---	---	---	---

- עדכון הסרטים

M' סורקת את הסרט שלה פעם נוספת כדי לפעול על פי פונקצית המעברים, כלומר, לעדכן את התאים שמתחת לראשים ולעדכן את מיקום הראשים.



שיעור 4

מכונת טיורינג אי-דטרמיניסטית

4.1 הגדרה של מכונת טיורינג אי-דטרמיניסטית

4.1 מכונת טיורינג אי-דטרמיניסטית

מכונת טיורינג אי-דטרמיניסטית (מ"ט א"ד) היא שביעייה

$$M = (Q, \Sigma, \Gamma, \Delta, q_0, q_{acc}, q_{rej})$$

כאשר $Q, \Sigma, \Gamma, q_0, q_{acc}, q_{rej}$ מוגדרים כמו במ"ט דטרמיניסטי (ראו הגדרה 1.2).

Δ היא פונקצית המעברים

$$\Delta : (Q \setminus \{q_{acc}, q_{rej}\}) \times \Gamma \rightarrow P(Q \times \Gamma \times \{L, R, S\}) .$$

$$\Delta(q, a) = \{(q_1, a, S), (q_2, b, L), \dots\} .$$

כלומר, לכל זוג $q \in Q, a \in \Gamma$ ייתכן מספר מעברים אפשריים, 0, 1 או יותר.

- קונפיגורציה של מ"ט א"ד זהה לקונפיגורציה של מ"ט דטרמיניסטית.

- לכל קונפיגורציה ייתכן מספר קונפיגורציות עוקבות.

- לכל מילה $w \in \Sigma^*$ ייתכן מספר ריצות שונות:

- * ריצות שמגיעות ל- q_{acc} .

- * ריצות שמגיעות ל- q_{rej} .

- * ריצות שלא עוצרות.

- * ריצות שנתקעות.

4.2 הגדרה

מילה $w \in \Sigma^*$ מתקבלת במ"ט א"ד M אם קיימת לפחות ריצה אחת שמגיעה ל- q_{acc} .

השפה של מ"ט א"ד M היא

$$L(M) = \{w \in \Sigma^* \mid \exists u, v \in \Gamma^* : q_0 w \vdash_* u q_{acc} v\}$$

כלומר,

$w \in L(M)$ אם קיימת ריצה אחת שבה M מקבלת את w .

$w \notin L(M)$ אם בכל ריצה של M על w , M דוחה או לא עוצרת, או נתקעת.

הגדרה 4.3 מ"ט א"ד המכריעה שפה L

תהי M מ"ט א"ד.
אומרים כי מ"ט א"ד M מכריעה שפה L אם לכל $w \in \Sigma^*$:

• אם $w \in L$ אז M מקבלת את w .

• אם $w \notin L$ אז M דוחה את w .

הגדרה 4.4 מ"ט א"ד המקבלת שפה L

תהי M מ"ט א"ד.
אומרים כי מ"ט א"ד M מקבלת שפה L אם לכל $w \in \Sigma^*$:

• אם $w \in L$ אז M מקבלת את w .

• אם $w \notin L$ אז M דוחה את w או M לא עוצרת על w .

דוגמה 4.1

נתונה השפה

$$L = \{1^n \mid n \text{ אינו ראשוני}\}, \quad \Sigma = \{1\}.$$

בנו מ"ט המכריעה את השפה L .

פתרון:הרעיון

נבנה מ"ט א"ד N המכריעה את L .

N תבחר באופן א"ד מספר $1 < t < n$ ותבדוק האם t מחלק את n .

	n							
סרט 1	␣	1	1	1	1	1	1	...
	t							
סרט 2	␣	1	1	1	␣	...		

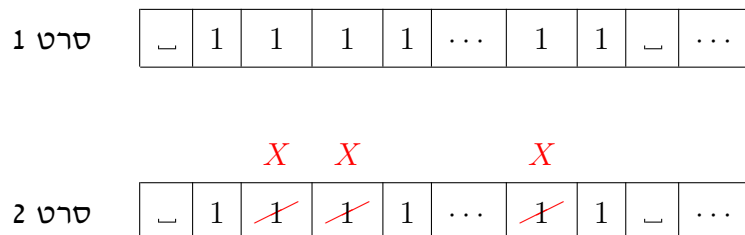
תאור הבניה

$N =$ על קלט 1^n

(שלב 1)

• N בוחרת באופן א"ד מספר $1 < t < n$.

- מעתיקה את w לסרט 2.
- עוברת על העותק משמאל לימין, ובכל תא מחליטה באופן א"ד האם להשאיר את ה-1 או למחוק אותו ע"י X (לדאוג שהמספר שנבחר הוא לא 1 ולא n).
- בסוף המעבר המספר t שנבחר הוא כמות ה-1-ים שלא נמחקו.



שלב 2) N בודקת האם t שנבחר מחלק את n .

- אם כן $N \Leftarrow$ מקבלת.
- אם לא $N \Leftarrow$ דוחה.

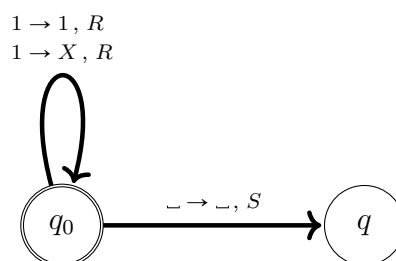
4.2 עץ החישוב של מ"ט א"ד

הגדרה 4.5 עץ החישוב של מ"ט א"ד

בהינתן מ"ט א"ד M ומילה $w \in \Sigma^*$, עץ החישוב של M ו- w הוא עץ מורש שבו:

- (1) כל קדקוד בעץ מתאר קונפיגורציה בחישוב של M על w .
- (2) שורש העץ מתאר את הקונפיגורציה ההתחלתית $q_0 w$.
- (3) לכל קדקוד v בעץ הבנים של v הם כל הקדקודים הנובעים מהקונפיגורציה המתוארת ע"י v .

דוגמה 4.2





4.3 שקילות בין מ"ט א"ד למ"ט דטרמיניסטית

משפט 4.1 שקילות בין מ"ט א"ד למ"ט דטרמיניסטית ב- RE

לכל מ"ט א"ד N קיימת מ"ט דטרמיניסטית D כך ש-

$$L(N) = L(D) .$$

כלומר לכל $w \in \Sigma^*$:

- אם N מקבלת את $w \Leftarrow D$ תקבל את w .
- אם N לא מקבלת את $w \Leftarrow D$ לא תקבל את w .

הוכחה: בהינתן מ"ט א"ד N נבנה מ"ט דטרמיניסטית D ונוכיח כי

$$L(N) = L(D) .$$

רעיון ההוכחה

בהינתן קלט $w \in \Sigma^*$, D תבצע ריצה של כל החישובים האפשריים של N על w , ואם אחד החישובים מסתיים ב- q_{acc} אזי D תעצור ותקבל.

מכיוון שייטכנו חישובים אינסופיים, לא נוכל לסרוק את עץ החישוב לעומק. במקום זה נסרוק את העץ לרוחב. כלומר, נבדוק את כל החישובים באורך 1, ואחרי זה נבדוק את כל החישובים באורך 2, וכן הלאה. אם אחד החישובים הסתיים ב- q_{acc} , אזי D תעצור ותקבל.

תאור הבניה

מכיוון שלכל $q \in Q$ ולכל $\alpha \in \Gamma$:

$$\Delta(q, \alpha) \subseteq Q \times \Gamma \times \{L, R, S\}.$$

אזי

$$|\Delta(q, \alpha)| \leq |Q| \cdot |\Gamma| \cdot |\{L, R, S\}| = 3|Q| \cdot |\Gamma|.$$

נסמן:

$$C = 3|Q| \cdot |\Gamma|.$$

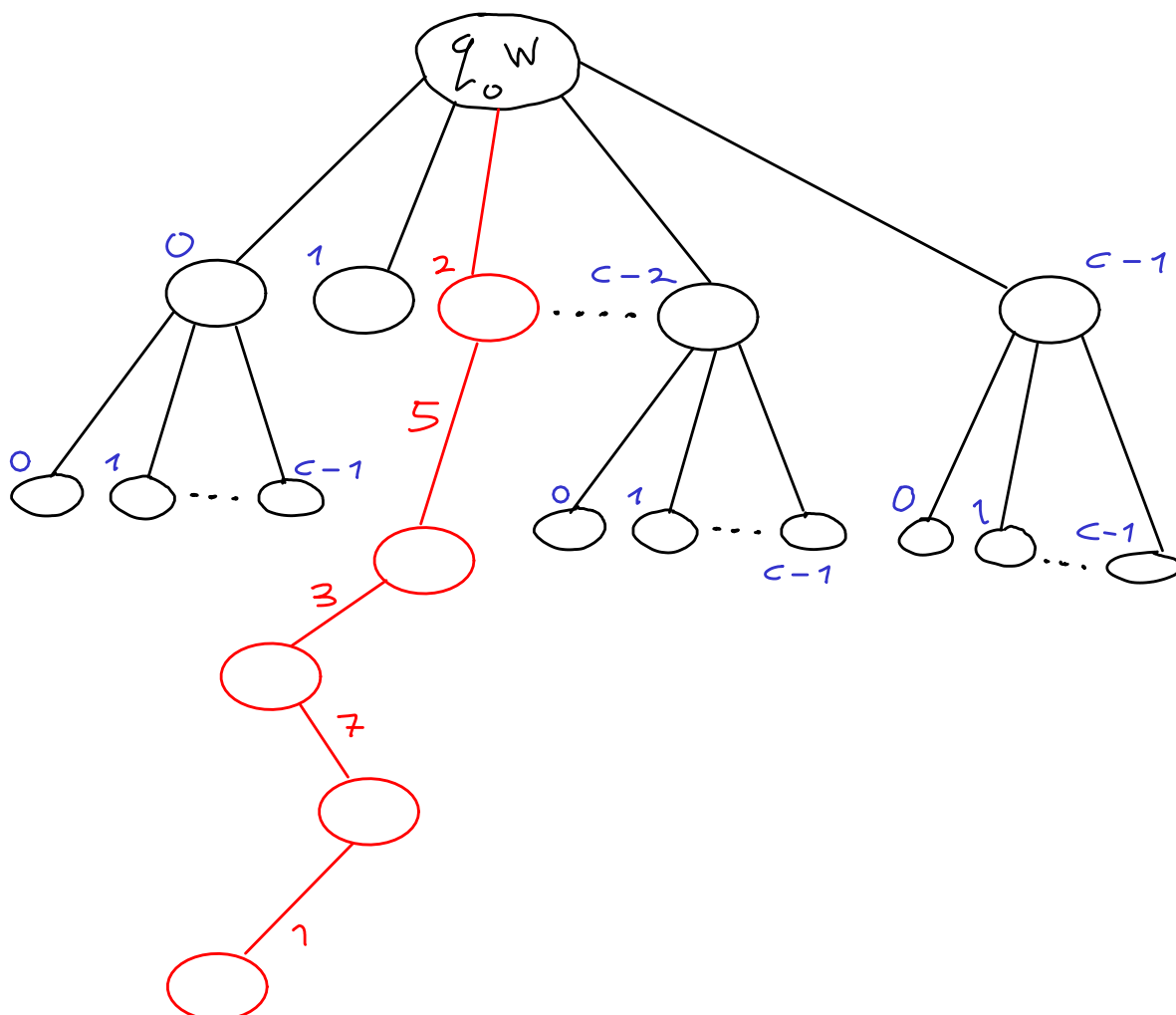
- לכל מצב $q \in Q$ ולכל אות $\alpha \in \Gamma$ נמספר את המעברים ב- $\Delta(q, \alpha)$ שרירותית $\{0, 1, 2, \dots, C-1\}$.



- אם $|\Delta(q, \alpha)| = j < C$, אזי לכל $j \leq k \leq C-1$ נקבע $k = (q_{rej}, \alpha, S)$.



- נשים לב כי שינוי זה לא משנה את השפה של N .



קידום לקסיקוגרפי:

0	00	10	...	$(C-1)0$	000
1	01	11	...	$(C-1)1$	001
2	02	12	...	$(C-1)2$	002
\vdots	\vdots	\vdots	...	\vdots	\vdots
$C-1$	$0(C-1)$	$1(C-1)$...	$(C-1)(C-1)$	$00(C-1)$

הבניה של D

D מכילה 3 סרטים:

	n								
סרט 1	$_$	1	1	1	1	1	1	1	...
	t								
סרט 2	$_$	1	1	1	$_$...			
סרט 3	$_$	1	1	1	$_$...			

$D = "$ על קלט w :

(1) מאתחלת את המחרוזת בסרט 3 ל-0.

(2) מעתיקה את w לסרט 2.

(3) מריצה את N על w לפי המחרוזת בסרט 3.

• אם N קיבלה את $w \Leftarrow D$ עוצרת ומקבלת.

• אחרת, D מוחקת את סרט 2, מקדמת את המחרוזת בסרט 3 לקסיקוגרפית וחוזרת לשלב (2).
“



שיעור 5

תכונות סגירות של R ו- RE 5.1 הגדרה של השפות R ו- RE הגדרה 5.1 R

אוסף השפות הכריעות מסומן R ומוגדר

$$R = \{L \subseteq \Sigma^* : L \text{ מכריעה את } L\}.$$

הגדרה 5.2 RE

אוסף השפות הקבילות מסומן RE ומוגדר

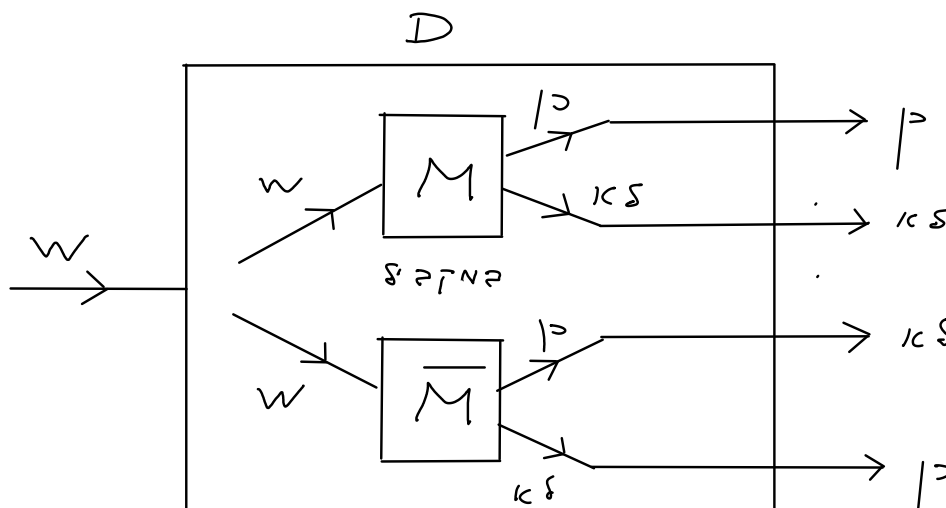
$$RE = \{L \subseteq \Sigma^* : L \text{ מקבלת את } L\}.$$

למה 5.1

אם $L \in RE$ וגם $\bar{L} \in RE$ אזי $L \in R$.

הוכחה: תהי M מ"ט המקבלת את L ותהי \bar{M} מ"ט המקבלת את \bar{L} .

נבנה מ"ט D המכריעה את L .



$D = \text{על קלט } w$

(1) D מעתיקה את w לסרט נוסף.

(2) מריצה במקביל את M על w ואת \bar{M} על העותק של w .

• אם M מקבלת $D \Leftarrow$ מקבלת.

• אם \bar{M} מקבלת $D \Leftarrow$ דוחה.

• אם M דוחה $D \Leftarrow$ דוחה.

• אם \bar{M} דוחה $D \Leftarrow$ מקבלת.

נוכיח כי D מכריעה את L .

אם $w \in L$

$w \in L(M) \Leftarrow$

$\Leftarrow (M \text{ מקבלת את } w) \text{ או } (\bar{M} \text{ דוחה את } w)$

$\Leftarrow D \text{ עוצרת ומקבלת את } w.$

אם $w \notin L$

$w \in \bar{L} \Leftarrow$

$\Leftarrow w \in L(\bar{M})$

$\Leftarrow (\bar{M} \text{ מקבלת את } w) \text{ או } (M \text{ דוחה את } w)$

$\Leftarrow D \text{ עוצרת ודוחה את } w.$



משפט 5.1 סגירות של השפות הכריעות

R סגורה תחת:

(1) איחוד

(2) חיתוך

(3) משלים

(4) שרשור

(5) סגור קליין

משפט 5.2 סגירות של השפות הקבילות

RE סגורה תחת:

(1) איחוד

(2) חיתוך

(3) שרשור

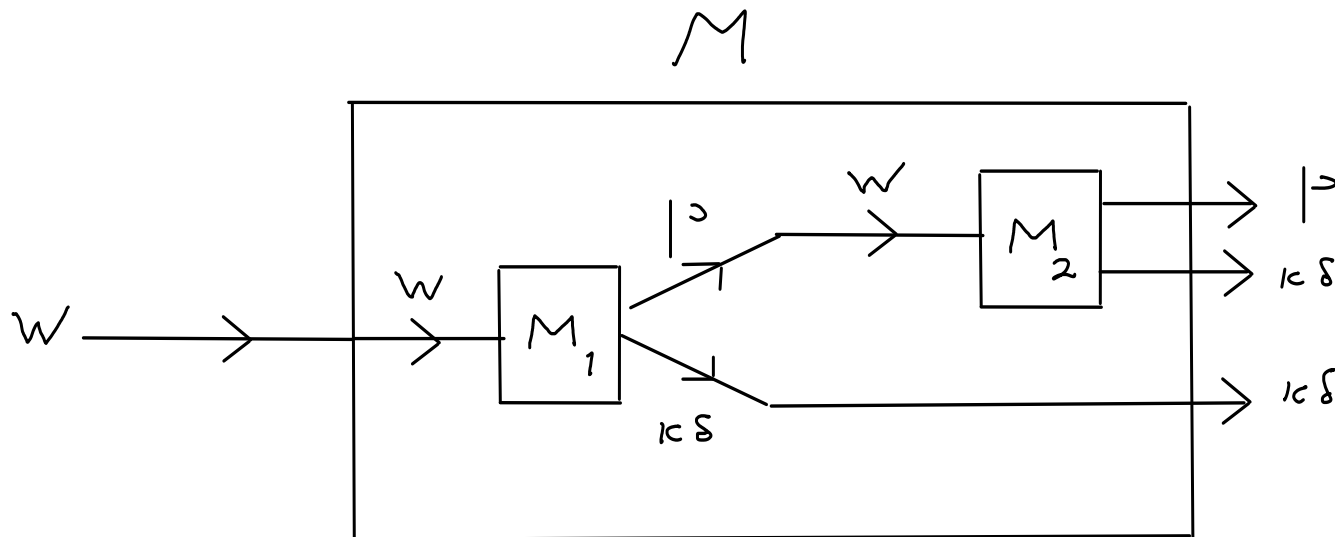
(4) סגור קליין

(1) חיתוך:

(א) סגורה תחת חיתוך

נוכיח כי לכל שתי שפות $L_1, L_2 \in R$ מתקיים $L_1 \cap L_2 \in R$.

תהי M_1 ו- M_2 מ"ט המכריעות את L_1 ו- L_2 בהתאמה. נבנה מ"ט M המכריעה את $L_1 \cap L_2$.

תאור הבנייה

$M =$ על קלט w :

(1) מעתיקה את w לסרט נוסף.

(2) מריצה את M_1 על w .

• אם M_1 דוחה $M \Leftarrow$ דוחה.

• אחרת M מריצה את M_2 על העותק של w ועונה כמוה.

נכונות:

נוכיח כי M מכריעה את $L_1 \cap L_2$.

אם $w \in L_1 \cap L_2$

$w \in L_1$ וגם $w \in L_2 \Leftarrow$

M_1 מקבלת את w וגם M_2 מקבלת את $w \Leftarrow$

M מקבלת את $w \Leftarrow$

אם $w \notin L_1 \cap L_2$

$w \notin L_1$ או $w \notin L_2 \Leftarrow$

M_1 דוחה את w או M_2 דוחה את $w \Leftarrow$

M דוחה את $w \Leftarrow$

RE סגורה תחת חיתוך (ב)

נוכיח כי לכל שתי שפות $L_1, L_2 \in RE$ מתקיים $L_1 \cap L_2 \in RE$.

תהיינה M_1 ו- M_2 שתי מכונות טיורינג המקבלות את L_1 ו- L_2 בהתאמה.

נבנה מ"ט M המקבלת את $L_1 \cap L_2$ באותו אופן כמו (א).

(2) איחוד:

R סגורה תחת איחוד (א)

נוכיח כי לדל שתי שפות $L_1, L_2 \in R$ מתקיים $L_1 \cup L_2 \in R$.

תהיינה M_1 מ"ט המכריעה את L_1 ו- M_2 מ"ט המכריעה את L_2 .

נבנה מ"ט M המכריעה את $L_1 \cup L_2$.

תאור הבנייה

$M = \text{על קלט } w$:

(1) מעתיקה את w לסרט נוסף.

(2) מריצה את M_1 על w .

• אם M_1 מקבלת $\Leftarrow M$ מקבלת.

• אחרת, M מריצה את M_2 על העותק של w ועונה כמוה.

