תוכן העניינים

חישוביות וסיבוכיות | דף נוסחאות למבחן | סמסטר א, תשפ"ו'

1 מכונות טיורינג

הגדרה 1: מכונת טיורינג

מכונת טיורינג (מ"ט) היא שביעיה $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\mathsf{acc}}, q_{\mathsf{rej}})$ כאשר:

Q	קבוצת מצבים סופית ולא ריקה	
Σ	א"ב הקלט סופי	$\sqcup \notin \Sigma$
Γ	א"ב הסרט סופי	$\Sigma \cup \{\sqcup\} \subseteq \Gamma$
δ	פונקציית המעברים	$\delta : (Q \backslash \{q_{\mathsf{rej}}, q_{\mathsf{acc}}\} \times \Gamma \to Q \times \Gamma \times \{L, R\}$
q_0	מצב התחלתי.	
q_{acc}	מצב מקבל יחיד.	
q_{rej}	מצב דוחה יחיד.	

הגדרה 2: קונפיגורציה

בהינתן מכונת טיורינג M ומילה $w \in \Sigma^*$. **קונפיגורציה** בריצה של M על w היא שלושה (u, q, v) (או $uq\mathsf{v}$ לשם קיצור) כאשר:

- $u \in \Sigma^*$: המילה מתחילת הסרט עד (לא כולל) התו שמתחת לראש.
- $\mathsf{v} \in \Sigma^*$: המילה שמתחילה מהתו שמתחת לראש ועד (לא כולל) ה- $\sqcup$ הראשון.

הגדרה 3: גרירה בצעד אחד

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\mathsf{acc}}, q_{\mathsf{rej}})$ מכונת טיורינג, ותהיינה 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.

הגדרה 4: גרירה בכללי

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\mathsf{acc}}, q_{\mathsf{rej}})$ מכונת טיורינג, ותהיינה 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.

הגדרה 5: קבלה ודחייה של מילה

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\mathsf{acc}}, q_{\mathsf{rej}})$ מכונת טיורינג, ו- $w \in \Sigma^*$ מחרוזת. אומרים כי

- M **מקבלת** את w אם $q_0 w \vdash_M^* u\, q_{\mathsf{acc}}\, \mathsf{v}$
- M **דוחה** את w אם $q_0 w \vdash_M^* u\, q_{\mathsf{rej}}\, \mathsf{v}$

עבור $u, \mathsf{v} \in \Gamma^*$ כלשהם.

הגדרה 6: הכרעה של שפה

תהי $M = (Q, \Sigma, \Gamma, \delta, q_0, \mathsf{acc}, q_{\mathsf{rej}})$ מכונת טיורינג, ו- $L \subseteq \Sigma^*$ שפה. אומרים כי M **מכריעה** את L אם לכל $w \in \Sigma^*$ מתקיים

- $w \in L \Leftarrow M$ מקבלת את w.

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

הגדרה 7: 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- $L(M)=L$.

הגדרה 8: מכונת טיורינג שמחשבת פונקציה f
תהי $f:\Sigma_1^*\to\Sigma_2^*$ ותהי $M=(Q,\Sigma,\Gamma,\delta,q_0,q_{\text{acc}},q_{\text{rej}})$ מכונת טיורינג. אומרים כי M מחשבת את f אם:
- $\Sigma=\Sigma_1$ ו- $\Sigma_2\subset\Gamma$.
- לכל $w\in\Sigma_1^*$ מתקיים $q_0 w\vdash q_{\text{acc}} f(w)$.

2 וריאציות של מכונות טיורינג

הגדרה 9: מודל חישוב
מודל חישובי = אוסף של מכונות שעבורם מוגדרים המושגים של הכרעה וקבלה של שפות.

הגדרה 10: מודלים שקולים חישובית
יהיו A,B מודלים חישוביים. נאמר כי A ו- B שקולים אם לכל שפה L:
- קיימת מכונה במודל A שמכריעה את L אם"ם קיימת מכונה כזו במודל B.
- קיימת מכונה במודל A שמקבלת את L אם"ם קיימת מכונה כזו במודל B.

הגדרה 11: מכונות שקולות חישובית
שתי מכונות הן שקולות חישובית אם הן מקבלות ודוחות בדיוק את אותן המילים.

משפט 1: מכונת טיורינג עם סרט ימינה בלבד
מודל מ"ט עם סרט אינסופי לכיוון אחד בלבד (מודל O) שקול למודל אינסופי בשני הכיוונים (מודל T).
כלומר, לכל שפה L:
- יש מ"ט ממודל O שמקבלת את L אם"ם יש מ"ט במודל T שמקבלת את L.
- יש מ"ט ממודל O שמכריעה את L אם"ם יש מ"ט במודל T שמכריעה את L.