RE סגורה תחת איחוד (ב)

נוכיח כי לכל שתי שפות $L_1, L_2 \in RE$ מתקיים $L_1 \cup L_2 \in RE$.

תהיינה M_1 מ"ט המקבלת את L_1 ו- M_2 מ"ט המקבלת את L_2 .

נבנה מ"ט א"ד M המקבלת את $L_1 \cup L_2$.

תאור הבנייה

$M = \text{על קלט } w$:

(1) M בוחרת באופן א"ד $i \in \{1, 2\}$.

(2) M מריצה את M_i על w ועונה כמוה.

(3) שרשור:

R סגורה תחת שרשור (א)

נוכיח כי לכל שתי שפות $L_1, L_2 \in R$ מתקיים $L_1 \cdot L_2 \in R$ כאשר

$$L_1 \cdot L_2 = \{w = w_1w_2 \mid w_1 \in L_1 \wedge w_2 \in L_2\}.$$

תהיינה M_1 מ"ט המכריעה את L_1 ו- M_2 מ"ט המכריעה את L_2 .

נבנה מ"ט א"ד M המכריעה את $L_1 \cdot L_2$.

תאור הבנייה

$M = \text{על קלט } w$:

(1) M בוחרת באופן א"ד חלוקה של w ל- $w = w_1 w_2$.

(2) M מריצה את M_1 על w_1 .

• אם M_1 דוחה $\Leftarrow M$ דוחה.

• אחרת, M מריצה את M_2 על w_2 ועונה כמוה.

(ב) RE סגורה תחת שרשור

RE סגורה תחת שרשור באותו אופן כמו ב- (א)

(4) * קליני

(א) R סגורה תחת * קליני

נוכיח כי לכל שפה L :

$$L \in R \Rightarrow L^* R$$

כאשר

$$L^* = \{w = w_1 w_2 \cdots w_k \mid \forall 1 \leq i \leq k, w_i \in L\}.$$

תהי M מ"ט המכריעה את L .

נבנה מ"ט M^* א"ד המכריעה את L^* .

תאור הבנייה

$M^* =$ על קלט w :

(1) אם $w = \varepsilon$ אז M^* מקבלת.

(2) אחרת M^* בוחרת באופן א"ד חלוקה של w ל- $w = w_1 \cdots w_k$.

(3) לכל $1 \leq i \leq k$:

M^* מריצה את M על w_i .

• אם M דוחה את w_i אז M^* דוחה.

• אחרת חוזרים לשלב (3).

(4) אם M קיבלה את כל המחרוזות $\{w_i\}$ אזי M^* מקבלת.

(ב) RE סגורה תחת * קליני

(5) משלים

(א) R סגורה תחת המשלים

נוכיח כי

$$L \in R \Rightarrow \bar{L} \in R,$$

כאשר

$$\bar{L} = \{w \in \Sigma^* \mid w \notin L\}.$$

תהי M מ"ט המכריעה את L .

נבנה מ"ט \bar{M} המכריעה את \bar{L} .

$\bar{M} =$ על קלט w :

(1) \bar{M} מריצה את M על w .

• אם M מקבלת $\bar{M} \Leftarrow$ דוחה.

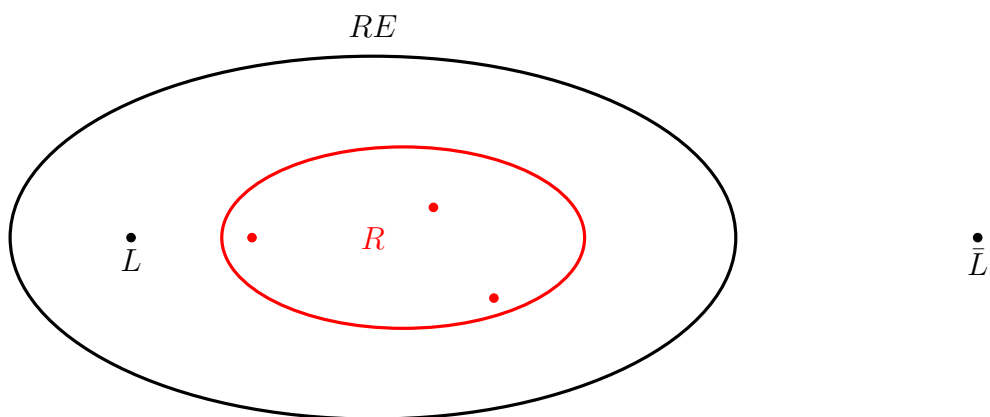
• אם M דוחה $\bar{M} \Leftarrow$ מקבלת.

(ב) RE אינה סגורה תחת המשלים

■

משפט 5.3 RE אינה סגורה תחת המשלים

$$L \in RE \setminus R \Rightarrow \bar{L} \notin RE.$$



הוכחה:

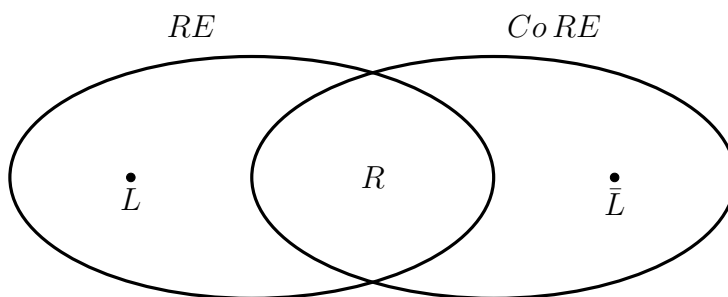
נניח כי $L \in RE \setminus R$ ונניח בשלילה כי $\bar{L} \in RE$.

אזי לפי טענת עזר (למה 5.1), $L \in R$ וזו סתירה.

■

הגדרה 5.3 $CoRE$

$$CoRE = \{L \subseteq \Sigma^* \mid \bar{L} \in RE\}.$$



אבחנה

לפי למה 5.1:

$$RE \cap CoRE = R.$$

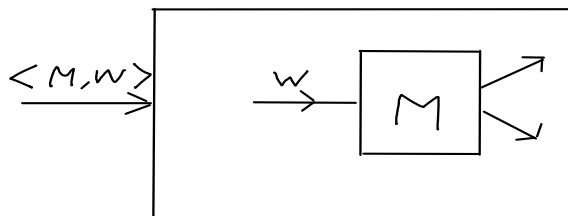
5.2 קידוד של מ"ט דטרמיניסטית

הגדרה 5.4 קידוד של מ"ט

בהינתן קבוצה O של עצמים מופשטים (למשל מכונת טיורינג, תוכנית מחשב, גרף). הקידוד של O , מסומן $\langle O \rangle$, הוא מיפוי של O אל מחרוזת מעל אלפבית סופי שיש בו לפחות שני סימנים.

במידה ויש רב עצמים O_1, \dots, O_k נסמן את הקידוד שלהם $\langle O_1, O_2, \dots, O_k \rangle$.

5.3 מ"ט אוניברסלית U



מ"ט אוניברסלית U מקבלת כקלט זוג, קידוד של מ"ט $\langle M \rangle$ וקידוד של מילה $\langle w \rangle$, ומבצעת סימוציה של ריצה של M על w ועונה בהתאם.

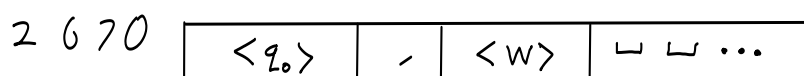
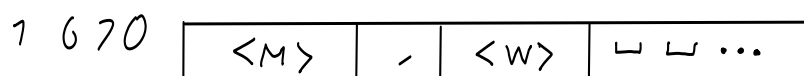
תאור הפעולה של U

$U = \text{על קלט } x$:

(1) בודקת האם x הוא קידוד של מ"ט $\langle M \rangle$ וקידוד של מילה $\langle w \rangle$.

• אם לא \Leftarrow דוחה.

(2) מבצעת סימולציה של M על w :



- רושמת את הקונפיגורציה ההתחלתית $q_0 w$ על סרט 2.
- מחשבת את הקונפיגורציה הבאה בעזרת טבלת המעברים.
- בסוף כל מעבר בין שתי קונפיגורציות, U בודקת האם המצב הנוכחי הוא q_{acc} .
- אם כן U עוצרת ומקבלת.

- * אחרת U בודקת האם המצב הוא q_{rej} .
- * אם כן U עוצרת ודוחה.
- * אחרת U ממשיכה לקונפיגורציה הבאה.

מהי השפה של U ?

לכל x :

(1) אם $U \Leftarrow x \neq \langle M, w \rangle$ דוחה את x .

(2) אם $x = \langle M, w \rangle$:

- אם M מקבלת $w \Leftarrow U$ מקבלת את x .
- אם M דוחה את $w \Leftarrow U$ דוחה את x .
- אם M לא עוצרת על $w \Leftarrow U$ לא עוצרת על x .

$$L(U) = \{ \langle M, w \rangle \mid w \in L(M) \} .$$

הגדרה 5.5 L_{acc}

$$L_{acc} = \{ \langle M, w \rangle \mid w \in L(M) \} \in RE \setminus R$$

הגדרה 5.6 L_{halt}

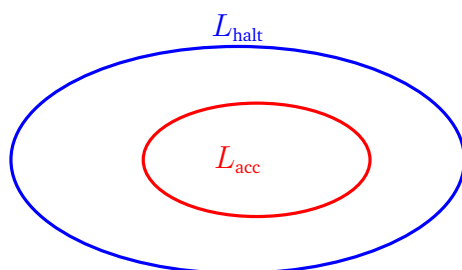
$$L_{halt} = \{ \langle M, w \rangle \mid M \text{ עוצרת על } w \} \in RE \setminus R$$

הגדרה 5.7 L_d

$$L_d = \{ \langle M \rangle \mid \langle M \rangle \notin L(M) \} \notin RE$$

אבחנה:

$$L_{acc} \subseteq L_{halt} .$$



משפט 5.4

$$L_{\text{acc}} \in RE.$$

■

הוכחה: מכיוון ש- $L(U) = L_{\text{acc}}$, U מקבלת את L_{acc} ולכן $L_{\text{acc}} \in RE$.

משפט 5.5

$$L_{\text{halt}} \in RE.$$

הוכחה: נבנה מ"ט U' שהיא למעשה U פרט למקום שבו U עצרה ודחתה, U' תעצור ותקבל.

נוכיח כי U' מקבלת את L_{halt} :

אם $x \in L_{\text{halt}}$

$x = \langle M, w \rangle \Leftarrow M$ עוצרת על w

U' עוצרת ומקבלת את x .

אם $x \notin L_{\text{halt}}$ שני מקרים:

• $x = \langle M, w \rangle \Leftarrow U'$ דוחה את x .

• $x = \langle M, w \rangle \Leftarrow M$ לא עוצרת על w $U' \Leftarrow U'$ לא עוצרת על x .

■

שיעור 6

אי-כריעות

6.1 השפות L_d, L_{halt}, L_{acc} לא כריעות

הגדרה 6.1 L_{acc}

$$L_{acc} = \{ \langle M, w \rangle \mid w \in L(M) \} \in RE \setminus R$$

הגדרה 6.2 L_{halt}

$$L_{halt} = \{ \langle M, w \rangle \mid M \text{ עוצרת על } w \} \in RE \setminus R$$

הגדרה 6.3 L_d

$$L_d = \{ \langle M \rangle \mid \langle M \rangle \notin L(M) \} \notin RE$$

משפט 6.1 $L_{acc} \in RE$

$$L_{acc} \in RE.$$

הוכחה: מכיוון ש- $L(U) = L_{acc}$, כאשר U המכונת טיורינג האוניברסלית אשר מקבלת את L_{acc} , לכן $L_{acc} \in RE$. ■

משפט 6.2 $L_{halt} \in RE$

$$L_{halt} \in RE.$$

הוכחה: נבנה מ"ט U' שהיא למעשה U פרט למקום שבו U עצרה ודחתה, U' תעצור ותקבל.

נוכיח כי U' מקבלת את L_{halt} :

אם $x \in L_{halt}$

$\Leftarrow x = \langle M, w \rangle$ ו- M עוצרת על w

$\Leftarrow U'$ עוצרת ומקבלת את x .

אם $x \notin L_{\text{halt}} \Leftarrow$ שני מקרים:

• $x \neq \langle M, w \rangle \Leftarrow U'$ דוחה את x .

• $x = \langle M, w \rangle \Leftarrow U'$ לא עוצרת על w ו- M לא עוצרת על x .

משפט 6.3 $L_d \notin RE$

$$L_d \notin RE.$$

הוכחה:

נניח בשלילה כי $L_d \in RE$.

$\Leftarrow \exists$ מ"ט M_d המקבלת את L_d .

$\Leftarrow L(M_d) = L_d$.

נבדוק ריצה של M_d על $\langle M_d \rangle$:

• אם $\langle M_d \rangle \in L(M_d) \Leftarrow \langle M_d \rangle \notin L_d \Leftarrow L(M_d) \neq L_d$.

• אם $\langle M_d \rangle \notin L(M_d) \Leftarrow \langle M_d \rangle \in L_d \Leftarrow L(M_d) \neq L_d$.

בשני המקרים קיבלנו סתירה לכך ש- $L(M_d) = L_d$ ולכן $L_d \notin RE$.

משפט 6.4 L_{acc} לא כריעה

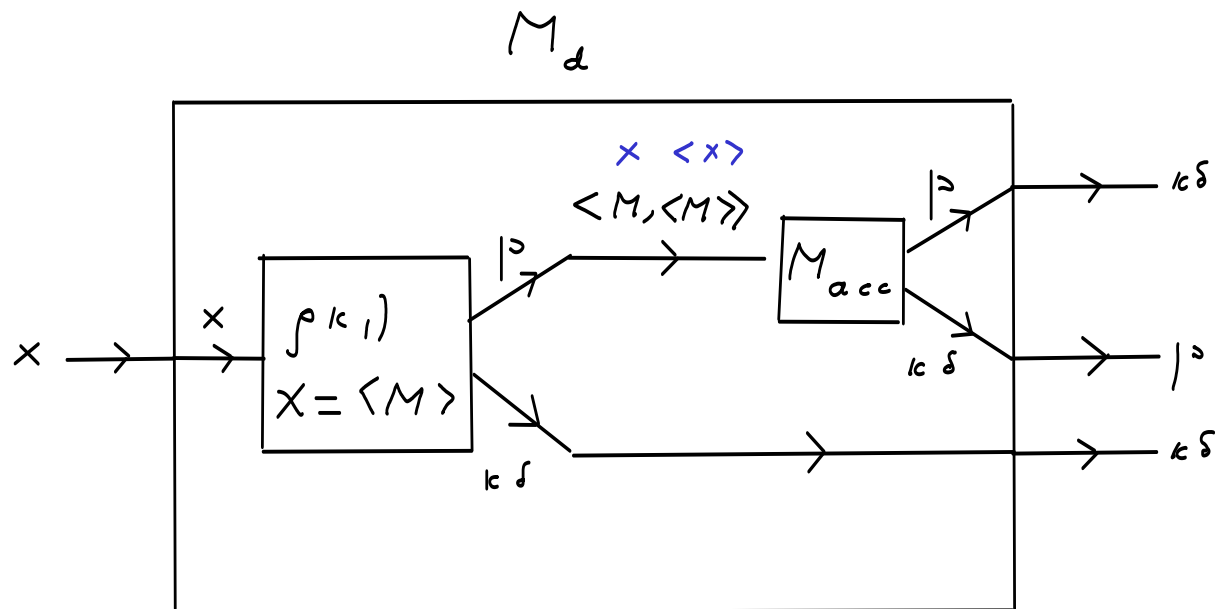
$$L_{\text{acc}} = \{ \langle M, w \rangle \mid w \in L(M) \} \notin R.$$

הוכחה:

נניח בשלילה כי $L_{\text{acc}} \in R$ ותהי M_{acc} המכריעה את L_{acc} .

נשתמש ב- M_{acc} כדי לבנות מ"ט M_d המכריעה את L_d (בסתירה לכך ש- $L_d \notin RE$ כפי שהוכחנו במשפט 6.3).

$$L_d = \{ \langle M, w \rangle \mid \langle M \rangle \notin L(M) \}.$$



התאור של M_d

$M_d =$ על קלט x :

(1) בודקת האם $x = \langle M \rangle$. אם לא \Leftarrow דוחה.

(2) מחשבת את $\langle x \rangle = \langle \langle M \rangle \rangle$.

(3) מריצה את M_{acc} על הזוג $\langle M, \langle M \rangle \rangle$:

• אם M_{acc} מקבלת $\Leftarrow M_d$ דוחה.

• אם M_{acc} דוחה $\Leftarrow M_d$ מקבלת.

כעת נוכיח כי M_d מכריעה את L_d :

אם $x \in L_d$

$\Leftarrow x = \langle M \rangle$ ו- $\langle M \rangle \notin L(M)$

$\Leftarrow M_{acc}$ דוחה את הזוג $\langle M, \langle M \rangle \rangle$

$\Leftarrow M_d$ מקבלת את x .

אם $x \notin L_d$ שני מקרים:

מקרה (1): $x \neq \langle M \rangle$ $\Leftarrow M_d$ דוחה את x .

מקרה (2): $x = \langle M \rangle$ ו- $\langle M \rangle \in L(M)$

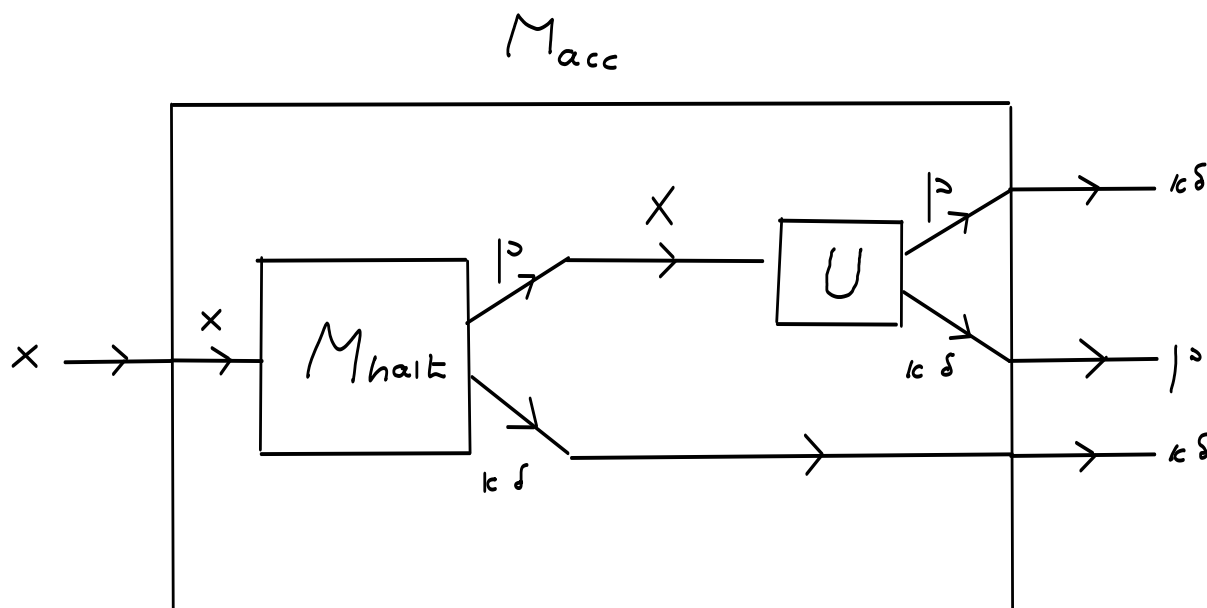
$\Leftarrow M_{acc}$ מקבלת את זוג $\langle M, \langle M \rangle \rangle$

$\Leftarrow M_d$ דוחה את x .

משפט 6.5 L_{halt} לא כריעה

$$L_{\text{halt}} = \{ \langle M, w \rangle \mid M \text{ עוצרת על } w \} \notin R.$$

הוכחה:

נניח בשלילה כי $L_{\text{halt}} \in R$ ותהי M_{halt} מ"ט המכריעה את L_{halt} .נשתמש ב- M_{halt} כדי לבנות מ"ט M_{acc} המכריעה את L_{acc} (בסתירה לכך ש- $L_{\text{acc}} \notin R$ כפי שהוכחנו במשפט 6.4).התאור של M_{acc} M_{acc} = על קלט x :(1) מריצה את M_{acc} על x .

- אם M_{halt} דוחה $\Leftarrow M_{\text{acc}}$ דוחה.
- אם M_{halt} מקבלת $\Leftarrow M_{\text{acc}}$ מריצה את U על x ועונה כמוה.

אבחנהנוכיח כי M_{acc} מכריעה את L_{acc} :אם $x \in L_{\text{acc}}$ $\Leftarrow x = \langle M, w \rangle$ ו- $\langle w \rangle \in L(M)$ $\Leftarrow M_{\text{halt}}$ מקבלת את x וגם U מקבלת את x $\Leftarrow M_{\text{acc}}$ מקבלת את x .

אם $x \notin L_{acc} \Leftarrow$ שני מקרים:

מקרה (1): $x \neq \langle M, w \rangle$

M_{halt} דוחה את $x \Leftarrow$

M_{acc} דוחה את $x \Leftarrow$

מקרה (2): $x = \langle M, w \rangle$ ו- $\langle w \rangle \notin L(M) \Leftarrow$ שני מקרים:

מקרה (א): M לא עוצרת על $w \Leftarrow M_{halt}$ דוחה את $x \Leftarrow M_{acc}$ דוחה את x .

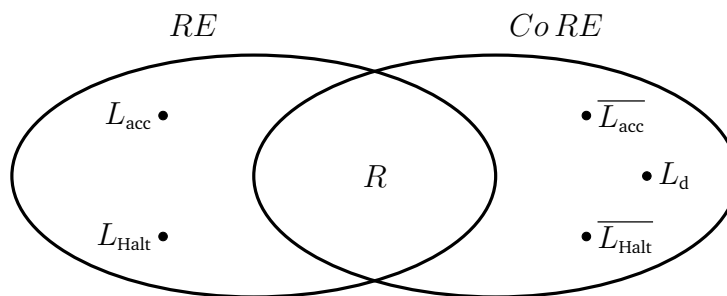
מקרה (ב): M דוחה את $w \Leftarrow M_{halt}$ מקבלת את x אבל U דוחה את $x \Leftarrow M_{acc}$ דוחה את x .

הראנו כי M_{acc} מכריעה את L_{acc} בסתירה לכך ש- $L_{acc} \notin R$.

לכן $L_{halt} \notin R$.

משפט 6.6

$$\begin{aligned} L_{acc} \in RE \setminus R &\Rightarrow \bar{L}_{acc} \notin RE, \\ L_{halt} \in RE \setminus R &\Rightarrow \bar{L}_{halt} \notin RE, \\ L_d &\notin RE \setminus R. \end{aligned}$$



6.2 השפה L_E לא כריעה

הגדרה 6.4 השפה L_E

$$L_E = \{ \langle M \rangle \mid L(M) = \emptyset \}.$$

משפט 6.7 $L_E \notin R$

$$L_E \notin R.$$

כלומר L_E לא כריעה.

הוכחה:

נניח בשלילה כי L_E כריעה. אז נבנה מ"ט M_{acc} המכריעה את L_{acc} באופן הבא.

בנייה של M_w

ראשית נגדיר את המ"ט M_w :

$$M_w = \text{על כל קלט } x:$$

(1) אם $x \neq w \Leftarrow$ דוחה.

(2) אם $x = w$ אז מריצה M על w ועונה כמוה.

אבחנה

אם $x = w$ ו- M מקבלת את w אז $L(M_w) = \Sigma^*$.

אם $x \neq w$ או אם $x = w$ ו- M דוחה את w אז $L(M_w) = \emptyset$.

בנייה של M_{acc}

נניח כי קיימת מ"ט M_E המכריעה את L_E . אז נבנה מ"ט M_{acc} המכריעה את L_{acc} :

$$M_{acc} = \text{על כל קלט } x:$$

(1) אם $\langle M, w \rangle \neq x \Leftarrow$ דוחה.

(2) אם $x = \langle M, w \rangle$, בעזרת התאור $\langle M, w \rangle$, בונה מ"ט M_w .

(3) מריצה M_E על $\langle M_w \rangle$:

(4) • אם M_E מקבלת \Leftarrow דוחה.

• אם M_E דוחה \Leftarrow מקבלת.

נכונות

אם $x \in L_{acc} \Leftarrow x = \langle M, w \rangle \Leftarrow x = \langle M, w \rangle \Leftarrow L(M_w) = \Sigma^* \neq \emptyset \Leftarrow M_E$ דוחה $\langle M_w \rangle \Leftarrow M_{acc}$ מקבלת.

אם $x \notin L_{acc} \Leftarrow$ שני מקרים:

מקרה 1: $x \neq \langle M, w \rangle \Leftarrow L(M_w) = \emptyset \Leftarrow M_E$ מקבלת $\langle M_w \rangle \Leftarrow M_{acc}$ דוחה.

מקרה 2: $x = \langle M, w \rangle \Leftarrow w \notin L(M) \Leftarrow L(M_w) = \emptyset \Leftarrow M_E$ מקבלת $\langle M_w \rangle \Leftarrow M_{acc}$ דוחה.

לסיכום:

אם L_E כריעה אז אפשר לבנות מ"ט M_{acc} המכריעה את L_{acc} בסתירה לכך ש- $L_{acc} \notin R$.
לכן $L_E \notin R$.

משפט 6.8 $L_E \notin RE$

$$L_E \notin RE$$

הוכחה:
הרעיון

נבנה מ"ט א"ד N המקבלת את

$$\bar{L}_E = \{\langle M \rangle \mid L(M) \neq \emptyset\}$$

$x = N$ על קלט x : \square

(1) אם $x \neq \langle M \rangle$ דוחה.

(2) אם $x = \langle M \rangle$ אז N בוחרת מילה $w \in \Sigma^*$ באופן א"ד.

(3) מריצה M על w .

• אם M מקבלת $N \Leftarrow$ מקבלת.

• אם M דוחה $N \Leftarrow$ דוחה.

הוכחת הנכונות

אם $x \in \bar{L}_E$

$x = \langle M \rangle$ ו- $L(M) \neq \emptyset \Leftarrow$

\Leftarrow קיימת מילה $w \in \Sigma^*$ כך ש- $w \in L(M)$

$\Leftarrow \exists$ ניחוש $w \in \Sigma^*$ כך ש M מקבלת את w

\Leftarrow קיים חישוב של N המקל את $\langle M \rangle$ $x = \langle M \rangle$

$\Leftarrow x \in L(N)$

לכן קיימת מ"ט א"ד N המקבלת את השפה \bar{L}_E לכן $\bar{L}_E \in RE$.

כעת נוכיח כי $L_E \notin RE$.

נניח בשלילה כי $L_E \in RE$. הוכחנו למעלה ש- $\bar{L}_E \in RE$. לכן לפי משפט 5.1, $L_E \in R$.

זו בסתירה לכך ש- $L_E \notin R$.

לכן $L_E \notin RE$.

■

6.3 השפה L_{EQ} לא כריעה

הגדרה 6.5 L_{EQ}

$$L_{EQ} = \{\langle M_1, M_2 \rangle \mid L(M_1) = L(M_2)\}$$

משפט 6.9 $L_{EQ} \notin R$

$$L_{EQ} \notin R$$

השפה L_{EQ} לא כריעה.

הוכחה:

נניח בשלילה כי L_{EQ} כריעה. תהי M_{EQ} מ"ט המכריעה את L_{EQ} . אז נבנה מ"ט M_E המכריעה את L_E באופן הבא.

בנייה של M_E

$M_E = \text{על כל קלט } x$:

(1) אם $x \neq \langle M \rangle \Leftarrow$ דוחה.

(2) אם $x = \langle M \rangle$, מריצה M_{EQ} על $\langle M, M_\emptyset \rangle$ כאשר M_\emptyset המ"ט שדוחה כל קלט.

(3) • אם M_{EQ} מקבלת \Leftarrow מקבלת.

• אם M_{EQ} דוחה \Leftarrow דוחה.

נכונות

אם $x \in L_E$

$x = \langle M \rangle$ ו- $L(M) = \emptyset \Leftarrow$

$L(M) = L(M_\emptyset) \Leftarrow$

$\langle M, M_\emptyset \rangle \in L_{EQ} \Leftarrow$

M_{EQ} מקבלת $\langle M, M_\emptyset \rangle \Leftarrow$

M_E מקבל. \Leftarrow

אם $x \notin L_E$ שני מקרים:

מקרה 1: $x \neq \langle M \rangle \Leftarrow M_E$ דוחה.

מקרה 2: $x = \langle M \rangle$ ו- $L(M) \neq \emptyset \Leftarrow$

$L(M) \neq L(M_\emptyset) \Leftarrow$

$\langle M, M_\emptyset \rangle \notin L_{EQ} \Leftarrow$

M_{EQ} דוחה $\langle M, M_\emptyset \rangle \Leftarrow$

M_E דוחה. \Leftarrow

לסיכום:

אם L_{EQ} כריעה אז אפשר לבנות מ"ט M_E המכריעה את L_E בסתירה למשפט 6.7 האומר ש- $L_E \notin R$.
לכן $L_{EQ} \notin R$.

משפט 6.10 $L_{EQ} \notin RE$

$L_{EQ} \notin RE$

L_{EQ} לא קבילה.

הוכחה:

נניח בשלילה כי L_{EQ} קבילה. תהי M_{EQ} מ"ט המקבלת את L_{EQ} . אז נבנה מ"ט M_E המקבלת את L_E באופן הבא.

בנייה של M_E

$$M_E = \text{על כל קלט } x:$$

(1) אם $\langle M \rangle \neq x \Leftarrow$ דוחה.

(2) אם $x = \langle M \rangle$, מריצה M_{EQ} על $\langle M, M_\emptyset \rangle$ כאשר M_\emptyset המ"ט שדוחה כל קלט.

(3) • אם M_{EQ} מקבלת \Leftarrow מקבלת.

נכונות

אם $x \in L_E$

$$\Leftarrow \langle M \rangle = x \text{ ו- } L(M) = \emptyset$$

$$\Leftarrow L(M) = L(M_\emptyset)$$

$$\Leftarrow \langle M, M_\emptyset \rangle \in L_{EQ}$$

$$\Leftarrow M_{EQ} \text{ מקבלת } \langle M, M_\emptyset \rangle$$

$$\Leftarrow M_E \text{ מקבל.}$$

לסיכום:

אם L_{EQ} קבילה אז אפשר לבנות מ"ט M_E המקבלת את L_E בסתירה למשפט 6.8 האומר ש- $L_E \notin RE$.
לכן $L_{EQ} \notin RE$.

משפט 6.11 $\bar{L}_{EQ} \notin RE$

$$\bar{L}_{EQ} \notin RE.$$

הוכחה:

נניח בשלילה כי \bar{L}_{EQ} קבילה. תהי M_{EQ} מ"ט המקבלת את \bar{L}_{EQ} . אז נבנה מ"ט M_{acc} המקבלת את \bar{L}_{acc} באופן הבא.

בנייה של M_1

ראשית נגדיר מ"ט M_1 באופן הבא:

$$M_1 = \text{על קלט } x:$$

(1) מריצה M על w ועונה כמוה.

בנייה של M_{acc}

$$M_{acc} = \text{על כל קלט } x:$$

(1) אם $\langle M, w \rangle \neq x \Leftarrow$ מקבלת.

(2) אם $x = \langle M, w \rangle$ אז בונה M_1 .

(3) מריצה $M_{\overline{EQ}}$ על $\langle M_1, M^* \rangle$ כאשר M^* המ"ט שמקבלת כל קלט.

(4) • אם $M_{\overline{EQ}}$ מקבלת \Leftarrow מקבלת.

נכונות

אם $x \in L_{\overline{acc}}$

$\Leftarrow M$ לא מקבלת w

$\Leftarrow L(M_1) = \emptyset$

$\Leftarrow \langle M_1, M^* \rangle \in L_{\overline{EQ}}$

$\Leftarrow M_{\overline{EQ}}$ מקבלת $\langle M_1, M^* \rangle$

$\Leftarrow M_{\overline{acc}}$ מקבל.

לסיכום:

אם $L_{\overline{EQ}}$ קבילה אז אפשר לבנות מ"ט $M_{\overline{acc}}$ המקבלת את $L_{\overline{acc}}$ בסתירה למשפט 6.6 האומר ש- $L_{\overline{acc}} \notin RE$.
לכן $L_{\overline{EQ}} \notin RE$.



6.4 סיכום: כריעות וקבילות של שפות

קבילה	כריעה	
✓	×	$L_{\overline{acc}}$
×	×	$\overline{L_{\overline{acc}}}$
×	×	L_d
✓	×	L_{Halt}
×	×	$\overline{L_{\text{Halt}}}$
×	×	L_E
✓	×	$\overline{L_E}$
×	×	L_{EQ}
×	×	$\overline{L_{\text{EQ}}}$
×	×	L_{REG}
×	×	L_{NOTREG}

שיעור 7

רדוקציה

7.1 טבלה של רדוקציות

טבלה של רדוקציות

רדוקציה	עמוד
$L_{\text{HALT}} \leq L_{\text{acc}}$	דוגמה 7.6 עמוד 72
$\bar{L}_{\text{acc}} \leq L_{\text{NOTREG}}$	דוגמה 7.11 עמוד 76
$L_{\text{acc}} \leq L_{\text{NOTREG}}$	דוגמה 7.12 עמוד 77
$L_{\text{HALT}} \leq L_{\text{NOTREG}}$	דוגמה 7.13 עמוד 78
$L_{\text{acc}} \leq L_{\text{REG}}$	דוגמה 7.15 עמוד 80
$\bar{L}_{\text{acc}} \leq L_{\text{REG}}$	דוגמה 7.14 עמוד 79
$\bar{L}_{\text{acc}} \leq L_{M_1 \neg M_2}$ כאשר $L_{M_1 \neg M_2} = \{ \langle M_1, M_2, w \rangle \mid w \in L(M_1) \wedge w \notin L(M_2) \}$	דוגמה 7.16 עמוד 81
$\bar{L}_{\text{acc}} \leq L_{M_1 \subset M_2}$ כאשר $L_{M_1 \subset M_2} = \{ \langle M_1, M_2 \rangle \mid L(M_1) \subset L(M_2) \}$	דוגמה 7.17 עמוד 81

7.2 מ"ט המחשבת את פונקציה

הגדרה 7.1 מ"ט המחשבת פונקציה

בהינתן פונקציה $f : \Sigma^* \rightarrow \Sigma^*$ אומרים כי מ"ט M מחשבת את f אם לכל $x \in \Sigma^*$:

- M מגיעה ל- q_{acc} בסוף החישוב של $f(x)$ וגם
- על סרט הפלט של M רשום $f(x)$.

הערה 7.1

מ"ט שמחשבת פונקציה עוצרת תמיד.

הגדרה 7.2 מ"ט המחשבת פונקציה

בהינתן פונקציה $f : \Sigma^* \rightarrow \Sigma^*$ אומרים כי f חשיבה אם קיימת מ"ט המחשבת את f .

דוגמה 7.1

$$f_1(x) = xx. \quad (7.1)$$

$f_1(x)$ חשיבה.

דוגמה 7.2

$$f_2(x) = \begin{cases} x & |x| \text{ זוגי} \\ xx & |x| \text{ אי-זוגי} \end{cases}. \quad (7.2)$$

$f_2(x)$ חשיבה.

דוגמה 7.3

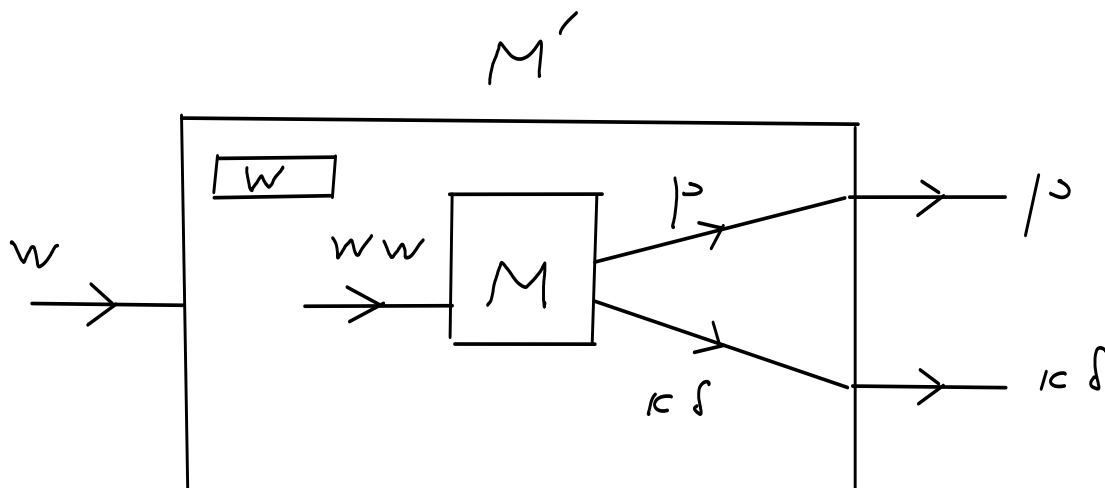
$$f_3(x) = \begin{cases} \langle M' \rangle & x = \langle M \rangle \\ \langle M^* \rangle & x \neq \langle M \rangle \end{cases}. \quad (7.3)$$

כאשר

• M^* מ"ט שמקבלת כל קלט.

• M' מ"ט המקבלת את השפה

$$L(M') = \{w \in \Sigma^* \mid ww \in L(M)\}.$$



$f_3(x)$ חשיבה כי ניתן לבנות מ"ט שבודקת האם $x = \langle M \rangle$. אם לא, מחזירה קידוד קבוע $\langle M^* \rangle$. ואם כן, מחזירה קידוד $\langle M' \rangle$ ע"י הוספת מעברים המשכפלים את הקלט בתחילת הקידוד $\langle M \rangle$.

דוגמה 7.4

$$f_4(x) = \begin{cases} 1 & x = \langle M \rangle \wedge \langle M \rangle \in L(M) \\ 0 & \text{אחרת} \end{cases} \quad (7.4)$$

$f_4(x)$ לא חשיבה כי ייתכנו קלטים $x = \langle M \rangle$ ו- M לא עוצרת על $\langle M \rangle$.

7.3 רדוקציות

הגדרה 7.3 רדוקציות

בהינתן שתי שפות $L_1, L_2 \subseteq \Sigma^*$ אומרים כי L_1 ניתנת לרדוקציה ל- L_2 , ומסמנים

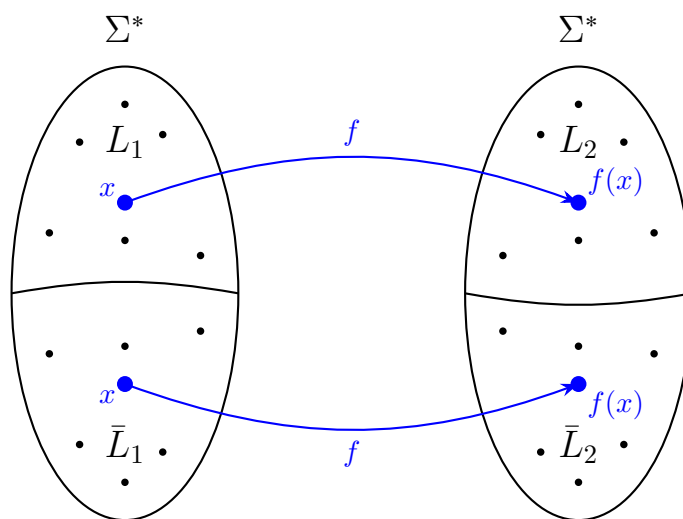
$$L_1 \leq L_2 ,$$

אם \exists פונקציה $f : \Sigma^* \rightarrow \Sigma^*$ המקיימת:

(1) f חשיבה

(2) לכל $x \in \Sigma^*$:

$$x \in L_1 \iff f(x) \in L_2 .$$



דוגמה 7.5

נתונות השפות

$$L_1 = \{x \in \{0,1\}^* \mid |x| \text{ זוגי} \} ,$$

$$L_2 = \{x \in \{0,1\}^* \mid |x| \text{ אי-זוגי} \} .$$

הוכיחו כי

$$L_1 \leq L_2 .$$

פתרון:

נגדיר את הפונקציה

$$f(x) = \begin{cases} 1 & |x| \text{ זוגי} \\ 10 & |x| \text{ אי-זוגי} \end{cases}$$

הוכחת הנכונות:

$$f(x) \in L_2 \text{ אי-זוגי } |f(x)| \Leftarrow f(x) = 1 \Leftarrow |x| \text{ זוגי } \Leftarrow x \in L_1$$

$$f(x) \notin L_2 \text{ זוגי } |f(x)| \Leftarrow f(x) = 10 \Leftarrow |x| \text{ אי-זוגי } \Leftarrow x \notin L_1$$

משפט 7.1 משפט הרדוקציהלכל שתי שפות $L_1, L_2 \subseteq \Sigma^*$, אם קיימת רדוקציה

$$L_1 \leq L_2$$

אזי התנאים הבאים מתקיימים:

$$L_1 \in R \Leftarrow L_2 \in R \quad (1)$$

$$L_1 \in RE \Leftarrow L_2 \in RE \quad (2)$$

$$L_1 \notin R \Rightarrow L_2 \notin R \quad (3)$$

$$L_1 \notin RE \Rightarrow L_2 \notin RE \quad (4)$$

הוכחה: מכיוון ש-

$$L_1 \leq L_2$$

קיימת פונקציה f חשיבה המקיימת:

$$x \in L_1 \Leftrightarrow f(x) \in L_2$$

לכל $x \in \Sigma^*$.תהי M_f מ"ט המחשבת את f .

$$(1) \quad \underline{L_1 \in R \Leftarrow L_2 \in R} \text{ נוכיח}$$

תהי M_2 מ"ט המכריעה את L_2 .נבנה מ"ט M_1 המכריעה את L_1 .התאור של M_1

$$M_1 = \text{על קלט } x:$$

1. מחשבת את $f(x)$ בעזרת M_f .2. מריצה את M_2 על $f(x)$ ועונה כמוה.נוכיח כי M_1 מכריעה את L_1 .