משפט 2: מכונת טיורינג מרובת סרטים
במכונת טיורינג מרובת סרטים:
- יתכנו מספר סרטים.
- מספר הסרטים סופי וקבוע מראש בזמן בניית המ"ט, ואינו תלוי בקלט או במהלך החישוב.
- לכל סרט יש ראש נפרד.

- הפעולות (תנועה וכתיבה) בכל סרט נעשית בנפרד.
בפרט, הראשים יכולים לזוז בכיוונים שונים בסרטים שונים.
- ישנו בקר מרכזי יחיד, שקובע את הפעולות בכל אחד מהסרטים, על סמך המידע שמתקבל מכל הסרטים.
לכן, תוכן סרט אחד יכול להשפיע על הפעולות בשאר הסרטים.
- בתחילת החישוב, הקלט נמצא בסרט הראשון ושאר הסרטים ריקים.

משפט 3: מ"ט מרובת סרטים שקולה למ"ט עם סרט יחיד
לכל k, המודל של מ"ט עם k סרטים שקול חישובי למודל של מ"ט עם סרט אחד.

משפט 4: קבלה ודחייה של מילה ע"י מ"ט אי-דטרמיניסטית
עבור מ"ט לא דטרמיניסטית N ומילה w:
- N **מקבלת** את w אם קיים חישוב של N על w שמגיע למצב מקבל.
- N **דוחה** את w אם כל החישובים של N על w עוצרים במצב דוחה.

משפט 5: קבלה ודחייה של שפה ע"י מ"ט אי-דטרמיניסטית
נתון מ"ט לא דטרמיניסטית N ושפה L:
- N **מכריעה** את L אם N מקבלת את כל המילים ב- L ודוחה את כל המילים שאינן ב- L.
- N **מקבלת** את L אם N מקבלת את כל המילים ב- L ולא מקבלת את כל המילים שאינן ב- L.

משפט 6: מ"ט אי-דטרמיניסטית שקולה למ"ט דטרמיניסטית
לכל מ"ט לא דטרמיניסטית קיימת מ"ט דטרמיניסטית שקולה.

הגדרה 12: מכונת טיורינג אי-דטרמיניסטית
מכונת טיורינג אי-דטרמיניסטית (מ"ט א"ד) היא שביעייה

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

כאשר $Q,\Sigma,\Gamma,q_0,q_{\text{acc}},q_{\text{rej}}$ מוגדרים כמו במ"ט דטרמיניסטי (ראו הגדרה 1).
Δ היא פונקציית המעברים

$$\Delta:(Q\backslash\{q_{\text{acc}},q_{\text{rej}}\})\times\Gamma\to P\left(Q\times\Gamma\times\{L,R,S\}\right)\ .$$

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

כלומר, לכל זוג $q\in Q,\alpha\in\Gamma$ 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.

הגדרה 13: קבלה ודחייה של מילה ושפה של מכונת טיורינג אי דטרמיניסטית

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

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

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 14: מ"ט אי דטרמיניסטית המכריעה שפה L

אומרים כי מ"ט אי דטרמיניסטית M מכריעה שפה L אם לכל $w \in \Sigma^*$:

- אם $w \in L \Leftarrow M$ מקבלת את w.
- אם $w \notin L \Leftarrow M$ דוחה את w.

הגדרה 15: מ"ט א"ד המקבלת שפה L

אומרים כי מ"ט אי דטרמיניסטית M מקבלת שפה L אם לכל $w \in \Sigma^*$:

- אם $w \in L \Leftarrow M$ מקבלת את w.
- אם $w \notin L \Leftarrow M$ דוחה את w או M לא עוצרת על w.

משפט 7: 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.

3 התזה של צ'רץ'-טיורינג

שמות נרדפים לשפות כריעות ושפות קבילות

שפות כריעות	Decideable languages	שפות קבילות	Acceptable languages
שפות רקורסיביות	Recursive languages	שפות ניתנות לזיהוי	recognizable languages
		שפות כריעות למחצה	Semi-deidable languages
			Partially-deidable languages
		שפות הניתנות למנייה רקורסיביות	Recursively enumerable languages.

משפט 8: סגירות שפות כריעות

השפות הכריעות סגורות תחת:

- איחוד
- חיתוך
- משלים
- שרשור
- סגור קליין

משפט 9: סגירות שפות קבילות

- איחוד
- חיתוך
- שרשור
- סגור קליין

משפט 10: היחס בין הכרעה לקבלה

עבור כל שפה L התנאים הבאים מתקיימים.