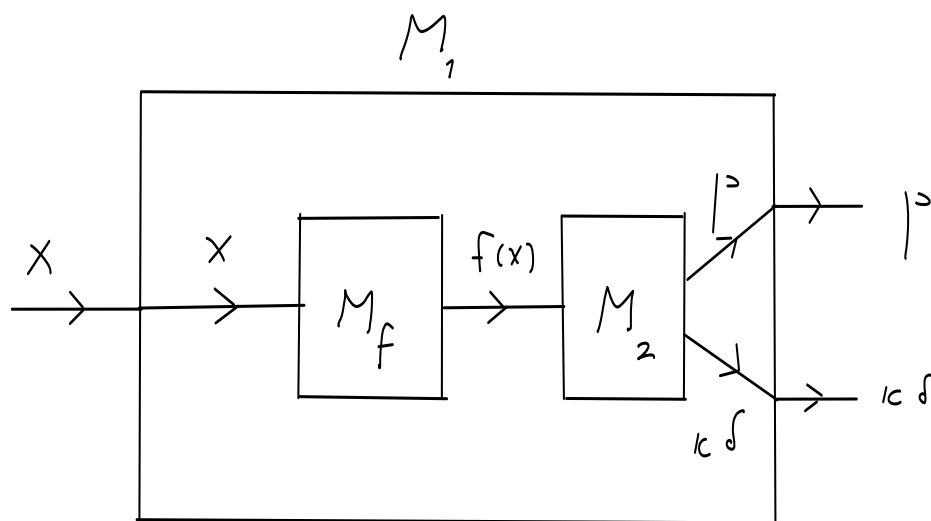
$$\bullet \text{ אם } x \in L_1 \Leftarrow f(x) \in L_2 \Leftarrow M_2 \text{ מקבלת את } f(x) \Leftarrow M_1 \text{ מקבלת את } x.$$

• אם $x \notin L_1 \Leftrightarrow f(x) \notin L_2 \Leftrightarrow M_2$ דוחה את $f(x) \Leftrightarrow M_1$ דוחה את x .

(2) נוכיח $L_1 \in RE \Leftrightarrow L_2 \in RE$

תהי M_2 מ"ט המקבלת את L_2 .

נבנה מ"ט M_1 המקבלת את L_1 .



התאור של M_1

$M_1 =$ על קלט x :

1. מחשבת את $f(x)$ בעזרת M_f .

2. מריצה את M_2 על $f(x)$ ועונה כמוה.

נוכיח כי M_1 מקבלת את L_1 :

• אם $x \in L_1 \Leftrightarrow f(x) \in L_2 \Leftrightarrow M_2$ מקבלת את $f(x) \Leftrightarrow M_1$ מקבלת את x .

• אם $x \notin L_1 \Leftrightarrow f(x) \notin L_2 \Leftrightarrow M_2$ לא מקבלת את $f(x) \Leftrightarrow M_1$ לא מקבלת את x .

(3)

(4)

כלל 7.1

• אם רוצים להוכיח כי שפה כלשהי $L \in RE$, בוחרים שפה אחרת $L' \in RE$ ומראים שקיימת רדוקציה

$$L \leq L'.$$

לדוגמה:

$$L \leq L_{\text{acc}}$$

(כנ"ל לגבי R)

- אם רוצים להוכיח כי שפה כלשהי $L \notin RE$ בוחרים שפה אחרת $L' \notin RE$ ומראים שקיימת רדוקציה

$$L' \leq L.$$

לדוגמה

$$L_d \leq L$$

(כנ"ל לגבי R).

דוגמה 7.6

נתונות השפות $L_{\text{acc}} = \{\langle M, w \rangle \mid w \in L(M)\}$ ו- $L_{\text{halt}} = \{\langle M, w \rangle \mid M \text{ עוצרת על } w\}$.
הוכיחו כי $L_{\text{acc}} \notin R$ ע"י רדוקציה $L_{\text{acc}} \leq L_{\text{halt}}$.

פתרון:

נבנה פונקציה f חשיבה ומקיימת

$$x \in L_{\text{acc}} \iff f(x) \in L_{\text{halt}}.$$

$$M \text{ מקבלת את } w \iff M' \text{ תעצור על } w'.$$

$$M \text{ דוחה את } w \iff M' \text{ לא תעצור על } w'.$$

$$M \text{ לא עוצרת את } w \iff M' \text{ לא תעצור על } w'.$$

$$f(x) = \begin{cases} \langle M', w \rangle & : x = \langle M, w \rangle \\ \langle M_{\text{loop}}, \varepsilon \rangle & : x \neq \langle M, w \rangle \end{cases}$$

כאשר

- M_{loop} מ"ט שלא עוצרת על אף קלט.
- M' מ"ט המתנהגת כמו M פרט למקומות בהם M עצרה ודחתה, M' תיכנס ללולאה אינסופית.

נכונות הרדוקציה

f חשיבה כי ניתן לבנות מ"ט שתבדוק האם $x = \langle M, w \rangle$.

אם לא, תחזיר קידוד קבוע $\langle M_{\text{loop}}, w \rangle$

ואם כן, תחזיר קידוד $\langle M', w \rangle$ ע"י ביצוע שינויים לוקלים בקידוד של M .

$$x \in L_{\text{acc}} \iff f(x) \in L_{\text{halt}} \text{ נוכיח כי}$$

אם $x \in L_{\text{acc}}$

$$w \in L(M) \text{ ו- } x = \langle M, w \rangle \Leftarrow$$

$$w \text{ עוצרת ומקבלת את } M' \text{ ו- } f(x) = \langle M', w \rangle \Leftarrow$$

$$f(x) \in L_{\text{halt}} \Leftarrow$$

אם $x \notin L_{\text{acc}}$ אז שני מקרים:

מקרה 1:

$$f(x) \notin L_{\text{halt}} \Leftarrow \varepsilon \text{ לא עוצרת על } M_{\text{loop}} \text{ ו- } f(x) = \langle M_{\text{loop}}, \varepsilon \rangle \Leftarrow x \neq \langle M, w \rangle$$

מקרה 2:

$$\text{שני מקרים:} \quad \Leftarrow f(x) = \langle M', w \rangle \Leftarrow w \notin L(M) \text{ ו- } x = \langle M, w \rangle$$

$$\text{מקרה א:} \quad M \text{ לא עוצרת על } w \Leftarrow M' \text{ לא עוצרת על } w \Leftarrow f(x) \notin L_{\text{halt}}$$

$$\text{מקרה ב:} \quad M \text{ דוחה את } w \Leftarrow M' \text{ לא עוצרת על } w \Leftarrow f(x) \notin L_{\text{halt}}$$

לסיכום, הוכחנו רדוקציה $L_{\text{acc}} \leq L_{\text{halt}}$. ומכיוון ש- $L_{\text{acc}} \notin R$ (משפט 6.4) אז ממשט הרדוקציה 7.1, מתקיים $L_{\text{halt}} \notin R$.

7.7 דוגמה

נתונה השפה

$$L_{\Sigma^*} = \{ \langle M \rangle \mid L(M) = \Sigma^* \}$$

ונתונה השפה

$$\bar{L}_{\Sigma^*} = \{ \langle M \rangle \mid L(M) \neq \Sigma^* \} \cup \{ x \neq \langle M \rangle \}.$$

הוכיחו כי:

$$\text{א) } L_{\Sigma^*} \notin RE$$

$$\text{ב) } L_{\Sigma^*} \notin R$$

$$\text{ג) } \bar{L}_{\Sigma^*} \notin RE$$

פתרון:

נוכיח כי $L_{\Sigma^*} \notin R$ ע"י רדוקציה

$$L_{\text{acc}} \leq L_{\Sigma^*}.$$

נבנה פונקציה חשיבה f המקיימת

$$x \in L_{\text{acc}} \Leftrightarrow f(x) \in L_{\Sigma^*}.$$

$$L(M') = \Sigma^* \Leftarrow w \in L(M)$$

$$L(M') \neq \Sigma^* \Leftarrow w \notin L(M)$$

$$f(x) = \begin{cases} \langle M' \rangle & : x = \langle M, w \rangle \\ \langle M_{\emptyset} \rangle & : x \neq \langle M, w \rangle \end{cases}$$

- M_\emptyset מ"ט שדוחה כל קלט.
- M' היא מ"ט שעל כל קלט x , מתעלמת מ- x ומריצה את M על w ועונה כמוה.

אבחנה:

$$L(M') = \begin{cases} \Sigma^* & : w \in L(M) \\ \emptyset & : w \notin L(M) \end{cases}$$

נכונות הרדוקציה:

f חשיבה כי ניתן לבנות מ"ט שתבדוק האם $x = \langle M, w \rangle$.

אם לא תחזיר קידוד קבוע $\langle M_\emptyset \rangle$.

אם כן, תחזיר קידוד $\langle M' \rangle$ ע"י הוספת קוג ל- M שמוחק את הקלט מהסרט וכותב w במקומו.

נוכיח כי

$$x \in L_{\text{acc}} \Leftrightarrow f(x) \in L_{\Sigma^*}$$

$$\Leftrightarrow L(M') = \Sigma^* \text{ ולפי האבחנה } f(x) = \langle M' \rangle \Leftrightarrow w \in L(M) \text{ ו- } x = \langle M, w \rangle \Leftrightarrow x \in L_{\text{acc}} \text{ אם } f(x) \in L_{\Sigma^*}$$

$$\text{אם } x \in L_{\text{acc}} \Leftrightarrow \text{שני מקרים:}$$

$$\text{מקרה 1: } f(x) \notin L_{\Sigma^*} \Leftrightarrow L(M_\emptyset) = \emptyset \text{ ו- } f(x) = \langle M_\emptyset \rangle \Leftrightarrow x \neq \langle M, w \rangle$$

$$\text{מקרה 2: } f(x) \notin L_{\Sigma^*} \Leftrightarrow L(M') = \emptyset \text{ ולפי האבחנה } f(x) = \langle M' \rangle \Leftrightarrow w \notin L(M) \text{ ו- } x = \langle M, w \rangle$$

לסיכום, הוכחנו רדוקציה $L_{\text{acc}} \leq L_{\Sigma^*}$. ומכיוון ש- $L_{\text{acc}} \notin R$ (משפט 6.4) אז ממשט הרדוקציה 7.1, מתקיים $L_{\Sigma^*} \notin R$.

7.8 דוגמה

נתונה השפה

$$L_d = \{ \langle M \rangle \mid \langle M \rangle \notin L(M) \}$$

ונתונה השפה

$$\bar{L}_{\text{acc}} = \{ \langle M, w \rangle \mid w \notin L(M) \} \cup \{ x \neq \langle M, w \rangle \} .$$

הוכיחו כי

$$\bar{L}_{\text{acc}} \notin RE \text{ ע"י רדוקציה}$$

$$L_d \leq \bar{L}_{\text{acc}} .$$

פתרון:

נבנה פונקציה חשיבה f המקיימת

$$x \in L_d \Leftrightarrow f(x) \in L_{\text{acc}} .$$

$$w' \notin L(M') \Leftrightarrow \langle M \rangle \notin L(M)$$

$$w' \in L(M') \Leftrightarrow \langle M \rangle \in L(M)$$

$$f(x) = \begin{cases} \langle M, \langle M \rangle \rangle & : x = \langle M \rangle \\ \langle M^*, \varepsilon \rangle & : x \neq \langle M \rangle \end{cases}$$

כאשר M^* המ"ט שמקבלת כל קלט.

נכונות הרדוקציה:

f חשיבה כי ניתן לבנות מ"ט שתבדוק האם $x = \langle M, w \rangle$

אם לא תחזיר קידוד קבוע $\langle M^*, \varepsilon \rangle$.

אם כן, תחשב $\langle M, \langle M \rangle \rangle$.

נוכיח כי

$$\begin{aligned} x \in L_d &\Leftrightarrow f(x) \in \bar{L}_{acc} \\ \Leftrightarrow \langle M \rangle \notin L(M) \text{ ו- } f(x) = \langle M, \langle M \rangle \rangle &\Leftrightarrow \langle M \rangle \notin L(M) \text{ ו- } x = \langle M \rangle \Leftrightarrow \begin{aligned} &x \in L_d \text{ אם } \\ &f(x) \in \bar{L}_{acc} \end{aligned} \end{aligned}$$

אם $x \notin L_d$ שני מקרים:

$$\text{מקרה 1: } f(x) \notin \bar{L}_{acc} \Leftrightarrow \varepsilon \in L(M^*) \text{ ו- } f(x) = \langle M^*, \varepsilon \rangle \Leftrightarrow x \neq \langle M \rangle$$

$$\text{מקרה 2: } f(x) \notin \bar{L}_{acc} \Leftrightarrow \langle M \rangle \in L(M) \text{ ו- } f(x) = \langle M, \langle M \rangle \rangle \Leftrightarrow \langle M \rangle \in L(M) \text{ ו- } x = \langle M \rangle$$

לסיכום, הוכחנו רדוקציה $L_d \leq \bar{L}_{acc}$, ומכיוון ש- $L_d \notin RE$ (משפט 6.3) אז ממשט הרדוקציה 7.1, מתקיים $\bar{L}_{acc} \notin RE$.

משפט 7.2 משפט הרדוקציה בין שפות משלימות

אם קיימת רדוקציה $L_1 \leq L_2$, אזי קיימת רדוקציה $\bar{L}_1 \leq \bar{L}_2$.

הוכחה:

אם \exists רדוקציה

$$L_1 \leq L_2$$

אזי \exists פונקציה חשיבה f המקיימת

$$x \in L_1 \Leftrightarrow f(x) \in L_2$$

ולכן עבור אותה פונקציה f היא גם חשיבה וגם מקיימת

$$x \in \bar{L}_1 \Leftrightarrow f(x) \in \bar{L}_2$$

ולכן

$$\bar{L}_1 \leq \bar{L}_2 .$$

7.4 דוגמאות בשימוש של משפט הרדוקציה בין שפות משלימות (משפט 7.2)

7.9 דוגמה

הוכחנו בדוגמה 7.7 רדוקציה

$$L_{acc} \leq L_{\Sigma^*}.$$

לכן לפי משפט 7.2 קיימת רדוקציה

$$\bar{L}_{acc} \leq \bar{L}_{\Sigma^*}.$$

מכיוון ש- $\bar{L}_{acc} \notin RE$, אזי ממשפט הרדוקציה 7.1 מתקיים $\bar{L}_{\Sigma^*} \notin RE$.

7.10 דוגמה

הוכחנו בדוגמה 7.8 רדוקציה

$$L_d \leq \bar{L}_{acc}.$$

לכן לפי משפט 7.2 קיימת רדוקציה

$$\bar{L}_d \leq L_{acc}.$$

מכיוון ש- $L_{acc} \in RE$, אזי ממשפט הרדוקציה 7.1 מתקיים $\bar{L}_d \in RE$.

7.5 דוגמאות בשימוש של משפט הרדוקציה (משפט 7.1)

7.11 דוגמה

$$\bar{L}_{acc} \leq L_{NOTREG}$$

תהי L_{NOTREG} השפה

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

הוכיחו כי השפה L_{NOTREG} לא כריעה על ידי רדוקציה מ- \bar{L}_{acc} .

פתרון:

השפה \bar{L}_{acc} מוגדרת

$$\bar{L}_{acc} = \{ \langle M, w \rangle \mid w \text{ לא מקבלת } M \} \cup \{ x \neq \langle M, w \rangle \}.$$

והשפה L_{NOTREG} מוגדרת

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

נגדיר הפונקציה הבאה:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ w' \in PAL & x \neq \langle M, w \rangle \end{cases}$$

כאשר M' מ"ט הבאה:

$M' =$ על כל קלט y :

(1) אם $y \in PAL \Leftarrow$ מקבלת.

(2) אחרת מריצה M על w ועונה כמוה.

הוכחת נכונות הרדוקציה

אם $x \in \bar{L}_{acc}$ \Leftarrow שני מקרים:

מקרה 1: $x = \langle M, w \rangle$

$\Leftarrow M$ לא מקבלת w

$\Leftarrow L(M') \in PAL$

$\Leftarrow \langle M' \rangle \in PAL$

$\Leftarrow f(x) \in PAL$

$\Leftarrow f(x) \in L_{NOTREG}$

מקרה 2: $x \neq \langle M, w \rangle$ $\Leftarrow f(x) \in PAL \Leftarrow f(x) \in L_{NOTREG}$

אם $x \notin \bar{L}_{acc}$ $\Leftarrow M$ מקבלת w $\Leftarrow L(M') = \Sigma^*$ $\Leftarrow f(x) \in \Sigma^*$ $\Leftarrow f(x) \in L_{NOTREG}$.

לכן הוכחנו כי $x \in \bar{L}_{acc} \Leftrightarrow f(x) \in NOTERG$, ז"א $f(x)$ היא רדוקציה מ- L_{acc} ל- L_{NOTREG} .

השפה \bar{L}_{acc} לא כריעה. לפיכך, לפי משפט הרדוקציה גם L_{NOTREG} לא כריעה.

7.12 דוגמה $L_{acc} \leq L_{NOTREG}$

תהי L_{NOTREG} השפה

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

הוכיחו כי השפה L_{NOTREG} לא כריעה על ידי רדוקציה מ- L_{acc} .

פתרון:

השפה L_{acc} מוגדרת

$$L_{acc} = \{ \langle M, w \rangle \mid M \text{ מקבלת } w \}.$$

והשפה L_{NOTREG} מוגדרת

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

נגדיר הפונקציה הבאה:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ \langle M_{\emptyset} \rangle & x \neq \langle M, w \rangle \end{cases}$$

כאשר M' מ"ט הבאה:

$M' =$ על כל קלט y :

(1) M' מריצה M על w .

(2) • אם M דוחה \Leftarrow דוחה.

• אם M מקבלת $\Leftarrow M'$ בודקת אם y פלינדרום.

* אם כן \Leftarrow מקבלת.

* אם לא \Leftarrow דוחה.

הוכחת נכונות הרדוקציה

אם $x \in L_{acc}$ $\Leftarrow M$ מקבלת w $\Leftarrow L(M') = PAL$ $\Leftarrow f(x) \in PAL$ $\Leftarrow f(x) \in L_{NOTREG}$.

$x \notin L_{acc}$ \Leftarrow שני מקרים.

מקרה 1: $x \neq \langle M, w \rangle \Leftarrow f(x) = \langle M_\emptyset \rangle$ ו- $L(M_\emptyset) = \emptyset \Leftarrow \langle M_\emptyset \rangle \notin L_{NOTREG}$ $\Leftarrow f(x) \notin L_{NOTREG}$.

מקרה 2: $x = \langle M, w \rangle$ ו- M לא מקבלת w $\Leftarrow L(M') = \emptyset \Leftarrow \langle M' \rangle \notin L_{NOTREG}$ $\Leftarrow f(x) \notin L_{NOTREG}$.

7.13 דוגמה $L_{HALT} \leq L_{NOTREG}$

תהי L_{NOTREG} השפה

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

הוכיחו כי השפה L_{NOTREG} לא כריעה על ידי רדוקציה מ- L_{HALT} .

פתרון:

השפה L_{HALT} מוגדרת

$$L_{HALT} = \{ \langle M, w \rangle \mid M \text{ עוצרת על } w \}.$$

והשפה L_{NOTREG} מוגדרת

$$L_{NOTREG} = \{ \langle M \rangle \mid L(M) \text{ לא רגולרית} \}.$$

נגדיר הפונקציה הבאה:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ \langle M_\emptyset \rangle & x \neq \langle M, w \rangle \end{cases}.$$

כאשר M' מ"ט הבאה:

$M' =$ על כל קלט y :

(1) M' מריצה M על w .

(2) אם M דוחה \Leftarrow דוחה.

• אם M מקבלת \Leftarrow ממשיכה לשלב (3).

(3) M' בודקת אם $y \in PAL$.

• אם כן \Leftarrow מקבלת.

• אם לא \Leftarrow דוחה.

הוכחת הנכונות

$$L(M') \in L_{\text{NOTREG}} \iff L(M') \in PAL \iff x \in L_{\text{HALT}}$$

$$\text{שני מקרים:} \iff x \notin L_{\text{HALT}}$$

$$\langle M_\emptyset \rangle \notin L_{\text{NOTREG}} \iff L(M_\emptyset) = \emptyset \text{ ו- } f(x) = \langle M_\emptyset \rangle \iff x \neq \langle M, w \rangle \quad \text{מקרה 1:} \\ f(x) \notin L_{\text{NOTREG}} \iff$$

$$\langle M_\emptyset \rangle \notin L_{\text{NOTREG}} \iff L(M_\emptyset) = \emptyset \iff x = \langle M, w \rangle \text{ ו- } M \text{ לא עוצרת על } w \quad \text{מקרה 2:} \\ f(x) \notin L_{\text{NOTREG}} \iff$$

דוגמה 7.14 $\bar{L}_{\text{acc}} \leq L_{\text{REG}}$

תהי L_{REG} השפה

$$L_{\text{REG}} = \{ \langle M \rangle \mid L(M) \text{ רגולרית} \}.$$

הוכיחו כי השפה L_{REG} לא כריעה על ידי רדוקציה מ- \bar{L}_{acc} .