- אם L הינה כריעה אז היא קבילה. כלומר:

$$L \in R \quad \Rightarrow \quad L \in RE \ .$$

- אם השפה L קבילה וגם המשלים שלה $\bar{L}$ קבילה אז L כריעה. כלומר:

$$L \in RE \wedge \bar{L} \in RE \quad \Rightarrow \quad L \in R \ .$$

הגדרה 16: שפת סימפל

<u>משתנים</u>

- טבעיים: `i,j,k,...`
  מקבלים כערך מספר טבעי.
- מערכים: `A[],B[],C[],...` בכל תא ערך מתוך א"ב Γ אין סופיים.
- אתחול: הקלט נמצא בתאים הראשונים של `A[]`.
  כל שאר המשתנים מאותחלים ל- `0`.

<u>פעולות</u>

- השמה בקבוע:

`i=3, B[i]="#"`
- השמה בין משתנים:

`i=k, A[k]=B[i]`
- פעולות חשבון:

`x = y + z , x = y − z , x = y.z`

תנאים
- `B[i]==A[j]`
(מערכים).
- `x >= y`
(משתנים טבעיים).

כל משתנה מופיע רק פעם אחת בכל פעולה או תנאי.

זרימה
- סדרה פקודות ממוספרות.
- `goto`: מותנה ולא מותנה.
- `stop` עצירה עם ערך חזרה.

```
one = 1
zero = 0
B[zero] = "0"
i=0
j=i
if A[i] == B[zero] goto 9
i=j + one
goto 3
C[one] = A[j]
if C[one] ==  A[zero] goto 12
stop(0)
stop(1)
```

הגדרה 17: קבלה ודחייה של מחרוזות בשפה SIMPLE
עבור קלט w ותוכנית P בשפת SIMPLE. נאמר כי
- P **מקבלת** את w אם הריצה של P על w עוצרת עם ערך חזרה 1.
- P **דוחה** את w אם הריצה של P על w עוצרת עם ערך חזרה 0.

הגדרה 18: הכרעה וקבלה של שפות
עבור שפה L ותוכנית P בשפת SIMPLE. נאמר כי
- P **מכריעה** את L אם היא מקבלת את המילים שב- L ודוחה את אלה שלא ב- L.
- P **מקבלת** את L אם היא מקבלת את כל ורק המילים ב- L.

משפט 11: שפת SIMPLE שקולה למכונת טיורינג
המודלים של מכונת טיורינג ותוכניות SIMPLE שקולים.

משפט 12: מ"ט ותוכניות מחשב
מ"ט חזקה לפחות כמו תוכנית משחב.
כל תוכנית מחשב ניתנת למימוש במ"ט.
לכן, כל שפה שהינה כריעה ע"י מחשב היא כם כריעה ע"י מ"ט.
וכמו כן, שפה שהינה קבילה ע"י מחשב היא גם קבילה ע"י מ"ט.

הגדרה 19: דקדוקים כלליים
בדקדוק כללי, בצד שמאל של כל יצירה יכולה להופיע מחרוזת (לא ריקה) כלשהי.
פורמלית, כלל יצירה בדקדוק כללי הוא מהצורה

$$\gamma \to u$$

כאשר $\gamma \in (V \cup \Sigma)^+$, $u \in (V \cup \Sigma)^*$.

משפט 13:
תהי L שפה. L קבילה אם"ם קיים דקדוק כללי G כך ש- $L(G) = L$.

משפחת שפות	דקדוק	מודל חישובי
קבילות	כללי	מכונת טיורינג
חסרות הקשר	חסר הקשר	אוטומט מחסנית
רגולריות	רגולרי	אוטומט סופי

משפט 14:
כל שפה חסרת הקשר הינה כריעה.

משפט 15: התזה של צ'רץ' טיורינג
התזה של צ'רץ' טיורינג מודל מ"ט מגלם את המושג האבסטרקרטי של "אלגוריתם".
כלומר, כל אלגוריתם שניתן לתיאור כתהליך מכניסטי שבו:
- התהליך מתבצע כסדרה של צעדים.
- כל צעד מצריך כמות סופית של "עבודה".

ניתן גם לתיאור כמ"ט.
בפרט, אין מודל מכניסטי / אוטומטי יותר ממ"ט.

הגדרה 20: מודלים שקולים חישובית

יהיו A ו- B מודלים חישוביים. אומרים כי A ו- B שקולים אם לכל שפה L 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.

הגדרה 21: מכונת טיורינג מרובת סרטים

מכונת טיורינג מרובת סרטים היא שביעייה:

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

כאשר Q, Σ, Γ, q_0, q_{acc}, q_{rej} מוגדרים כמו מ"ט עם סרט יחיד (ראו הגדרה 1).
ההבדל היחיד בין מ"ט עם סרט יחיד לבין מטמ"ס הוא הפונקציית המעברים. עבור מטמ"ס הפונקצית המעברים היא מצורה הבאה:

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

הקונפיגורציה של מכונת טיורינג מרובת סרטים מסומנת $(u_1 q\ \mathsf{v}_1\ ,\ u_2 q\ \mathsf{v}_2\ ,\ \dots\ ,\ u_k q\ \mathsf{v}_k\ .)$

משפט 16: שקילות בין מ"ט מרובת סרטים 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 $\Leftarrow$ M' מקבלת את w.
- אם M דוחה את w $\Leftarrow$ M' דוחה את w.
- אם M לא עוצרת על w $\Leftarrow$ M' לא עוצרת על w.

4 אי-כריעות

משפט 17: סיווג שפות ידועות - חישוביות

$L_{\text{acc}} = \{\langle M, w\rangle | w \in L(M)\}$ $\in RE \backslash R$

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

$L_M = \{\langle M\rangle \ ||$ M המקבלת את $\langle M\rangle$ $\}$ $\in RE \backslash R$

$L_{\text{d}} = \{\langle M\rangle | \langle M\rangle \notin L(M)\}$ $\in CoRE \backslash R$

$L_E = \{\langle M\rangle | L(M) = \varnothing\}$ $\in CoRE \backslash R$

$L_{EQ} = \{\langle M_1, M_2\rangle | L(M_1) = L(M_2)\}$ $\notin RE \backslash R, \notin CoRE \backslash R$

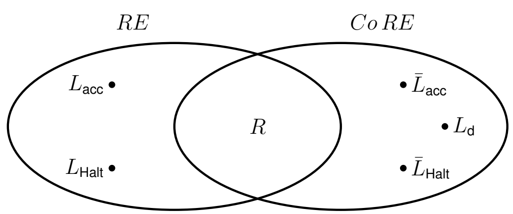
$L_{REG} = \{\langle M\rangle |$ $L(M)$ רגולרית $\}$ $\notin RE \backslash R, \notin CoRE \backslash R$

$L_{NOTREG} = \{\langle M\rangle |$ $L(M)$ לא רגולרית $\}$ $\notin RE \backslash R, \notin CoRE \backslash R$

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

משפט 18:

$$L_{\text{acc}} \in RE \backslash R \quad \Rightarrow \quad \bar{L}_{\text{acc}} \notin RE\ ,$$
$$L_{\text{halt}} \in RE \backslash R \quad \Rightarrow \quad \bar{L}_{\text{halt}} \notin RE\ ,$$
$$L_{\text{d}} \notin RE \backslash R\ .$$



5 המחלקות החישוביות R, RE ו- $CoRE$ ותכונותן

הגדרה 22: כוכב קליני

בהינתן השפה L. השפה L^* מוגדרת:

$$L^* = \{\varepsilon\} \cup \{w = w_1 w_2 \cdots w_k \ \big|\ \forall\ 1 \leqslant i \leqslant k\ ,\ w_i \in L\}$$

הגדרה 23:

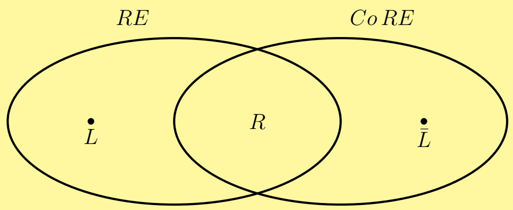
- אוסף השפות הכריעות מסומן R ומוגדר $R = \{L \subseteq \Sigma^* \mid L \text{ קיימת מ"ט המכריעה את}\}$.
- אוסף השפות הקבילות מסומן R ומוגדר $RE = \{L \subseteq \Sigma^* \mid L \text{ קיימת מ"ט המקבלת את}\}$.
- אוסף השפות שהמשלימה שלהן קבילה מסומן R ומוגדר $Co\,RE = \{L \subseteq \Sigma^* \mid \bar{L} \in RE\}$.

משפט 19: סגירות של השפות הכריעות והשפות הקבילות

- R סגורה תחת: **1)** איחוד **2)** חיתוך **3)** שרשור **4)** סגור קלין **5)** משלים.
- RE סגורה תחת: **1)** איחוד **2)** חיתוך **3)** שרשור **4)** סגור קלין.

משפט 20: תכונות של השפות החישוביות

1. אם $L \in RE$ וגם $\bar{L} \in RE$ אזי $L \in R$.
2. אם $L \in RE \backslash R$ אזי $\bar{L} \notin RE$ (כי $\bar{L} \in Co\,RE \backslash R$).
3. $RE \cap Co\,RE = R$.