פתרון:

השפה \bar{L}_{acc} מוגדרת

$$\bar{L}_{\text{acc}} = \{ \langle M, w \rangle \mid M \text{ לא מקבלת } w \} \cup \{ x \mid x \neq \langle M, w \rangle \}.$$

והשפה L_{REG} מוגדרת

$$L_{\text{REG}} = \{ \langle M \rangle \mid L(M) \text{ רגולרית} \}.$$

נגדיר הפונקציה הבאה:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ \langle M_\emptyset \rangle & x \neq \langle M, w \rangle \end{cases}$$

כאשר M_\emptyset המ"ט שדוחה כל קלט ו- M' מ"ט הבאה:

$$M' = \text{על כל קלט } y:$$

(1) מריצה M על w .

(2) אם M דוחה \Leftarrow דוחה.

• אם M מקבלת \Leftarrow בודקת אם y פלינדרום:

• אם כן \Leftarrow מקבלת.

• אם לא \Leftarrow דוחה.

אבחנה

$$L(M') = \begin{cases} PAL & w \in L(M) \\ \emptyset & w \notin L(M) \end{cases}$$

אם $x \in \bar{L}_{acc}$ שני מקרים: \Leftarrow

מקרה 1: $x \neq \langle M, w \rangle \Leftarrow f(x) = \langle M_{\emptyset} \rangle \Leftarrow L(M_{\emptyset}) = \emptyset \Leftarrow \langle M_{\emptyset} \rangle \in L_{REG} \Leftarrow f(x) \in L_{REG}$

מקרה 2: $x = \langle M, w \rangle \Leftarrow x \notin L(M) \Leftarrow f(x) = \langle M' \rangle \Leftarrow L(M') = \emptyset$ ולפי האבחנה $\langle M_{\emptyset} \rangle \in L_{REG} \Leftarrow f(x) \in L_{REG}$

אם $x \notin \bar{L}_{acc} \Leftarrow w \in L(M) \Leftarrow f(x) = \langle M' \rangle \Leftarrow L(M') \in PAL \Leftarrow f(x) \in PAL$
 $f(x) \notin L_{REG} \Leftarrow$

7.15 דוגמה $L_{acc} \leq L_{REG}$

תהי L_{REG} השפה

$$L_{REG} = \{ \langle M \rangle \mid L(M) \text{ רגולרית} \}.$$

הוכיחו כי השפה L_{REG} לא כריעה על ידי רדוקציה מ- L_{acc} .

פתרון:

השפה L_{acc} מוגדרת

$$L_{acc} = \{ \langle M, w \rangle \mid w \text{ מקבלת } M \}.$$

והשפה L_{REG} מוגדרת

$$L_{REG} = \{ \langle M \rangle \mid L(M) \text{ רגולרית} \}.$$

נגדיר הפונקציה הבאה:

$$f(x) = \begin{cases} \langle M' \rangle & x = \langle M, w \rangle \\ \langle M_{PAL} \rangle & x \neq \langle M, w \rangle \end{cases}$$

כאשר M_{PAL} המ"ט שמכריעה את השפה של פלינדרומים, ו- M' מ"ט הבאה:

$$M' = \text{על כל קלט } y:$$

(1) M' בודקת אם y פלינדרום:

- אם כן \Leftarrow מקבלת.
- אם לא מריצה M על w ועונה כמזה.

הוכחת נכונות הרדוקציה

אם $x \in L_{acc} \Leftarrow M \text{ מקבלת } w \Leftarrow L(M') = \Sigma^* \Leftarrow f(x) \in REG$

$x \notin L_{acc} \Leftarrow$ שני מקרים:

מקרה 1: $x \neq \langle M, w \rangle \Leftarrow f(x) = \langle M_{PAL} \rangle \Leftarrow L(M_{PAL}) = PAL \Leftarrow \langle M_{PAL} \rangle \notin L_{REG}$
 $f(x) \notin L_{REG} \Leftarrow$

מקרה 2: $x = \langle M, w \rangle \Leftarrow M \text{ לא מקבלת } w \Leftarrow L(M') = PAL \Leftarrow \langle M' \rangle \notin L_{REG}$
 $f(x) \notin L_{REG} \Leftarrow$

דוגמה 7.16 $\bar{L}_{acc} \leq L_{M_1 \neg M_2}$

נתונה השפה הבאה:

$$L = \{ \langle M_1, M_2, w \rangle \mid w \in L(M_1) \wedge w \notin L(M_2) \} .$$

הוכיחו כי $L \notin RE$ ע"י רדוקציה מ- \bar{L}_{acc} .**פתרון:**פונקצית הרדוקציה:

$$f(x) = \begin{cases} \langle M^*, M, w \rangle & x = \langle M, w \rangle \\ \langle M^*, M_\emptyset, \varepsilon \rangle & x \neq \langle M, w \rangle \end{cases}$$

כאשר

• M^* היא מ"ט שמקבלת כל קלט• M_\emptyset היא מ"ט שדוחה כל קלט.נכונת הרדוקציה:

ראשית, f חשיבה כי ניתן לבנות מ"ט שתבדוק האם $x = \langle M, w \rangle$. אם לא, תחזיר קידוד קבוע $\langle M^*, M_\emptyset, \varepsilon \rangle$ ואם כן, תחזיר קידוד $\langle M^*, M, w \rangle$.

נוכיח כי

$$x \in \bar{L}_{acc} \iff f(x) \in L_{M_1 \neg M_2} .$$

אם $x \in \bar{L}_{acc}$ שני מקרים:

$$\text{מקרה 1: } x \neq \langle M, w \rangle \iff f(x) = \langle M^*, M_\emptyset, \varepsilon \rangle \iff \varepsilon \in L(M^*) \text{ ו- } \varepsilon \notin L(M_\emptyset) \iff f(x) \in L_{M_1 \neg M_2} .$$

$$\text{מקרה 2: } x = \langle M, w \rangle \iff x \in L(M) \text{ ו- } w \notin L(M) \iff f(x) = \langle M^*, M, w \rangle \iff w \in L(M^*) \text{ ו- } w \notin L(M) \iff f(x) \in L_{M_1 \neg M_2} .$$

$$\text{אם } x \notin \bar{L}_{acc} \iff x = \langle M, w \rangle \text{ ו- } w \in L(M) \iff f(x) = \langle M^*, M, w \rangle \iff w \in L(M^*) \text{ ו- } w \in L(M) \iff f(x) \notin L_{M_1 \neg M_2} .$$

לסיכום, הוכחנו רדוקציה $\bar{L}_{acc} \leq L_{M_1 \neg M_2}$, ומכיוון ש- $\bar{L}_{acc} \notin RE$ ממשפט הרדוקציה מתקיים $L_{M_1 \neg M_2} \notin RE$.

דוגמה 7.17 $L_{acc} \leq L_{M_1 \subset M_2}$

נתונה השפה הבאה:

$$L = \{ \langle M_1, M_2, w \rangle \mid w \in L(M_1) \wedge w \notin L(M_2) \} .$$

הוכיחו כי $L \notin RE$ ע"י רדוקציה מ- L_{acc} .**פתרון:**פונקצית הרדוקציה:

$$f(x) = \begin{cases} \langle M_\emptyset, M' \rangle & x = \langle M, w \rangle \\ \langle M_\emptyset, M_\emptyset \rangle & x \neq \langle M, w \rangle \end{cases}$$

כאשר

- M_\emptyset היא מ"ט שדוחה כל קלט.
- M' היא מ"ט שעל קלט y מתעלמת מ- y ומריצה M על w ועונה כמוה.

אבחנה:

$$L(M') = \begin{cases} \Sigma^* & w \in L(M) \\ \emptyset & w \notin L(M) \end{cases}.$$

נכונת הרדוקציה:

ראשית, f חשיבה כי ניתן לבנות מ"ט שתבדוק האם $x = \langle M, w \rangle$. אם לא, תחזיר קידוד קבוע $\langle M_\emptyset, M_\emptyset \rangle$ ואם כן, תחזיר קידוד $\langle M^*, M' \rangle$, כאשר M_\emptyset היא קידוד קבוע ו- M' נוצר ע"י הוספת קוד ל- $\langle M \rangle$ המוחק את הקלט y ורושם w במקומו.

נוכיח כי

$$x \in L_{\text{acc}} \Leftrightarrow f(x) \in L_{M_1 \subset M_2}.$$

$$L(M') = \Sigma^* \text{ ולפי האבחנה } f(x) = \langle M_\emptyset, M' \rangle \Leftrightarrow \begin{aligned} & x = \langle M, w \rangle \text{ ו- } w \in L(M) \Leftrightarrow x \in L_{\text{acc}} \\ & f(x) \in L_{M_1 \subset M_2} \Leftrightarrow L(M_\emptyset) \subset L(M') \Leftrightarrow \end{aligned}$$

$$x \notin L_{\text{acc}} \Leftrightarrow \text{שני מקרים:}$$

$$\text{מקרה 1: } x \neq \langle M, w \rangle \Leftrightarrow f(x) = \langle M_\emptyset, M_\emptyset \rangle \text{ ו- } L(M_\emptyset) = L(M_\emptyset) \Leftrightarrow f(x) \notin L_{M_1 \subset M_2}.$$

$$\text{מקרה 2: } x = \langle M, w \rangle \text{ ו- } w \notin L(M) \Leftrightarrow f(x) = \langle M_\emptyset, M' \rangle \text{ ולפי האבחנה } L(M') = \emptyset \Leftrightarrow f(x) \notin L_{M_1 \subset M_2} \Leftrightarrow L(M') = L(M_\emptyset).$$

לסיכום, הוכחנו רדוקציה $L_{\text{acc}} \leq L_{M_1 \subset M_2}$, ומכיוון ש- $L_{\text{acc}} \notin R$ ממשפט הרדוקציה מתקיים $L_{M_1 \subset M_2} \notin R$.

שיעור 8

מבוא לסיבוכיות

8.1 הגדרה של סיבוכיות

8.1 הערה

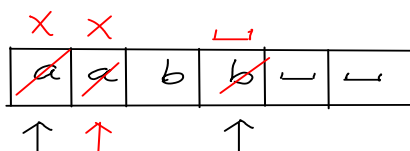
זמן ריצה של מ"ט M על קלט w , נמדד ביחס לגודל הקלט w , כלומר $f(|w|)$.

8.1 הגדרה

נאמר כי ניתן להכריע שפה L בזמן $f(n)$, אם קיימת מ"ט M המכריעה את L ולכן קלט $w \in \Sigma^*$, זמן הריצה של M על w חסום ע"י $f(|w|)$.

8.1 דוגמה

נבנה מ"ט M המכריעה השפה $L = \{a^n b^n \mid n \geq 0\}$.



התאור של M :

על קלט w :

(1) אם התו שמתחת לראש הוא $_$ \Leftarrow מקבלת.

(2) אם התו שמתחת לראש הוא b \Leftarrow דוחה.

(3) מוחקת את התו שמתחת לראש ע"י X .

(4) מזיזה את הראש ימינה עד התו הראשון משמאל ל- $_$.

• אם התו הוא a או X \Leftarrow דוחה.

• מוחקת את התו שמתחת לראש ע"י $_$, מזיזה את הראש שמאלה עד התו הראשון מימין ל- X וחוזרת ל- (1).

זמן הריצה

• $\frac{|w|}{2}$ איטרציות.

• בכל איטרציה מבצעים $O(|w|)$ צעדים.

$$\frac{|w|}{2} \cdot O(|w|) = O(|w|^2).$$

הגדרה 8.2 זמן הריצה

זמן הריצה של מ"ט M על קלט w היא פונקציה $f(|w|)$ השווה למספר הצעדים הנדרש בחישוב של M על w .

הערה 8.2

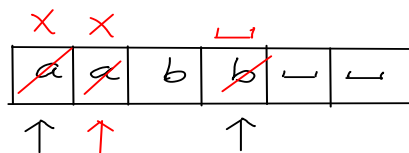
זמן הריצה של מ"ט נמדד ביחס לגודל הקלט $|w|$.

הגדרה 8.3

אומרים כי ניתן להכריעה שפה L בזמן $f(n)$ אם קיימת מ"ט M המכריעה את L כך שלכל $w \in \Sigma^*$, זמן הריצה של M על w חסום ע"י $f(|w|)$.

דוגמה 8.2

נבנה מ"ט M עם סרט יחיד שמכריעה את השפה $L = \{a^n b^n \mid n \geq 0\}$.



התאור של M :

על קלט w :

(1) אם התו שמתחת לראש הוא $_$ \Leftarrow מקבלת.

(2) אם התו שמתחת לראש הוא b \Leftarrow דוחה.

(3) מוחקת את התו שמתחת לראש ע"י X .

(4) מזיזה את הראש ימינה עד התו הראשון משמאל ל- $_$.

• אם התו הוא a או X \Leftarrow דוחה.

• מוחקת את התו שמתחת לראש ע"י $_$, מזיזה את הראש שמאלה עד התו הראשון מימין ל- X וחוזרת ל- (1).

זמן הריצה

• M מבצעת $\frac{|w|}{2}$ איטרציות.

• בכל איטרציה M סורקת את הסרט פעמיים וזה עולה $O(|w|)$.

• לכן סה"כ זמן הריצה של M חסום ע"י

$$\frac{|w|}{2} \cdot O(|w|) = O(|w|^2).$$

8.3 דוגמה

נבנה מ"ט מרובת סרטים M' שמכריעה את השפה $L = \{a^n b^n \mid n \geq 0\}$.

1)

a	a	b	b	␣	␣
---	---	---	---	---	---

2)

6	6				
---	---	--	--	--	--

התאור של M' :

על קלט w :

(1) מעתיקה את ה- b ים לסרט 2 (ותוך כדי בודקת האם w מהצורה a^*b^*). $O(|w|)$

(2) מזיזה את הראשים לתחילת הסרטים. $O(|w|)$

(3) אם שני הראשען מצביעים על ␣ מקבלת.

(4) אם אחד הראשים מצביע על ␣ והשני לא ␣ לא.

(5) מזיזה את שהע הראשים ימינה וחוזרת לשלב (3). שלבים (3-5): $O(|w|)$.

זמן הריצה

זמן הריצה של M' הוא $O(|w|)$.

8.2 יחס בין הסיבוכיות של מ"ט סרט יחיד ומטמ"ס

8.1 משפט

לכל מ"ט מרובת סרטים M הרצה בזמן $f(n)$ קיימת מ"ט סרט יחיד M' השקולה ל- M ורצה בזמן $O(f^2(n))$.

הוכחה:

בהינתן מ"ט מרובת סרטים M , הרצה בזמן $f(n)$, נבנה מ"ט עם סרט יחיד M' באותו אופן כמו בהוכחת השקילות במשפט 3.1.

כלומר, M' שומרת את התוכן של k סרטים של M על הסרט היחיד שלה (עם הפרדה ע"י #), ובכל צעד חישוב, M' סורקת את הסרט שלה כדי לזהות שת האותיות שמתחת לראשים (שמסומנות ב- \hat{a}) ואחרי זה, משתמשת בפונקצית המעברים של M , וסורקת את הסרט פעם נוספת כדי לעדכן את התוכן בכל אחד מהסרטים ואת מיקום הראש בכל אחד מהסרטים.

1) 2)

⋮

k)

#	$\hat{\alpha}_1$	#	$\hat{\alpha}_2$	#	$\hat{\alpha}_3$	#	
---	------------------	---	------------------	---	------------------	---	--

כמה לוקח ל- M' לסרוק את הסרט שלה? מכיוון שהסרט של M' מכיל את התוכן של k הסרטים של M , והגודל של כל אחד מהסרטים של M חסום ע"י $f(n)$, גודל הסרט של M' חסום ע"י

$$k \cdot f(n) = O(f(n)) .$$

העלות של הסריקה של M' לסרט שלה היא $O(f(n))$ וזה עלות של צעד חישוב בריצה של M' על הקלט.

מכיוון ש- M רצה בזמן $f(n)$, זמן היצרה של M' חסום ע"י

$$f(n) \cdot O(f(n)) = O(f^2(n)) .$$

■

8.3 יחס בין הסיבוכיות של מ"ט דטרמיניסטית ומ"ט א"ד

הגדרה 8.4

בהינתן מ"ט א"ד M , זמן הריצה של M על קלט w , היא פונקציה $f(|w|)$ השווה למספר הצעדים בחישוב המקסימלי של M על w .

משפט 8.2

לכל מ"ט א"ד N הרצה בזמן $f(n)$, קיימת מ"ט דטרמיניסטית D השקולה ל- N ורצה בזמן $2^{(f(n))}$.

הוכחה:

בהינתן מ"ט א"ד N הרצה בזמן $f(n)$ מ"ט דטרמיניסטית D באותו אופן כמו בהוכחת השקילות במשפט 4.1.

כלומר, בהינתן קלט w , D תסרו' את עץ החישוב של N ו- w לרוחב ותקבל כל אחד החישובים של N המסתיים ב- q_{acc} .

בהינתן קלט w באורך n :

- כל מסלול בעץ החישוב של N על w חסום ע"י $f(n)$.
- מספר החישובים ש- D מבצעת חסום ע"י מספר הקודקודים בעץ החישוב של N ו- w .
- מכיוון שמספר הבנים של כל קודקוד בעץ החישוב חסום ע"י

$$C = 3|Q| \cdot |\Gamma|$$

מספר הקודקודים בעץ החישוב חסום ע"י

$$C^0 + C^2 + \dots + C^{f(n)} \leq C^{f(n)+1} = C \cdot C^{f(n)}.$$

ולכן זמן הריצה של D חסום ע"י

$$f(n) \cdot C \cdot C^{f(n)} \leq C^{f(n)} \cdot C^{f(n)} = C^{2f(n)} = (C^2)^{f(n)} = 2^{C' \cdot f(n)} = 2^{O(f(n))}.$$

נתייחס כאן לשני החסמים הבאים:



(1) חסם פולינומיאלי הוא חסם מהצורה n^c עבור $c > 0$ כלשהו.

(2) חסם אקספוננציאלי הוא חסם מהצורה 2^{n^c} עבור $c > 0$ כלשהו.

הגדרה 8.5 בעיית הכרעה

בעיית הכרעה מוגדרת באופן הבא:

"בהינתן קלט כלשהו, האם הקלט מקיים תנאי מסוים"

דוגמה 8.4

בהינתן מספר n , האם n ראשוני?

כל בעיית הכרעה ניתן לתאר כפשה שקולה:

$$L_{\text{prime}} = \{ \langle n \rangle \mid n \text{ ראשוני} \}.$$

משפט 8.3

. שפה \equiv בעיית הכרעה

הגדרה 8.6 אלגוריתם זמן פולינומיאלי

אומרים כי אלגוריתם A מכריעה בעייה בזמן פולינומיאלי אם קיים קבוע $c > 0$ כך שזמן הריצה של A על כל קלט w חסום ע"י $O(|w|^c)$.

משפט 8.4 התזה של צירץ' (Church Thesis)

אם קיים אלגוריתם המכריע בעייה בזמן פולינומיאלי, אז קיימת מ"ט דטרמיניסטית המכריעה את השפה השקולה לבעייה זו בזמן פולינומיאלי.

. מכונת טיורינג \equiv אלגוריתם מכריעה

8.4 המחלקה P **הגדרה 8.7 המחלקה P**

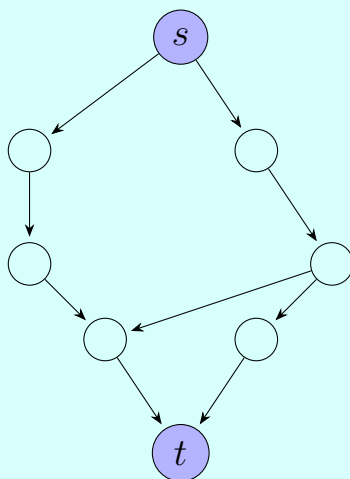
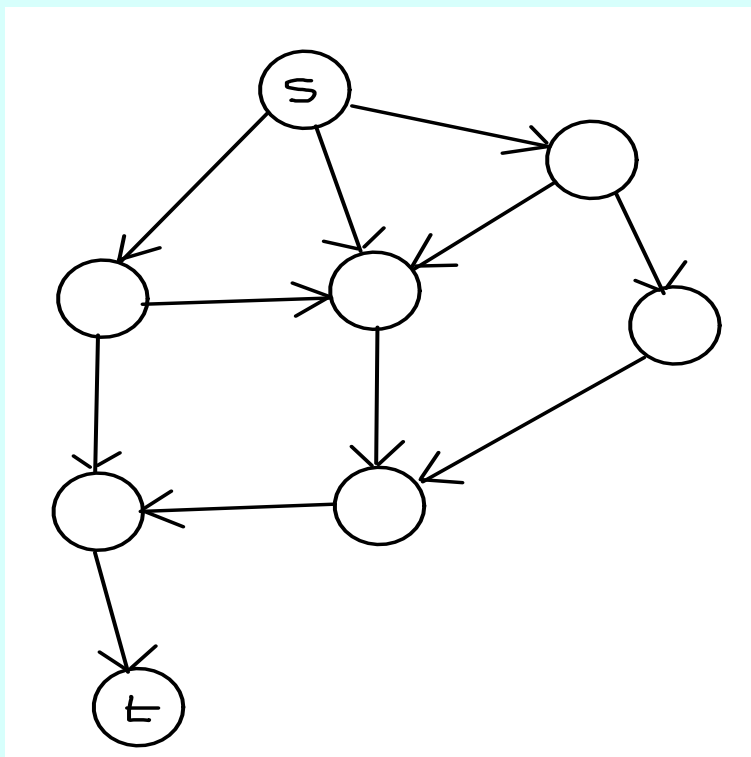
המחלקה P היא אוסף כל הבעיות (השפות) שקיים עבורן אלגוריתם (מכונת טיורינג דטרמיניסטית) המכריע אותן בזמן פולינומיאלי.