הגדרה 24: מכונת טיורינג אוניברסלית

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

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

6 רדוקציות

הגדרה 25: מ"ט המחשבת פונקציה

בהינתן פונקציה $f : \Sigma^* \to \Sigma^*$ 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 $f(x)$.

הגדרה 26: מ"ט המחשבת פונקציה

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

הגדרה 27: רדוקציה

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

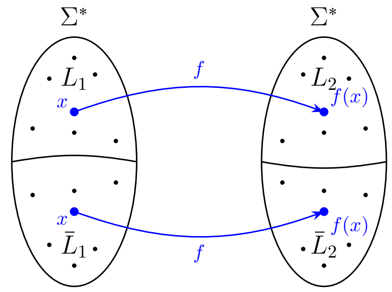
$$L_1 \leqslant L_2 \ ,$$

אם קיימת פונקציה $f : \Sigma^* \to \Sigma^*$ המקיימת:

1) f חשיבה

2) לכל $x \in \Sigma^*$:

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



משפט 21: משפט הרדוקציה

לכל שתי שפות $L_1, L_2 \subseteq \Sigma^*$, אם קיימת רדוקציה $L_1 \leqslant L_2$ אזי

$$\begin{aligned}
L_1 \in R &\quad \Leftarrow \quad L_2 \in R \\
L_1 \in RE &\quad \Leftarrow \quad L_2 \in RE \\
L_1 \notin R &\quad \Rightarrow \quad L_2 \notin R \\
L_1 \notin RE &\quad \Rightarrow \quad L_2 \notin RE
\end{aligned}$$

משפט 22: תכונות של רדוקציה

- לכל שפה L מתקיים: $L \leqslant L$.
- אם $L_1 \leqslant L_2$ אזי $\bar{L}_1 \leqslant \bar{L}_2$.
- אם $L_1 \leqslant L_2$ וגם $L_2 \leqslant L_3$ אזי $L_1 \leqslant L_3$.
- לכל $L \in R$ ולכל L' שאינה $\varnothing, \Sigma^*$ מתקיים $L \leqslant L'$.

משפט 23: משפט רייס

עבור כל תכונה S של שפות שאינה טריויאלית מתקיים: $L_S \notin R$

- תכונה S לא טריויאלית היא קבוצה של שפות ב RE כך ש $S \neq RE$ וגם $S \neq \varnothing$.
- $L_S = \{\langle M \rangle \mid L(M) = S\}$.

7 סיבוכיות

הגדרה 28: סיבוכיות זמן של מ"ט
סיבוכיות זמן של מכונת טיורינג (או אלגוריתם) M היא פונקציה $f(|w|)$ שווה למספר צעדים לכל היותר ש- M מבצעת בחישוב של M על הקלט w.

משפט 24: קשר בין סיבוכיות של מ"ט מרובת סרטים ומ"ט סרט יחיד
לכל מ"ט מרובת סרטים M הרצה בזמן $f(n)$, קיימת מ"ט סרט יחיד M' השקולה ל- M ורצה בזמן $O\left(f^2(n)\right)$.

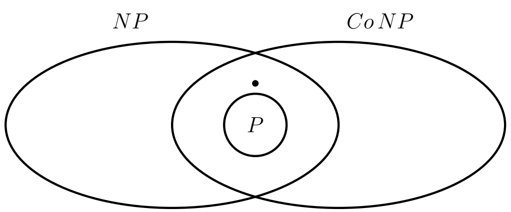
משפט 25: קשר בין סיבוכיות של מ"ט אי-דטרמיניסטית ומ"ט דטרמיניסטית
לכל מ"ט א"ד N הרצה בזמן $f(n)$, קיימת מ"ט דטרמיניסטית D השקולה ל- N ורצה בזמן $2^{(f(n))}$.

הגדרה 29: אלגוריתם אימות
אלגוריתם אימות עבור בעייה A הוא אלגוריתם V כך שלכל קלט $w\in\Sigma^*$ מתקיים:
$w\in A$ אם ורק אם קיימת מילה y באורך פולינומיאלי ב- $|w|$ כך ש- V מקבל את הזוג (w,y). כלומר:
- אם $w\in A$ $\Leftarrow$ קיים $y\in\Sigma^*$ כך ש- $V(w,y)=T$.
- אם $w\notin A$ $\Leftarrow$ לכל $y\in\Sigma^*$ מתקיים $V(w,y)=F$.

הגדרה 30: המחלקות P ו- NP
- P = קבוצת כל השפות שיש להן מ"ט דטרמיניסטית המכריעה אותן בזמן פולינומי.
- NP = קבוצת כל השפות שיש להן אלגוריתם אימות המאמת אותן בזמן פולינומי.

הגדרה שקולה:
- NP = קבוצת כל השפות שיש להן מ"ט אי-דטרמיניסטית המכריעה אותן בזמן פולינומי.
- $CoNP$ = קבוצת כל השפות שהמשלימה שלהן שייכת ל- NP $\quad CoNP=\left\{A \mid \bar{A}\in NP\ .\right\}$

משפט 26: תכונות של P ו- NP
- $P\subseteq NP$.
- P סגורה תחת משלים: אם $A\in P$ אזי גם $\bar{A}\in P$.
- $P\subseteq NP\cap CoNP$.



8 רדוקציה פולינומיאלית

הגדרה 31: פונקציה פולינומיאלית
בהינתן פונקציה $f:\Sigma^*\to\Sigma^*$. אומרים כי f חשיבה בזמן פולינומיאלי אם קיים אלגוריתם (מ"ט דטרמיניסטית) המחשב את f בזמן פולינומיאלי.

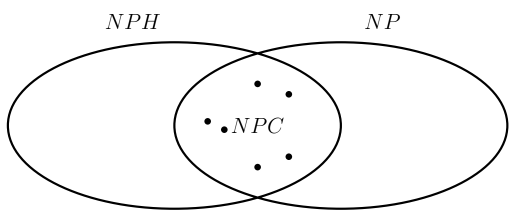
הגדרה 32: רדוקציה פולינומיאלית
בהינתן שתי הבעיות A ו- B. אומרים כי A ניתנת לרדוקציה פולינומיאלית ל- B, ומסמנים $A\leqslant_P B$, אם קיימת פונקציה $f:\Sigma^*\to\Sigma^*$ המקיימת:
1) f חשיבה בזמן פולינומיאלי
2) לכל $w\in\Sigma^*$:
$$w\in A \quad\Leftrightarrow\quad f(w)\in B\ .$$

משפט 27: משפט הרדוקציה
לכל שתי בעיות A ו- B, אם $A\leqslant_P B$ אזי
$$\begin{aligned} A\in P &\Leftarrow B\in P\\ A\in NP &\Leftarrow B\in NP\\ A\notin P &\Rightarrow B\notin P\\ A\notin NP &\Rightarrow B\notin NP \end{aligned}$$

9 שלמות NP

הגדרה 33: NP - קשה (NP-hard)
בעייה B נקראת NP קשה אם לכל בעייה $A\in NP$ קיימת רדוקציה $A\leqslant_P B$.

הגדרה 34: NP-שלמה (NP-complete)
בעייה B נקראת NP שלמה אם
1) $B\in NP$
2) לכל בעייה $A\in NP$ קיימת רדוקציה $A\leqslant_p B$.



משפט 28: תכונות של רדוקציה פולינומיאלית
- אם קיימת שפה $B \in NPC$ (NP שלמה) וגם $B \in P$ אזי $P = NP$.
- אם $A \leqslant_P B$ אזי $\bar{A} \leqslant_P \bar{B}$.
- אם $A \leqslant_p B$ וגם $B \leqslant_p C$ אזי $A \leqslant_p C$.
- לכל $A \in P$ ולכל B שאינה $\emptyset, \Sigma^*$ מתקיים $A \leqslant_P B$.

משפט 29: טרנזיטיביות של NP- שלמות
תהי B בעייה NP- שלמה. אזי לכל בעייה $C \in NP$, אם $B \leqslant_p C$ אזי גם C היא NP שלמה.

10 בעיית הספיקות (SAT)

הגדרה 35: נוסחת CNF
נוסחת CNF, ϕ היא נוסחה בוליאנית מעל n משתנים $x_1, x_2, \ldots, x_n$ המכילה m פסוקיות $C_1, C_2, \ldots, C_m$, כאשר כל פסוקית מכילה אוסף של ליטרלים ($x_i \backslash \bar{x}_i$) המחוברים ע"י OR ($\vee$) בוליאני והפסוקיות מחוברות ע"י AND ($\wedge$) בוליאני. לדוגמה:
$$\phi = \left(\overset{C_1}{x_1 \vee \bar{x}_2 \vee x_4 \vee \bar{x}_7}\right) \wedge \left(\overset{C_2}{x_3 \vee x_5 \vee \bar{x}_8}\right) \wedge \quad \cdots$$

הגדרה 36: נוסחת $3CNF$
נוסחת $3CNF$, ϕ היא נוסחה CNF שבה בכל פסוקית יש בדיוק שלוש ליטרלים. לדוגמה:
$$\phi = \left(\overset{C_1}{x_1 \vee \bar{x}_2 \vee x_4}\right) \wedge \left(\overset{C_2}{x_3 \vee x_5 \vee \bar{x}_8}\right) \wedge \quad \cdots$$

הגדרה 37: נוסחת CNF ספיקה
נוסחת CNF, ϕ היא ספיקה אם קימת השמה למשתנים $x_1, x_2, \ldots, x_n$ ע"י $T \backslash F$ כך ש- ϕ מקבלת ערך T, כלומר בכל פסוקית ישנו לפחות ליטרל אחד שקיבל ערך T.