דוגמה 8.5

$$L = \{a^n b^n \mid n \geq 0\} \in P.$$

8.5 בעיית PATH

הגדרה 8.8 בעיית המסלול בגרף מכוון



קלט: גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$.

פלט: האם קיים מסלול ב- G מ- s ל- t ?

$$PATH = \{ \langle G, s, t \rangle \mid t \text{ ל-} s \text{ ב-} G \}$$

משפט 8.5

$$PATH \in P.$$

הוכחה: נבנה אלגוריתם A עבור הבעיה $PATH$.

$A = \langle G, s, t \rangle$ על קלט

(1) צובע את s .

(2) מבצע $|V| - 1$ פעמים:

• לכל $(u, v) \in E$ צלע

* אם u צבוע \Leftarrow צבע את v .

(3) • אם t צבוע \Leftarrow החזיר "כן".

• אחרת \Leftarrow החזיר "לא".

זמן ריצה של האלגוריתם הוא $O(|V| \cdot |E|)$ פולינומיאלי במספר הקודקודים $|V|$.

האם זה פולינומיאלי בגודל הקלט $|\langle G \rangle|$?

איך נקודד את G ?

• נניח כי $|V| = n$ ו- $V = \{1, 2, 3, \dots, n\}$.

• נניח כי הצלעות נתונות ע"י מטריצה M בגודל $n \times n$ כך ש-

$$M_{ij} = \begin{cases} 1 & (i, j) \in E \\ 0 & (i, j) \notin E \end{cases}.$$

• נניח כי מספרים מקודדים בבסיס ביניארי.

• אזי גודל הקידוד של G שווה $n^2 + n \log_2 n$, כלומר

$$|\langle G \rangle| = \Omega(|V|^2) \Rightarrow |V| = O(|\langle G \rangle|).$$

ולכן כל אלגוריתם הרץ בזמן פולינומיאלי במספר הקודקודים $|V|$ ירוץ בזמן פולינומיאלי בגודל הקידוד $|\langle G \rangle|$.



ולכן A רץ בזמן פולינומיאלי בגודל הקלט.

8.6 בעיית RELPRIME

הגדרה 8.9 מספרים זרים (Relatively prime)

שני מספרים x, y זרים אם המחלק המשותף הגדול ביותר, מסומן $\gcd(x, y)$, שווה 1.

הגדרה 8.10 בעיית RELPRIME

קלט: שני מספרים x ו- y .

פלט: האם x ו- y זרים?

$$RELPRIME = \{ \langle x, y \rangle \mid \gcd(x, y) = 1 \}.$$

משפט 8.6

$$RELPRIME \in P.$$

הוכחה: נבנה אלגוריתם A המכריע את $RELPRIME$ בזמן פולינומיאלי.

האלגוריתם מבוסס על העובדה ש-

$$\gcd(x, y) = 1 \iff \langle x, y \rangle \in RELPRIME.$$

ולכן נשתמש באלגוריתם האוקלידי לחישוב \gcd :

$$\gcd(x, y) = \begin{cases} x & y = 0 \\ \gcd(y, x \bmod y) & y \neq 0 \end{cases}.$$

הוכחה: נסמן $d = \gcd(x, y)$. אזי קיימים שלמים s, t כך ש- $dx + ty = d$. נסמן $r = x \bmod y$. אז $x = qy + r$.
לכן

$$s(qy + r) + ty = d \implies sr + (t + sq)y = d \implies \gcd(x, y) = d = \gcd(y, r).$$

לדוגמה:

$$\gcd(18, 32) = \gcd(32, 18) = \gcd(18, 14) = \gcd(14, 4) = \gcd(4, 2) = \gcd(2, 0) = 2.$$

האלגוריתם האוקלידי:

על קלט x ו- y :

(1) כל עוד $y \neq 0$

$$x \bmod y \rightarrow x$$

$$\text{swap}(x, y)$$

(כלומר מחליפים בין x ו- y).

(2) מחזירים את x .

האלגוריתם A המכריע $RELPRIME$:

$A = \text{על קלט } \langle x, y \rangle$

(1) מריץ את האלגוריתם האוקלידי על x ו- y .

• אם האלגוריתם האוקלידי החזיר 1 מקבל.

• אחרת דוחה.

נכונות האלגוריתם נובעת מנכונות האלגוריתם האוקלידי.

נוכיח כי A רץ בזמן פולינומיאלי בגודל הקלט.

טענת עזר:

$$\text{אם } x > y \text{ אזי } x \bmod y < \frac{x}{2}.$$

הוכחה:

יש שתי אפשרויות:

• אם $y \leq \frac{x}{2}$ אזי

$$x \bmod y < y \leq \frac{x}{2}.$$

• נניח ש- $\frac{x}{2} < y < x$

מכיוון ש- $x = qy + (x \bmod y)$, וגם $x < 2y$ אז בהכרח $q < 2$ ולכן $x = y + (x \bmod y)$ ולכן $x - y = x \bmod y$.

לפיכך

$$x \bmod y = x - y < \frac{x}{2}.$$

■

לפי טענת העזר, אחרי כל איטרציה x קטן בלפחות חצי.

מכיוון שבכל איטרציה מחליפים בין x ו- y , אחרי כל שתי איטרציות גם x וגם y קטנים בלפחות חצי.

ולכן לאחר $\log_2 x + \log_2 y$ איטרציות לפחות x או y שווים ל-0.

ולכן מספר האיטרציות באלגוריתם האוקלידי חסום ע"י $\log_2 x + \log_2 y$, וזה בדיוק זמן הריצה של האלגוריתם A .

ולכן A רץ בזמן פולינומיאלי בגודל הקלט.

ולכן

$$RELPRIME \in P.$$

■

שיעור 9

המחלקה P והמחלקה NP

9.1 המחלקה P

- המחלקה P היא אוסף כל הבעיות שקיים עבורן אלגוריתם המכריע אותן בזמן פולינומיאלי.
- אלגוריתם מכריע \equiv מ"ט דטרמיניסטי ,
בעיית הכרעה \equiv שפה ,
- אלגוריתם A מכריע בעייה בזמן פולינומיאלי אם קיים קבוע $c > 0$ כך שזמן הריצה של A על כל קלט w חסום ע"י $O(|w|^c)$.

9.2 דוגמאות לבעיות ב-P

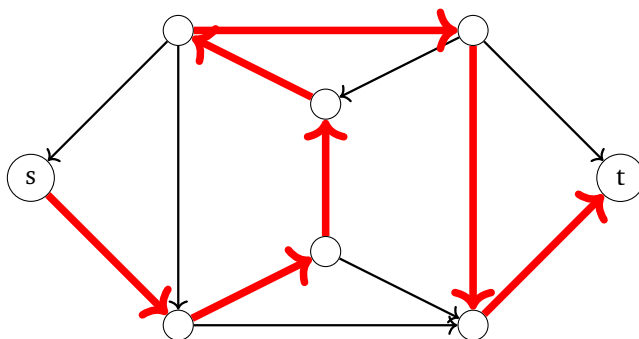
- (1) $PATH = \{ \langle G, s, t \rangle \mid G \text{ גרף מכוון המכיל מסלול מ- } s \text{ ל- } t \} \in P$
- (2) $RELPRIME = \{ \langle x, y \rangle \mid x \text{ ו- } y \text{ זרים} \} \in P$

9.3 בעיית המסלול ההמילטוני HAMPATH

הגדרה 9.1 HAMPATH

בהינתן גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$. מסלול ההמילטוני מ- s ל- t ב- G הוא מסלול מ- s ל- t שעובר דרך כל קודקוד בגרף בדיוק פעם אחת.

לדוגמה:



הגדרה 9.2 בעיית HAMPATH

קלט: גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$.

פלט: האם G מכיל מסלול המילטוני מ- s ל- t ?

$$HAMPATH = \{ \langle G, s, t \rangle \mid \text{?} t \text{ ל-} s \}$$

נשאל שאלה: האם $HAMPATH \in P$?

לא ידוע האם קיים אלגוריתם המכריע את $HAMPATH$ בזמן פולינומיאלי (שאלה פתוחה).

- בהינתן קלט $\langle G, s, t \rangle$, האם $\langle G, s, t \rangle \in HAMPATH$?
- נענה על שאלה אחרת:

בהינתן קלט $\langle G, s, t \rangle$, ומחרוזת y , האם $\langle G, s, t \rangle \in HAMPATH$?

- יתן לבדוק האם y היא מסלול המילטוני מ- s ל- t ב- G בזמן פולינומיאלי ולענות בהתאם.
- במקרה זה, אומרים כי $HAMPATH$ ניתנת לאימות בזמן פולינומיאלי.

9.4 אלגוריתם אימות

הגדרה 9.3 אלגוריתם אימות

אלגוריתם אימות עבור בעיית A הוא אלגוריתם V כך שלכל קלט $w \in \Sigma^*$ מתקיים:

$w \in A$ אם ורק אם קיימת מחרוזת (עדות) y באורך פולינומיאלי ב- $|w|$ כך ש- V מקבל את הזוג (w, y) כלומר:

• אם $w \in A$ $\iff \exists y : V(w, y) = T$

• אם $w \notin A$ $\iff \forall y : V(w, y) = F$

9.1 הערה

- זמן ריצה של אלגוריתם אימות נמדד ביחס לגודל הקלט $|w|$.
- אלגוריתם אימות פולינומיאלי אם הוא רץ בזמן פולינומיאלי.

9.5 המחלקה NP

הגדרה 9.4 המחלקה NP

המחלקה NP היא אוסף כל הבעיות שקיים עבורן אלגוריתם אימות פולינומיאלי.

משפט 9.1 $HAMPATH \in NP$

בעיית המסלול ההמילטוני $HAMPATH$:

קלט: גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$.

פלט: האם G מכיל מסלול המילטוני מ- s ל- t ?

$$HAMPATH = \{ \langle G, s, t \rangle \mid \text{ } G \text{ מכיל מסלול המילטוני מ-} s \text{ ל-} t \}$$

הוכיחו כי $HAMPATH \in NP$.

הוכחה: נבנה אלגוריתם אימות עבור $HAMPATH$.

$V = \text{על קלט } \langle \langle G, s, t \rangle, y \rangle$:

(1) בודק האם y היא סדרה של

$$u_1, u_2, \dots, u_n$$

השונים זה מזה.

• אם לא \Leftarrow דוחה.

(2) בודק האם $u_1 = s$ ו- $u_n = t$.

• אם לא \Leftarrow דוחה.

(3) בודק שכל הצלעות (u_i, u_{i+1}) (לכל $1 \leq i \leq n$) קיימות ב- G .

• אם כן \Leftarrow מקבל.

• אם לא \Leftarrow דוחה.

נכונות

• זמן הריצה של האלגוריתם הוא פולינומיאלי בגודל הקלט.

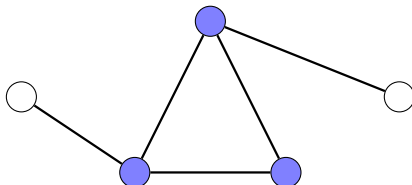
• אם $\langle G, s, t \rangle \in HAMPATH \Leftarrow G$ מכיל מסלול המילטוני מ- s ל- $t \Leftarrow$ עבור y שהוא קידוד של מסלול זה, V יקבל את הזוג $(\langle G, s, t \rangle, y)$.

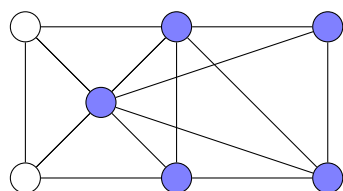
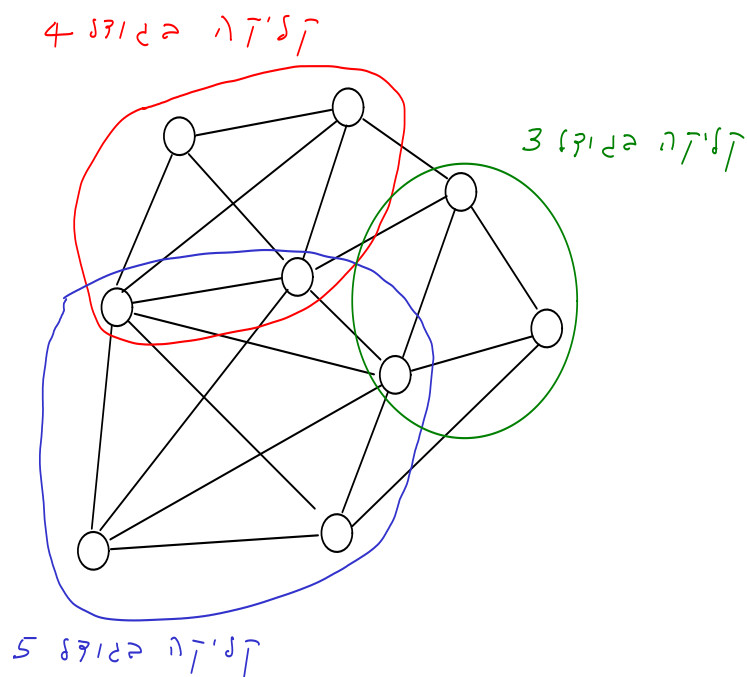
• אם $\langle G, s, t \rangle \notin HAMPATH \Leftarrow G$ לא מכיל מסלול המילטוני מ- s ל- $t \Leftarrow$ לכל y , האלגוריתם ידחה את הזוג $(\langle G, s, t \rangle, y)$.

הגדרה 9.5 קליקה

בהינתן גרף לא מכוון $G = (V, E)$, קליקה ב- G היא תת-קבוצה של קודקודים $C \subseteq V$ כך שלכל שני קודקודים $u, v \in C$ מתקיים $(u, v) \in E$.

קליקה בגודל $k = 3$:



קליקה בגודל $k = 5$:**הגדרה 9.6 בעיית הקליקה**קלט: גרף לא מכוון $G = (V, E)$ ומספר k .פלט: האם G קליקה בגודל k ?

$$CLIQUE = \{ \langle G, k \rangle \mid k \text{ המכיל קליקה בגודל } k \}$$

משפט 9.2 $CLIQUE \in NP$

$$CLIQUE \in NP.$$

הוכחה: נבנה אלגוריתם אימות V עבור $CLIQUE$. $V = \text{על קלט } \langle G, k \rangle, y$ **(1)** בודק האם y היא קבוצה של k קודקודים שונים מ- G .• אם לא \Leftarrow דוחה.**(2)** בודק האם כל שני קודקודים מ- y מחוברים בצלע ב- G .• אם כן \Leftarrow מקבל.

- אם לא \Leftarrow דוחה.

הגדרה 9.7 בעיית $SubSetSum$

קלט: קבוצת מספרים $S = \{x_1, x_2, \dots, x_n\}$ ומספר t .

פלט: האם קיימת תת-קבוצה של S שסכום איבריה שווה t ?

$$SubSetSum = \left\{ \langle S, t \rangle \mid \sum_{x \in Y} x = t \text{ ש-} Y \subseteq S \text{ קיימת} \right\}$$

משפט 9.3 $SubSetSum \in NP$

$$SubSetSum \in NP.$$

הוכחה: נבנה אלגוריתם אימות V עבור $SubSetSum$.

$V =$ על קלט $(\langle S, t \rangle, y)$:

(1) בודק האם y היא תת-קבוצה של S .

- אם לא \Leftarrow דוחה.

(2) בודק האם סכום המספרים ב- y שווה t .

- אם לא \Leftarrow דוחה.

- אחרת \Leftarrow מקבל.

9.6 הקשר בין NP למ"ט א"ד

NP=Non-deterministic polynomial-time.

משפט 9.4

לכל בעייה A :

$A \in NP$ אם ורק אם קיימת מ"ט א"ד המכריעה את A בזמן פולינומיאלי.

דוגמה 9.1

נבנה מ"ט א"ד M המכריעה את $CLIQUE$ בזמן פולינומיאלי.

$M =$ על קלט $\langle G, k \rangle$:

- בוחרת באופן א"ד קבוצה y של k קודקודים מ- G .

- בודקת האם כל שני קודקודים מ- y מחוברים בצלע ב- G .

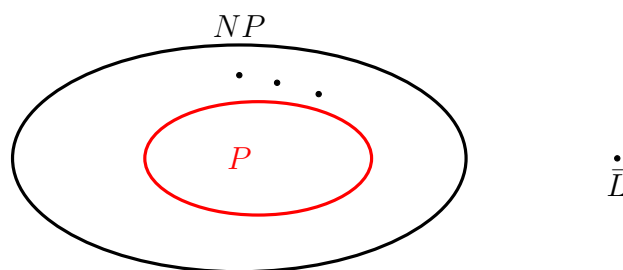
* אם כן \Leftarrow מקבלת.* אחרת \Leftarrow דוחה.אלגוריתם אימות \equiv מ"ט א"ד.

9.7 הקשר בין המחלקה P ו-NP

 $P =$ כל הבעיות שניתן להכריע בזמן פולינומיאלי. $NP =$ כל הבעיות שניתן לאמת בזמן פולינומיאלי.

משפט 9.5

$$P \subseteq NP.$$

שאלה פתוחה: האם $P = NP$?

משפט 9.6

 P סגורה תחת משלים.הוכחה: אם $A \in P$ אזי גם $\bar{A} \in P$.

הגדרה 9.8 $CoNP$

$$CoNP = \{A \mid \bar{A} \in NP.\}$$

לדוגמה:

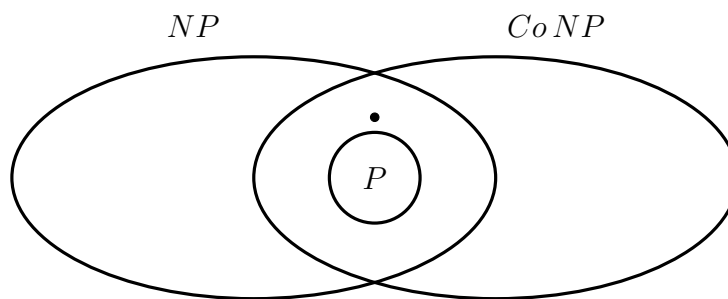
$$\overline{HAMPATH} \in CoNP.$$

$$\overline{CLIQUE} \in CoNP.$$

שאלה פתוחה: האם $NP = CoNP$?

משפט 9.7

$$P \subseteq NP \cap CoNP.$$



שאלה פתוחה: האם $P = NP \cap CoNP$?

נדון בשאלה המרכזית: האם $P = NP$?

הגדרה 9.9 פונקציה פולינומיאלית

בהינתן פונקציה $f : \Sigma^* \rightarrow \Sigma^*$, אומרים כי f חשיבה בזמן פולינומיאלי אם קיים אלגוריתם (מ"ט דטרמיניסטי) המחשב את f בזמן פולינומיאלי.

הגדרה 9.10 רדוקציה פולינומיאלית

בהינתן שתי הבעיות A ו- B . אומרים כי A ניתנת לרדוקציה פולינומיאלית ל- B , ומסמנים $A \leq_P B$, אם קיימת פונקציה $f : \Sigma^* \rightarrow \Sigma^*$ המקיימת:

(1) חשיבה בזמן פולינומיאלי

(2) לכל $w \in \Sigma^*$:

$$w \in A \iff f(w) \in B.$$

משפט 9.8 משפט הרדוקציה

לכל שתי בעיות A ו- B , אם $A \leq_P B$ אזי

(1) אם $B \in P$ אזי $A \in P$.

(2) אם $B \in NP$ אזי $A \in NP$.

מסקנה מ- (1) ו- (2):

(3) אם $A \notin P$ אזי $B \notin P$.

(4) אם $A \notin NP$ אזי $B \notin NP$.

הוכחה: מכיוון שקיימת רדוקציה $A \leq_P B$, קיימת פונקציה f חשיבה בזמן פולינומיאלי המקיימת, לכל $w \in \Sigma^*$,

$$w \in A \iff f(w) \in B.$$

יהי M_f האלגוריתם שמחשבת את f בזמן פולינומיאלי.

(1) נוכיח כי אם $B \in P$ אזי $A \in P$.

יהי M_B האלגוריתם שמכריע את B בזמן פולינומיאלי. נבנה אלגוריתם M_A המכריע את A בזמן פולינומיאלי.

התאור של M_A

$$M_A = \text{על כל קלט } w:$$

1. מחשב את $f(w)$ ע"י M_f .

2. מריץ את M_B על $f(w)$ ועונה כמוה.

נוכיח כי M_A מכריע את A בזמן פולינומיאלי:

- אם $w \in A \iff f(w) \in B \iff M_B \text{ מקבל את } f(w) \iff M_A \text{ מקבל את } w$.
- אם $w \notin A \iff f(w) \notin B \iff M_B \text{ דוחה את } f(w) \iff M_A \text{ דוחה את } w$.

נוכיח כי זמן הריצה של M_A הוא פולינומיאלי בגודל הקלט $|w|$ בזמן פולינומיאלי:

- נסמן ב- P_f את הפולינום של M_f .
- נסמן ב- P_B את הפולינום של M_B .