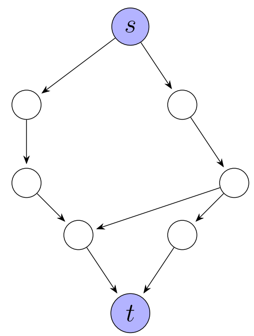
הגדרה 38: בעיית SAT
קלט: נוסחת CNF, ϕ.
פלט: האם ϕ ספיקה?
$$SAT = \{\langle\phi\rangle \mid \phi \text{ נוסחת } CNF \text{ ספיקה}\}$$

הגדרה 39: בעיית $3SAT$
קלט: נוסחת $3CNF$ ϕ.
פלט: האם ϕ ספיקה?
$$3SAT = \{\langle\phi\rangle \mid \phi \text{ נוסחת } 3CNF \text{ ספיקה}\}$$

משפט 30:
- $SAT \in NP$.
- **משפט קוק לוין:** $SAT \in NPC$.
- $3SAT \in NPC$.
- $P = NP \Leftrightarrow SAT \in P$.

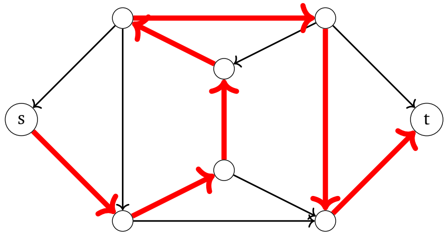
11 סיווג שפות ידיועות - סיבוכיות

הגדרה 40: בעיית מסלול $PATH$
קלט: גרף מכוון G ושני קודקודים s ו- t.
פלט: האם G מכיל מסלול מקודקוד s לקודקוד t.
$$PATH = \{\langle G,s,t\rangle \mid G \text{ גרף מכוון המכיל מסלול מ- } s \text{ ל- } t\}$$



הגדרה 41: בעיית $RELPRIME$
קלט: שני מספרים x ו- y.
פלט: האם x ו- y זרים?
$$RELPRIME = \{\langle x,y\rangle \mid \gcd(x,y) = 1\} \ .$$

הגדרה 42: מסלול המילטוני
בהינתן גרף מכוון $G = (V,E)$ ושני קודקודים $s,t \in V$. מסלול המילטוני מ- s ל- t הוא מסלול מ- s ל- t שעובר דרך כל קודקוד ב-G בדיוק פעם אחת.



הגדרה 43: בעיית מסלול המילטוני - $HAMPATH$

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

<u>פלט</u>: האם G מכיל מסלול המילטוני מ- s ל- t?

$$HAMPATH = \{\langle G,s,t\rangle \mid G \text{ גרף מכוון המכיל מסלול המילטוני מ- } s \text{ ל- } t?\}$$

הגדרה 44: מעגל המילטוני

בהינתן גרף מכוון $G=(V,E)$.

מעגל המילטוני הוא מסלול מעגלי שעובר כל קודקוד ב- G בדיוק פעם אחת.

הגדרה 45: בעיית מעגל המילטוני - $HAMCYCLE$

<u>קלט</u>: גרף מכוון $G=(V,E)$.

<u>פלט</u>: האם G מכיל מעגל המילטוני?

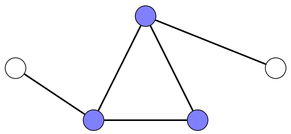
$$HAMCYCLE = \{\langle G\rangle \mid G \text{ גרף מכוון המכיל מעגל המילטוני.}\}$$

הגדרה 46: קליקה

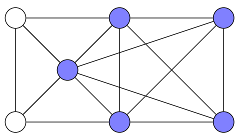
בהינתן גרף לא מכוון $G=(V,E)$.

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 47: בעיית הקליקה - $CLIQUE$

<u>קלט</u>: גרף לא מכוון $G=(V,E)$ ומספר k.

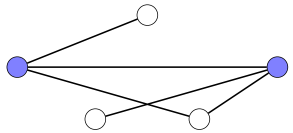
<u>פלט</u>: האם G קליקה בגודל k?