זמן הריצה של M_A על קלט w שווה

$$P_f(|w|) + P_B(|f(w)|)$$

מכיוו ש- $|f(w)| \leq P_f(|w|)$, זמו הריצה של M_A על w חסום ע"י

$$P_f(|w|) + P_B(P_f(|w|)) = P_f(|w|) + (P_B \circ P_f)(|w|)$$

כאשר $P_B \circ P_f$ מסמן את ההרכבה של שני פולינומים. לכן M_A רץ בזמן פולינומיאלי בגודל $|w|$.



שיעור 10

NP שלמות

10.1 המחלקות NPC ו- NPH

הגדרה 10.1 NP-hard

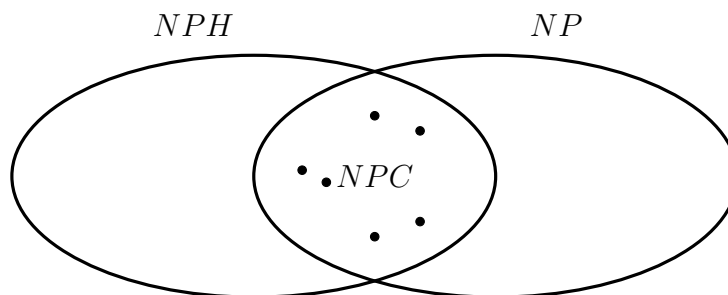
בעייה B נקראת NP קשה אם לכל בעייה $A \in NP$ קיימת רדוקציה $A \leq_p B$.

הגדרה 10.2 NP-complete

בעייה B נקראת NP שלמה אם

$$B \in NP \quad (1)$$

(2) לכל בעייה $A \in NP$ קיימת רדוקציה $A \leq_p B$.



משפט 10.1

אם $B \in NP$ שלמה וגם $B \in P$ אזי $P = NP$.

הוכחה:

• הוכחנו כבר ש- $P \subseteq NP$.

• נוכיח כי $NP \subseteq P$.

לכל בעייה $A \in NP$ קיימת רדוקציה $A \leq_p B$ ומכיוון ש- $B \in P$, ממשפט הרדוקציה מתקיים $A \in P$.

מסקנה 10.1

אם $A \leq_p B$ אזי $\bar{A} \leq_p \bar{B}$.

משפט 10.2

אם $A \leq_p B$ וגם $B \leq_p C$ אזי $A \leq_p C$.

הוכחה:

משפט 10.3

תהי B בעייה NP -שלמה. אזי לכל בעייה $C \in NP$, אם $B \leq_p C$ אזי גם C היא NP שלמה.

הוכחה: מכיוון ש- B היא NP -שלמה, לכל בעייה $A \in NP$ קיימת רדוקציה $A \leq_p B$. מכיוון ש- $B \leq_p C$ מהטרנזיטיביות מתקיים $A \leq_p C$ לכל בעייה $A \in NP$. ולכן C היא NP -שלמה.

10.2 בעיית הספיקות

הגדרה 10.3

נוסחת CNF ϕ היא נוסחה בוליאנית מעל n משתנים x_1, x_2, \dots, x_n המכילה m פסוקיות C_1, C_2, \dots, C_m , כאשר כל פסוקית מכילה אוסף של ליטרלים $(x_i \vee \bar{x}_i)$ המחוברים ע"י OR (\vee) בוליאני והפסוקיות מחוברים ע"י AND (\wedge) בוליאני.

לדוגמה

$$\phi = \left(x_1 \vee \bar{x}_2 \vee x_4 \vee \bar{x}_7 \right) \wedge \left(x_3 \vee x_5 \vee \bar{x}_8 \right) \wedge \dots$$

הגדרה 10.4 נוסחת CNF ספיקה

נוסחת CNF ϕ היא ספיקה אפ קימת השמה למשתנים x_1, x_2, \dots, x_n ע"י $T \setminus F$ כך ש- ϕ מקבלת ערך T , כלומר בכל פסוקית ישנו לפחות ליטרל אחד שקיבל ערך T .

10.3 בעיית SAT

הגדרה 10.5 בעיית SAT

קלט: נוסחת CNF ϕ .
פלט: האם ϕ ספיקה?

$$SAT = \{ \langle \phi \rangle \mid \text{נוסחת } CNF \text{ ספיקה} \}$$

משפט 10.4 $SAT \in NP$

$$SAT \in NP.$$

הוכחה: נבנה אלגוריתם אימות V עבור SAT .

$$V = \langle \langle \phi \rangle, y \rangle \text{ על קלט}$$

(1) בודק האם y היא השמה למשתנים x_1, x_2, \dots, x_n .

• אם לא $3CNF \Leftarrow$ דוחה.

(2) בודק האם השמה זו מספקת את ϕ .

• אם כן \Leftarrow מקבל.

• אם לא \Leftarrow דוחה.

■

10.4 משפט קוק לוין

משפט 10.5 (1973) משפט קוק לוין

הבעיית SAT היא NP - שלמה.

רעיון ההוכחה:

לכל $A \in NP$, $A \leq_p SAT$.
לכל $w \in \Sigma^*$:

$$w \in A \iff f(w) \in SAT,$$

כאן $f(w) = \langle \phi_w \rangle$.

מסקנה 10.2

$$P = NP \iff SAT \in P.$$

10.5 גרסאות של $kSAT$

ישנן לכל היותר k ליטרלים בכל פסוקית:

• $1SAT \in P$.

$$\phi = x_1 \wedge \bar{x}_2 \wedge x_3 \wedge \dots$$

• $2SAT \in P$.

$$\phi = (x_1 \vee \bar{x}_2) \wedge (x_2 \vee x_4) \wedge \dots$$

• $3SAT$ היא NP - שלמה.

10.6 בעיית $3SAT$

הגדרה 10.6 בעיית $3SAT$

קלט: נוסחת $3CNF$, ϕ .
פלט: האם ϕ ספיקה?

$$3SAT = \{ \langle \phi \rangle \mid \phi \text{ נוסחת } 3CNF \text{ ספיקה} \}$$

משפט 10.6 $3SAT$ היא NP שלמה. $3SAT$ היא NP שלמה.

הוכחה:

יש לקיים את השני תנאים הבאים:

$$3SAT \in NP \quad (1)$$

ניתן לבנות אלגוריתם אימות עבור $3SAT \in NP$ דומה לאלגוריתם האימות עבור SAT שבנינו בהוכחה של המשפט קוק-לויין 10.5 למעלה.

$$3SAT \text{ היא } NP \text{ קשה ע"י רדוקציה} \quad (2)$$

$$SAT \leq_p 3SAT.$$

ואז בגלל ש- SAT היא NP שלמה (לפי משפט קוק-לויין 10.5) ומכיוון ש- $3SAT \in NP$ אז לפי משפט האסימפטוטית 10.2 גם $3SAT$ היא NP -שלמה.

$$\underline{\text{קיום פונקצית הרדוקציה } SAT \leq_p 3SAT}$$

כעת נבנה את פונקציה הרדוקציה מ- SAT ל- $3SAT$.

ראשית נציין כי כל נוסחה בוליאנית ϕ ניתנת לרשום בצורה CNF בזמן פולינומיאלי.

בהינתן נוסחת CNF , ϕ (הקלט של SAT) נבנה בזמן פולינומיאלי נוסחת $3CNF$, ϕ' (הקלט של $3SAT$) ואז נוכיח שמתקיים

$$\langle \phi' \rangle \in 3SAT \iff \langle \phi \rangle \in SAT.$$

לכל פסוקית C ב- ϕ המכילה יותר מ-3 ליטרלים, ניצור אוסף C' ב- ϕ' של פסוקיות כך שכל פסוקית ב- C' תכיל 3 ליטרלים. למשל בהינתן הפסוקית C הבאה של ϕ :

$$C = x_1 \vee x_2 \vee x_3 \vee \bar{x}_4 \vee \bar{x}_5$$

ניצור את הפסוקית C' הבאה ב- ϕ' :

$$C' = (x_1 \vee x_2 \vee y_1) \wedge (\bar{y}_1 \vee x_3 \vee y_2) \wedge (\bar{y}_2 \vee \bar{x}_4 \vee \bar{x}_5).$$

באופן כללי, לכל פסוקית $C = a_1 \vee a_2 \vee \dots \vee a_k$ המכיל $k > 3$ ליטרלים, ניצור אוסף C' של פסוקיות שבו כל פסוקית מכילה 3 ליטרלים, ע"י הוספת $k-3$ משתנים y_1, y_2, \dots, y_{k-3} :

$$C' = (a_1 \vee a_2 \vee y_1) \wedge (\bar{y}_1 \vee a_3 \vee y_2) \wedge \dots \wedge (\bar{y}_{i-2} \vee a_i \vee y_{i-1}) \wedge \dots \wedge (\bar{y}_{k-3} \vee a_{k-1} \vee a_k).$$

בפרט, עבור כל פסוקית $C = (a_1 \vee a_2 \vee \dots \vee a_k)$ נניח $a_i = 1$ הוא הליטרל הראשון ששווה ל-1. אז

$$\bullet \text{ נשים } y_j = 1 \text{ לכל } 1 \leq j \leq i-2,$$

$$\bullet \text{ ונשים } y_j = 0 \text{ לכל } i-1 \leq j \leq k-3.$$

סיימנו להגדיר את הפונקציה הרדוקציה.

כעת נוכיח כי הפונקציה הזאת מקיימת את התנאי ההכרחי

$$\langle \phi' \rangle \in 3SAT \iff \langle \phi \rangle \in SAT.$$

כיוון \Leftarrow :

נניח כי $\langle \phi \rangle \in SAT$ ותהי X השמה המספקת את ϕ .

נוכיח שקיימת השמה X' מתאימה המספקת את ϕ' .

- בכל פסוקית C של ϕ , עבור הליטרלים a_1, a_2, \dots, a_k ניתן אותם ערכים כמו ב- X .
- מכיוון ש- X מספקת את ϕ , בכל פסוקית $C = (a_1 \vee a_2 \vee \dots \vee a_k)$ יש לפחות ליטרל אחד שקיבל ערך 1. נניח $a_i = 1$. אז על פי ההגדרה של פונקצית הרדוקציה:

$$* \text{ נשים } y_j = 1 \text{ לכל } 1 \leq j \leq i - 2,$$

$$* \text{ ונשים } y_j = 0 \text{ לכל } i - 1 \leq j \leq k - 3.$$

באופן הזה אנחנו ניצור אוסף C' של פסוקיות עם המבנה הבא:

$$\left(a_1 \vee a_2 \vee \overset{1}{y_1} \right) \wedge \left(\overset{0}{\bar{y}_1} \vee a_2 \vee \overset{1}{y_2} \right) \wedge \dots \wedge \left(\overset{0}{\bar{y}_{i-3}} \vee a_{i-1} \vee \overset{1}{y_{i-2}} \right) \wedge \left(\overset{0}{\bar{y}_{i-2}} \vee \overset{1}{a_i} \vee \overset{0}{y_{i-1}} \right) \wedge \left(\overset{1}{\bar{y}_{i-1}} \vee a_{i+1} \vee \overset{0}{y_i} \right) \\ \wedge \dots \wedge \left(\overset{1}{\bar{y}_{k-3}} \vee a_{k-1} \vee a_k \right)$$

ולכן השמה זו מספקת את C' ולכן $\langle \phi' \rangle \in 3SAT$.

כיוון \Rightarrow :

נניח כי $\langle \phi' \rangle \in 3SAT$ ותהי X' השמה המספקת את ϕ' .
נוכיח שקיימת השמה X המספקת את ϕ .

נסתכל על פסוקית $C = (a_1 \vee a_2 \vee \dots \vee a_k)$.
נניח בשלילה שלא קיימת השמה X המספקת את C . אז בהכרח

$$a_1 = a_2 = \dots = a_k = 0$$

לפי זה, באוסף פסוקיות C' שנקבל על פי ההגדרה של פונקצית הרדוקציה, $y_j = 1$ לכל $1 \leq j \leq k - 3$.
כלומר מתקיים $y_1 = y_2 = \dots = y_{k-3} = 0$. לכן

$$C' = \left(\overset{0}{a_1} \vee \overset{0}{a_2} \vee \overset{1}{y_1} \right) \wedge \left(\overset{0}{\bar{y}_1} \vee \overset{0}{a_3} \vee \overset{1}{y_2} \right) \wedge \dots \wedge \left(\overset{0}{\bar{y}_{i-2}} \vee \overset{0}{a_i} \vee \overset{1}{y_{i-1}} \right) \wedge \dots \wedge \left(\overset{0}{\bar{y}_{k-3}} \vee \overset{0}{a_{k-1}} \vee \overset{0}{a_k} \right)$$

הפסוקית האחרונה $\left(\overset{0}{\bar{y}_{k-3}} \vee \overset{0}{a_{k-1}} \vee \overset{0}{a_k} \right)$ אינה מסופקת.
לכן C' אינה מסופקת, בסתירה לכך ש- X' מספקת את C' .

ולכן $\langle \phi \rangle \in SAT$.

הוכחנו שקיימת הרדוקציה $SAT \leq 3SAT$.

כעת נוכיח כי הרדוקציה הזו היא זמן פולינומיאלית.

סיבוכיות

החישוב של הפונקציה מתבצע בזמן פולינומיאלי. ספציפי, אם האורך של הנוסחה ϕ הוא $n = |\phi|$ אז הרדוקציה היא $O(n)$.



10.7 הוכחת משפט קוק לוין*

משפט 10.7 משפט קוק לויין

הבעיית SAT היא NP - שלמה.

הוכחה:

חשיפה מלאה: ההוכחה הבאה מתבססת על ההוכחה שנתונה בהספר של Sipser.

על פי הגדרה 10.2 יש להוכיח ששני התנאים הבאים מתקיימים:

תנאי 1: $SAT \in NP$.תנאי 2: $A \leq_p SAT$ לכל $A \in NP$.ראשית נוכיח כי $SAT \in NP$:

כדי להוכיח כי SAT שייכת ל-NP, נוכיח כי אישור המורכב מהשמה מספקת עבור נוסחת קלט ϕ ניתן לאימות בזמן פולינומיאלי.

נניח כי $|\phi| = n$. כלומר ב- ϕ מופיעים n ליטרלים. ז"א השמה כלשהי דורשת n משתני בוליאניים לכל היותר.

- אלגוריתם האימות מחליף כל משתנה בנוסחה בערך המתאים לו על פי ההשמה. השלב הזה הוא $O(n)$.

- אחר כך האלגוריתם מחשב את ערכו של הביטוי:

* נניח כי הנוסחה ϕ מכילה k דורות של סוגריים בתוך סוגריים.

* החישוב מתחיל עם החישובים של הביטויים בתוך הסוגריים הכי בפנים.

* יש n סוגריים הכי-בפנים לכל היותר, וכל אחד של הסוגריים האלה מכיל n ליטרלים לכל היותר. לכן החישוב הזה הוא $O(n^2)$.

* יש k דורות של סוגריים לכן החישוב כולו הוא $O(kn^2)$.

- בסה"כ הסיבוכיות זמן הריצה היא

$$O(n) + O(kn^2) = O(n^2)$$

לפיכך אישור של השמה כלשהי מתבצע בזמן פולינומיאלי.

- אם ערכו של הביטוי הוא 1 הנוסחה ספיקה.

הוכחנו כי $SAT \in NP$. עכשיו נוכיח כי $A \leq_p SAT$.

תהי N מ"ט אי-דטרמיניסטית זמן-פולינומיאלית שמכריעה שפה A כלשהי בזמן $O(n^k)$ עבור k טבעי. התרשים למטה מראה טבלה של קונפיגורציות של N . ברשימה הבאה רשומות ההגדרות של הטבלה:

- כל שורה מראה את תוכן הסרט בשלב מסוים של מסלול אחד של N .
- בשורה הראשונה יש את הקונפיגורציה ההתחלתית.
- אנחנו מניחים כי האורך של המילה, כלומר אורך הקלט הוא n .
- הסימנים w_1, \dots, w_n מסמנים את התווים של הקלט.

- בתא הראשון בכל שורה יש #, ואחר כך רשומה הקונפיגורציה של N . בסוף הקונפיגורציה בכל שורה יש #.
- אחרי ה- # בקצה הימין של המילה, בכל תא יש תו רווח עד הסוף של השורה. התווי רווח לפני המשבצת הראשונה של הקונפיגורציה לא מופיעים בטבלה.
- האורך של כל שורה הוא בדיוק n^k תאים.
- בטבלה יש בדיוק n^k שורות לסיבה הבאה:
 - המכונת טיורינג מבצעת n^k צעדים לכל היותר.
 - בכל צעד המ"ט עוברת לקונפיגורציה חדשה.
 - בכל שורה רשומה קונפיגורציה.
 - בסה"כ יש n^k שורות עבור ה- n^k קונפיגורציות שונות האפשריות.

#	q_0	w_1	w_2	\dots	w_n	\sqsubset	\dots	\sqsubset	#						
#	q_0								#						
#	q_0								#						
				<table><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table>											
#									#						

אנחנו אומרים כי טבלה שלהי היא **טבלה המקבלת** אם באחת השורות יש קונפיגורציה אשר N מקבלת אותה.

בעזרת הטבלה נתאר את הרדוקציה זמן-פולינומיאלית f משפה A כלשהי ל- SAT .

הפונקציה הרדוקציה
 f מקבלת קלט w ומחזירה נוסחה $\phi = f(w)$, אשר לפי ההגדרה של פונקציה הרדוקציה, עומדת בתנאי הבא:

$$w \in A \quad \Leftrightarrow \quad f(w) \in SAT \text{ .}$$

יהיו Q קבוצת המצבים ו- Γ האלפיבית של הסרט של N . נגדיר

$$C = Q \cup \Gamma \cup \{\#\} \text{ .}$$

נסמן ב- s איבר כלשהו של C .

עבור כל תא ה- (i, j) של הטבלת הקונפיגורציות נגדיר משתנה בוליאני $x_{i,j,s}$ לכל $1 \leq i, j \leq n^k$.
המשתנה $x_{i,j,s}$ מוגדר על פי התנאי

$$x_{ijs} = 1$$

אם בתא ה- ij של הטבלה יש $s \in C$. למשל, אם בתא ה- $(2, 5)$ של הטבלה מופיע התו a אז

$$x_{2,5,a} = 1$$

בעוד

$$x_{2,5,b} = 0 .$$

במובן הזה, התכנים של כל התאים של הטבלה מסומנים על ידי המשתנים של ϕ .

עכשיו נבנה נוסחה ϕ על סמך התנאי שהשמה מספקת של ϕ תהיה מתאימה לטבלה המקבלת של N . נגדיר

$$\phi = \phi_{\text{cell}} \wedge \phi_{\text{start}} \wedge \phi_{\text{move}} \wedge \phi_{\text{acc}} . \quad (10.1)$$

אנחנו נסביר את כל הנוסחאות ϕ_{cell} , ϕ_{start} , ϕ_{move} ו- ϕ_{acc} אחד אחד למטה.

• הנוסחה ϕ_{cell}

כפי שמצויין לעיל, אם המשתנה $x_{i,j}$ "דולק", כלומר אם $x_{i,j,s} = 1$, זאת אומרת שיש סימן s בתא ה- ij של הטבלה. אנחנו רוצים להבטיח שהשמה כלשהי בנוסחה אשר מתאימה לקונפיגורציה של הטבלה, מדליקה בדיוק משתנה אחד לכל תא של הטבלה. למטרה זו נגדיר ϕ_{cell} כך:

$$\phi_{\text{cell}} = \bigwedge_{1 \leq i, j \leq n^k} \left[\left(\bigvee_{s \in C} x_{i,j,s} \right) \wedge \left(\bigwedge_{\substack{s, t \in C \\ s \neq t}} (\bar{x}_{i,j,s} \vee \bar{x}_{i,j,t}) \right) \right] \quad (10.2)$$

* האיבר הראשון בסוגריים מרובעים, $\bigvee_{s \in C} x_{i,j,s}$ מבטיח שלכל תא של הטבלה, לפחות משתנה אחד דולק.

* האיבר השני $\bigwedge_{\substack{s, t \in C \\ s \neq t}} (\bar{x}_{i,j,s} \vee \bar{x}_{i,j,t})$ מבטיח שעבור כל תא של הטבלה, משתנה אחד לכל היותר דולק.

לפיכך כל השמה מספקת עומדת בתנאי שיהיה בדיוק סימן אחד, s , בכל תא של הטבלה.

• הנוסחה ϕ_{start}

נוסחה ϕ_{start} מבטיחה ששורה הראשונה של הטבלה היא הקונפיגורציה ההתחלתית של N על הקלט w :

$$\begin{aligned} \phi_{\text{start}} = & x_{1,1,\#} \wedge x_{1,2,q_0} \wedge x_{1,3,w_1} \wedge x_{1,4,w_2} \\ & \wedge \dots \wedge \\ & x_{1,n+2,w_n} \wedge x_{1,n+3,\sqcup} \wedge \dots \wedge x_{1,n^k-1,\sqcup} \wedge x_{1,n^k,\#} \end{aligned} \quad (10.3)$$

• הנוסחה ϕ_{acc}

הנוסחה ϕ_{acc} מבטיחה שקיימת טבלה קונפיגורציה אשר המ"ט N מקבלת אותה.