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

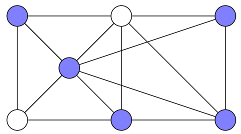
הגדרה 48: כיסוי בקודקודים

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 $v\in C$.

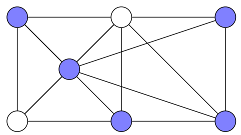
כיסוי בקודקודים בגודל $k=2$:



כיסוי בקודקודים בגודל $k=5$:



כיסוי בקודקודים בגודל $k=5$:



הגדרה 49: בעיית VC

<u>קלט</u>: גרף לא מכוון $G=(V,E)$ ומספר k.

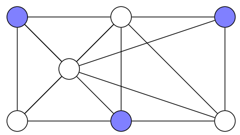
<u>פלט</u>: האם קיים כיסוי בקודקודים ב- G בגודל k?

$$VC = \{\langle G,k\rangle \mid G \text{ גרף לא מכוון המכיל כיסוי בקודקודים בגודל } k\}$$

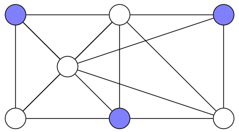
הגדרה 50: קבוצה בלתי תלויה

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 תלוייה בגודל $k=3$:



קבוצה בלתי תלויה בגודל $k=3$:



הגדרה 51: בעיית IS

קלט: גרף לא מכוון $G=(V,E)$ ומספר k.

פלט: האם קיימת קבוצה בלתי תלויה ב- G בגודל k?

$IS=\{\langle G,k\rangle \mid$ G גרף לא מכוון המכיל קבוצה בלתי תלויה בגודל k $\}$

הגדרה 52: בעיית $PARTITION$

קלט: קבוצת מספרים שלמים $S=\{x_1,x_2,\ldots,x_n\}$.

פלט: האם קיימת תת-קבוצה $Y\subseteq S$ כך ש- $\sum\limits_{y\in Y} y=\sum\limits_{y\in S\setminus Y} y$?

$PARTITION=\left\{S \,\middle|\right.$ S קבוצת שלמים, וקיימת תת-קבוצה $Y\subseteq S$ כך ש- $\left.\sum\limits_{y\in Y} y=\sum\limits_{y\in S\setminus Y} y\right\}$

הגדרה 53: בעיית $SubSetSum$

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

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

$SubSetSum=\left\{\langle S,t\rangle \,\middle|\right.$ קיימת $Y\subseteq S$ כך ש- $\left.\sum\limits_{x\in Y} x=t\right\}$

משפט 31:

$PATH=\{\langle G,s,t\rangle \mid$ G גרף מכוון המכיל מסלול מ- s ל- t $\}$ $\in P$

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

$SAT=\{\langle\phi\rangle \mid$ ϕ היא נוסחת CNF ספיקה $\}$ $\in NP, \in NPC$

$3SAT=\{\langle\phi\rangle \mid$ ϕ היא נוסחת $3CNF$ ספיקה $\}$ $\in NP, \in NPC$

$IS=\{\langle G,k\rangle \mid$ G גרף לא מכוון המכיל קליקה בגודל k $\}$ $\in NP, \in NPC$

$CLIQUE=\{\langle G,k\rangle \mid$ G גרף לא מכוון המכיל קליקה בגודל k $\}$ $\in NP, \in NPC$

$VC=\{\langle G,k\rangle \mid$ G גרף לא מכוון המכיל כיסוי בקודקודים בגודל k $\}$ $\in NP, \in NPC$

$HAMPATH=\{\langle G,s,t\rangle \mid$ G גרף מכוון המכיל מסלול המילטוני מ- s ל- t $\}$ $\in NP, \in NPC$

$HAMCYCLE=\{\langle G\rangle \mid$ G גרף מכוון המכיל מעגל המילטוני $\}$ $\in NP$

$SubSetSum=\left\{\langle S,t\rangle \,\middle|\right.$ קיימת $Y\subseteq S$ כך ש- $\left.\sum\limits_{x\in Y} x=t\right\}$ $\in NP$

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

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

משפט 32: בעיות פתוחות בתורת הסיבוכיות

- האם $P=NP$?
- האם $CoNP=NP$?
- האם $CoNP\cap NP=P$?

12 רדוקציות זמן פולינומיאליות

משפט 33: רדוקציות פולינומיאליות

$$\begin{aligned}
SAT &\leqslant_P 3SAT\\
3SAT &\leqslant_P CLIQUE\\
CLIQUE &\leqslant_P IS\\
IS &\leqslant_P VC\\
SubSetSum &\leqslant_P PARTITION\\
HAMPATH &\leqslant_P HAMCYCLE
\end{aligned}$$