בפרט ϕ_{acc} מבטיחה שהסימן q_{acc} מופיע בתא אחד של הטבלה דרך התנאי שלפחות אחד המשתנים $x_{i,j,q_{\text{acc}}}$ דולק:

$$\phi_{\text{acc}} = \bigvee_{1 \leq i, j \leq n^k} x_{i,j,q_{\text{acc}}} \quad (10.4)$$

• הנוסחה ϕ_{move}

הנוסחה ϕ_{move} מבטיחה שכל שורה של הטבלה היא "שורה חוקית".

כלומר בכל שורה, הקונפיגורציה היא כך שאפשר להגיע אליה על ידי תזוזה חוקית של N מהקונפיגורציה הקודמת שמופיעה בשורה אחת למעלה.

תזוזה חוקית בין כל שתי קונפיגורציות נקבעת על ידי הפונקציה המעברים של המ"ט N .

בשפה פורמלית, אם c_i הקונפיגורציה של שורה i , ו- c_{i+1} הקונפיגורציה של השורה $i + 1$ אחת למטה, אז ϕ_{move} מבטיחה כי לכל $1 \leq i \leq n^k - 1$ מתקיים

$$c_i \vdash_N c_{i+1}.$$

במונחי הטבלה, אפשר להגדיר תזוזה חוקית בין כל שתי שורות על ידי תת-טבלה מסדר 2×3 שמכילה 3 תאים מתאימים של שתי שורות שכנות.

מכאן ואילך אנחנו נקרא לתת-טבלה כזאת "חלון".

למטה יש דוגמאות של חלונות חוקיים:

a	q ₁	b
q ₂	a	c

a	q ₁	b
a	a	q ₂

a	a	q ₁
a	a	b

#	b	a
#	b	a

a	b	a
a	b	q ₂

b	b	b
c	b	b

החלונות האלה למטה הם דוגמאות לחלונות לא חוקיים:

a	b	a
a	a	a

a	q ₁	b
q ₁	a	a

b	q ₁	b
q ₂	b	q ₂

הנוסחה ϕ_{move} קובעת שכל חלון של הטבלה חוקי. בפרט, כל חלון מכיל 6 תאים. לכן ϕ_{move} קובעת שהתכנים של ה-6 תאים של כל חלון מהווה חלון חוקי. ז"א

$$\phi_{\text{move}} = \bigwedge_{\substack{1 \leq i \leq n^k \\ 1 \leq j \leq n^k}} (\text{חלון ה- } i, j \text{ חוקי}) \quad (10.5)$$

אנחנו מציבים בטקסט "חלון ה- i, j חוקי" את הנוסחה הבאה, כאשר a_1, \dots, a_6 מסמנים את התכנים של ה-6 תאים של כל חלון:

$$\bigvee_{\substack{\{a_1, a_2, a_3, a_4, a_5, a_6\} \\ \text{חלון חוקי}}} (x_{i,j-1,a_1} \wedge x_{i,j,a_2} \wedge x_{i,j+1,a_3} \wedge x_{i+1,j-1,a_4} \wedge x_{i+1,j,a_5} \wedge x_{i+1,j+1,a_6}) \quad (10.6)$$

עד כה הוכחנו שקיים רדוקציה מכל שפה $A \in NP$ ל- SAT . כעת נוכיח כי הרדוקציה זו חישובית בזמן-פולינומיאלי.

הטבלה של N היא מסדר $n^k \times n^k$ ולכן היא מכילה n^{2k} תאים.

נחשב את הסיבוכיות של כל הנוסחאות $\phi_{\text{move}}, \phi_{\text{acc}}, \phi_{\text{start}}, \phi_{\text{cell}}$.

- הנוסחה ϕ_{cell}

הנוסחה (10.2) של ϕ_{cell} מכילה n^{2k} נוסחאות עם 3 ליטרלים. לכן

$$\phi_{\text{cell}} = O(n^{2k}) .$$

- הנוסחה ϕ_{start}

הנוסחה (10.3) של ϕ_{start} מכילה בדיוק n^k ליטרלים. לכן

$$\phi_{\text{start}} = O(n^k) .$$

- הנוסחה ϕ_{acc}

הנוסחה (10.4) של ϕ_{acc} מכילה בדיוק n^k ליטרלים. לכן

$$\phi_{\text{acc}} = O(n^k) .$$

- הנוסחה ϕ_{move}

הנוסחה (10.6,10.5) של ϕ_{move} מכילה n^{2k} נוסחאות עם 6 ליטרלים. לכן

$$\phi_{\text{move}} = O(n^{2k}) .$$

לכן בסה"כ

$$\phi = O(n^{2k}) + O(n^k) + O(n^k) + O(n^{2k}) = O(n^{2k}) .$$

לפיכך קיימת רדוקציה חישובית בזמן פולינומיאלי מכל שפה $A \in NP$ ל- SAT .



שיעור 11

רדוקציות פולינומיליות

11.1 $CLIQUE$ היא NP - שלמה

משפט 11.1 $CLIQUE \in NPC$

הבעיית $CLIQUE$ היא (ראו הגדרה 9.5):

$$CLIQUE = \{ \langle G, k \rangle \mid k \text{ מכיל קליקה בגודל } k \} .$$

$CLIQUE$ היא NP - שלמה

הוכחה:

(1) הוכחנו כי $CLIQUE \in NP$ במשפט 9.2.

(2) נוכיח כי $CLIQUE$ היא NP קשה ע"י רדוקציה $3SAT \leq_P CLIQUE$.

פונקציית הרדוקציה

בהינתן נוסחת $3CNF$ ϕ מעל n משתנים x_1, x_2, \dots, x_n המכיל m פסוקיות, ניצור זוג $\langle G, k \rangle$ ונוכיח כי

$$\langle \phi \rangle \in 3SAT \iff \langle G, k \rangle \in CLIQUE .$$

נבנה את הגרף G באופן הבא:

הקדקודים של G :

לכל פסוקית C_i ב- ϕ המכילה 3 ליטרלים ניצור שלשה t_i המכילה 3 קודקודים המתאימים לליטרלים של C_i :

$$x_1 \vee \bar{x}_3 \vee x_4 \longrightarrow \begin{array}{ccc} \textcircled{x_1} & \textcircled{\bar{x}_3} & \textcircled{x_4} \end{array}$$

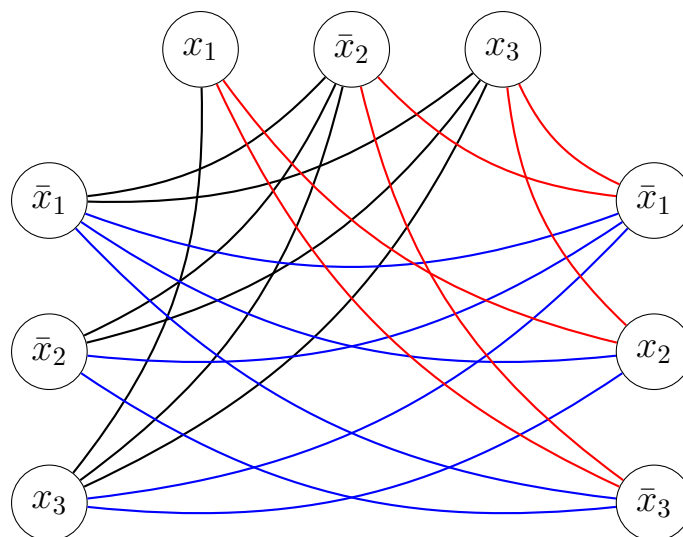
הצלעות של G :

נבחר בין כל שני קודקודים פרט לזוגות הבאים:

- זוג קודקודים המתאימים למשתנה ומשלמים שלו.
- זוג קודקודים שנמצאים באותה שלושה.

לדוגמה:

$$\phi = \underbrace{\left(\overset{T}{x_1} \vee \overset{T}{\bar{x}_2} \vee x_3 \right)}_{C_1} \wedge \underbrace{\left(\bar{x}_1 \vee \overset{T}{\bar{x}_2} \vee x_3 \right)}_{C_2} \wedge \underbrace{\left(\bar{x}_1 \vee x_2 \vee \overset{T}{\bar{x}_3} \right)}_{C_3}$$



נקבע $k = m$.

נכונות הרדוקציה

(1) ניתן לבנות את G בזמן פולינומיאלי בגודל ϕ .

(2) נוכיח כי

$$\langle \phi \rangle \in 3SAT \iff \langle G, k \rangle \in CLIQUE.$$

כיוון \Leftarrow

- נניח כי ϕ ספיקה ונסתכל על השמה המספקת את ϕ .
- בכל פסוקית C_i ב- ϕ יש לפחות ליטרל אחד שקיבל ערך T .
- נבחר מכל שלשה t_i בקודקוד אחד המתאים לליטרל שקיבל ערך T ב- C_i ונוסיף אותו לקליקה.
- מספר הקודקודים שבחרנו שווה k וכל שניים מהם מחוברים בצלע כי לא בחרנו שני קודקודים מאותה שלשה ולא בחרנו שני קודקודים המתאימים למשתנה ומשלים שלו.
- ולכן G מכיל קליקה בגודל k .

כיוון \Rightarrow

- נניח כי G מכיל קליקה בגודל k ונסתכל על קליקה כזו.
- לפי הבנייה הקליקה מכילה בדיוק קודקוד אחד מכל שלשה t_i . ניתן השמה למשתנים של ϕ כך שהליטרל שמתאים לקודקוד שנמצא בקליקה יקבל ערך T .
- השמה זו אפשרית מכיוון שהקליקה לא מכילה שני קודקודים המתאימים למשתנה ומשלים שלו.

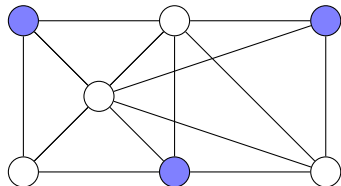
- בנוסף השם ϕ מספקת את ϕ מכיוון שהקליקה מכילה קודקוד מכל שלשה t_i ולכן הליטרל המתאים לקודקוד בשלשה t_i קיבל ערך T ולכן הוא מספק את הפסוקית C_i .
- לכן ϕ ספיקה.

■

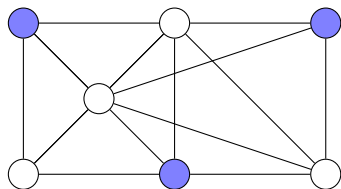
11.2 בעיית הקבוצה הבלתי תלויה

הגדרה 11.1 קבוצה בלתי תלויה

בהינתן גרף לא מכוון $G = (V, E)$, קבוצה בלתי תלויה ב- G היא תת-קבוצה של קודקודים $S \subseteq V$ כך שלכל שני קודקודים $u, v \in S$ מתקיים $(u, v) \notin E$.



קבוצה בלתי תלויה בגודל $k = 3$:



קבוצה בלתי תלויה בגודל $k = 3$:

הגדרה 11.2 בעיית IS

קלט: גרף לא מכוון $G = (V, E)$ ומספר k .
פלט: האם קיימת קבוצה בלתי תלויה ב- G בגודל k ?

$$IS = \{ \langle G, k \rangle \mid k \text{ קבוצה בלתי תלויה בגודל } k \}$$

משפט 11.2 $IS \in NPC$

הבעיה IS היא NP - שלמה.

הוכחה:

(1) נוכיח כי $IS \in NP$

נבנה אלגוריתם אימות עבור IS .
 $V = \langle \langle G, k \rangle, y \rangle$ על קלט

- בודק האם y היא קבוצה של k קודקודים מ- G השונים זה מזה.

○ אם לא \Rightarrow דוחה.

- בודק האם כל שני קודקודים מ- y לא מחוברים בצלע ב- G .

○ אם כן \Rightarrow מקבל.

○ אם לא \Rightarrow דוחה.

(2) נוכיח כי $CLIQUE \leq_P IS$

פונקציית הרדוקציה:

בהינתן זוג $\langle G, k \rangle$ הקלט של $CLIQUE$, ניצור זוג $\langle G', k' \rangle$, הקלט של IS , ונוכיח כי:

$$\langle G, k \rangle \in CLIQUE \Leftrightarrow \langle G', k' \rangle \in IS.$$

הפונקציית הרדוקציה מוגדרת כך שהתנאים הבאים מתקיימים:

(1) נניח שהגרף הוא $G = (V, E)$.

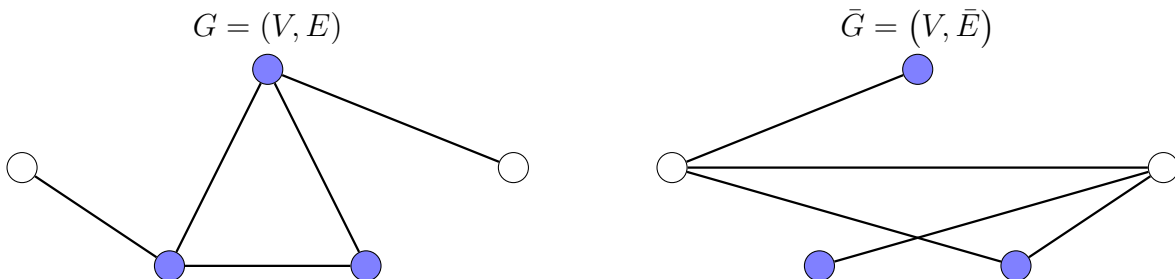
אז הגרף G' הוא הגרף המשלים של $G = (V, E)$.

ז"א $G' = \bar{G} = (V, \bar{E})$ כאשר

$$\bar{E} = \{(u_1, u_2) \mid (u_1, u_2) \notin E\}.$$

(2) $k' = k$.

לדוגמה, בהינתן הגרף $G = (V, E)$ שמכיל קליקה בגודל $k = 3$, הפונקציית הרדוקציה R מחזירה את הגרף $\bar{G} = (V, \bar{E})$ ואת המספר $k' = k = 3$, כמתואר בתרשים למטה:



נכונות הרדוקציה

(1) ניתן לבנות G' בזמן פולינומיאלי בגודל G .

(2) נוכיח כי $\langle G, k \rangle \in CLIQUE \Leftrightarrow \langle G', k' \rangle \in IS$.

כיוון \Leftarrow

בהינתן גרף $G = (V, E)$ ושלם k .

נניח כי $\langle G, k \rangle \in CLIQUE$.

\Leftarrow G מכיל קליקה S בגודל k .

\Leftarrow אם $u_1, u_2 \in S$ (אם u_1, u_2 שני קודקודים בקליקה S) אזי $(u_1, u_2) \in E$.

כלומר, כל שני קודקודים ב- S מחוברים בצלע של G .

\Leftarrow אם $u_1, u_2 \in S$ אזי $(u_1, u_2) \notin \bar{E}$.

כלומר, כל שני קודקודים ב- S לא מחוברים בצלע של המשלים של הגרף \bar{G} , דהיינו G' .

\Leftarrow אותה הקבוצה S היא קבוצה בלתי תלוייה ב- G' בגודל $k' = k$.

$\Leftarrow G' = \bar{G}(V, \bar{E})$ מכיל קבוצה בלתי תלוייה בגודל k' .

$\Leftarrow \langle G', k \rangle \in IS$

\Rightarrow כיוון

בהינתן גרף G' ושלים k' .

נניח כי $\langle G', k' \rangle \in IS$

$\Leftarrow G'$ מכיל קבוצה בלתי תלוייה S בגודל k' .

\Leftarrow אם $u_1, u_2 \in S$ אזי $(u_1, u_2) \notin \bar{E}$.

כלומר, כל שני קדקודים ב- S לא מחוברים בצלע של G' .

\Leftarrow אם $u_1, u_2 \in S$ אזי $(u_1, u_2) \in E$.

כלומר, כל שני קדקודים ב- S מחוברים בצלע של $G(V, E)$.

\Leftarrow אותה הקבוצה S היא קליקה ב- G בגודל $k = k'$.

$\Leftarrow G$ מכיל קליקה בגודל k .

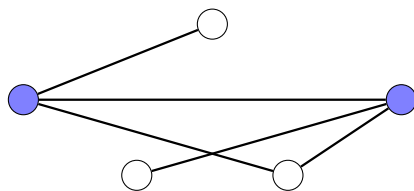
$\Leftarrow \langle G, k \rangle \in CLIQUE$

■

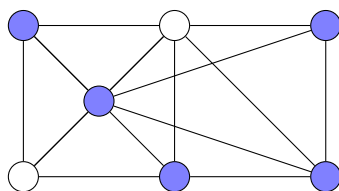
11.3 בעיית הכיסוי בקודקודים

הגדרה 11.3 כיסוי בקודקודים

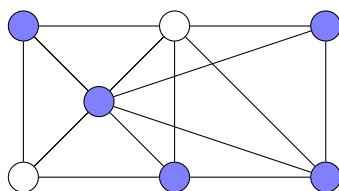
בהינתן גרף לא מכוון $G = (V, E)$, כיסוי בקודקודים ב- G הוא תת-קבוצה של קודקודים $C \subseteq V$ כך שלכל צלע $u, v \in S$ מתקיים $u \in C$ או $v \in C$.



כיסוי בקדקודים בגודל $k = 2$:



כיסוי בקדקודים בגודל $k = 5$:



כיסוי בקדקודים בגודל $k = 5$:

11.4 הבעיה VC

הגדרה 11.4 בעיית VC

קלט: גרף לא מכוון $G = (V, E)$ ומספר k .
פלט: האם קיים כיסוי בקודקודים ב- G בגודל k ?

$$VC = \{ \langle G, k \rangle \mid G \text{ גרף לא מכוון המכיל כיסוי בקודקודים בגודל } k \}$$

משפט 11.3 $VC \in NPC$

הבעיה VC היא NP - שלמה.

הוכחה:

נוכיח כי $VC \in NP$

נבנה אלגוריתם אימות V עבור VC .
 $V = \text{על קלט } \langle G, k \rangle, y$:

• בודק האם כל צלע ב- G מכילה לפחות קצה אחד ב- y .

◦ אם כן \Rightarrow מקבל.

◦ אם לא \Rightarrow דוחה.

נוכיח כי VC היא NP -קשה ע"י רדוקציה $IS \leq_P VC$

פונקציית הרדוקציה:

בהינתן זוג $\langle G, k \rangle$ הקלט של IS , ניצור זוג $\langle G', k' \rangle$ הקלט של VC ונוכיח כי

$$\langle G, k \rangle \in IS \iff \langle G', k' \rangle \in VC.$$

הפונקציית הרדוקציה מוגדרת כך שהתנאים הבאים מתקיימים:

(1) נניח שהגרף הוא $G = (V, E)$.

אז הגרף G' הוא אותו גרף $G = (V, E)$.

(2) $k' = |V| - k$.

נכונות הרדוקציה

(1) ניתן לבנות G' בזמן פולינומיאלי בגודל G .

(2) נוכיח כי $\langle G, k \rangle \in IS \iff \langle G', k' \rangle \in VC$.

כיוון \Leftarrow

בהינתן גרף $G = (V, E)$ ושלם k .

נניח כי $\langle G, k \rangle \in IS$

$\Leftarrow G$ מכיל קבוצה בלתי תלוייה S בגודל k .

\Leftarrow כל שני קדקודים ב- S לא מחוברים בצלע ב- G .

$\Leftarrow V \setminus S$ היא כיסוי קדקודים ב- G בגודל $k' = |V| - k$.

\Leftarrow הגרף $G' = G$ מכיל כיסוי קדקודים בגודל k' .

$\Leftarrow \langle G', k' \rangle \in VC$

\Rightarrow כיוון

בהינתן גרף G' ושלים k' .

נניח כי $\langle G', k' \rangle \in VC$

$\Leftarrow G'$ מכיל כיסוי קדקודים C בגודל k' .

\Leftarrow כל שני קדקודים ב- $V \setminus C$ לא מחוברים בצלע ב- G' .

$\Leftarrow V \setminus C$ הוא קבוצת בלתי תלוייה ב- G' בגודל $k = |V| - k'$.

\Leftarrow הגרף $G = G'$ מכיל קבוצה בלתי תלוייה בגודל k .

■

11.5 PARTITION

הגדרה 11.5 בעיית PARTITION

קלט: קבוצת מספרים שלמים $S = \{x_1, x_2, \dots, x_n\}$
 פלט: האם קיימת תת-קבוצה $Y \subseteq S$ כך ש- $\sum_{y \in Y} y = \sum_{y \in S \setminus Y} y$?

$$PARTITION = \left\{ S \mid \sum_{y \in Y} y = \sum_{y \in S \setminus Y} y \text{ כך ש-} Y \subseteq S \text{ וקיימת תת-קבוצה } Y \subseteq S \right\}$$

11.6 רדוקציות פולינומיאליות

משפט 11.4 רדוקציות פולינומיאליות

$$\begin{aligned} SAT &\leq_P 3SAT \\ 3SAT &\leq_P CLIQUE \\ CLIQUE &\leq_P IS \\ IS &\leq_P VC \\ SubSetSum &\leq_P PARTITION \\ HAMPATH &\leq_P HAMCYCLE \end{aligned}$$

11.7 שפות NP שלמות

משפט 11.5 שפות NP - שלמות

(משפט קוק לויין)	NP - שלמה.	SAT
	NP - שלמה.	$3SAT$
	NP - שלמה.	$HAMPATH$
	NP - שלמה.	$CLIQUE$
	NP - שלמה.	IS
	NP - שלמה.	VC