תוכן העניינים

1 מכונות טיורינג

הגדרה 1: מכונת טיורינג

מכונת טיורינג (מ"ט) היא שביעיה $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$ 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	$\delta : (Q \backslash \{q_{\text{rej}}, q_{\text{acc}}\} \times \Gamma \to Q \times \Gamma \times \{L, R\}$
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 $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$ 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 $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$ 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 $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{acc}}, q_{\text{rej}})$ מכונת טיורינג, ו- $w \in \Sigma^*$ מחרוזת. אומרים כי

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

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

הגדרה 6: הכרעה של שפה

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

- אם $w \notin L \Leftarrow M$ 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 $q_0w\vdash q_{\text{acc}}f(w)$.

הגדרה 9: 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 10: מכונט 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 מטב"ס הוא הפונקצית 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 $(u_1q\,\mathsf{v}_1\ ,\ u_2q\,\mathsf{v}_2\ ,\ \ldots\ ,\ u_kq\,\mathsf{v}_k\ .)$

משפט 1: 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.

הגדרה 11: 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 פונקצית 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 12: קבלה ודחייה של מילה ושפה של מכונט 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

$$L(M)=\left\{w\in\Sigma^*\ \middle|\ \exists u,\mathsf{v}\in\Gamma^*\ :\ q_0w\vdash_*\ u\ q_{\text{acc}}\ \mathsf{v}\right\}$$

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 13: 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 14: 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 2: 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.

2 המחלקות החישוביות R, RE ו- $Co\,RE$ ותכונותן

הגדרה 15: כוכב קליני
בהינתן השפה L. השפה L^* מוגדרת:

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

הגדרה 16:

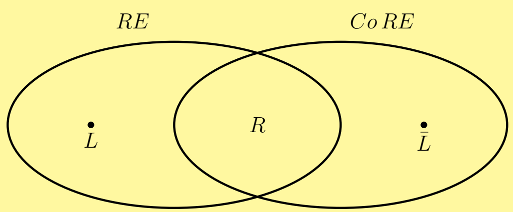
- אוסף השפות הכריעות מסומן R ומוגדר $R = \{L \subseteq \Sigma^* \mid \text{קיימת מ"ט המכריעה את } L\}$.
- אוסף השפות הקבילות מסומן R ומוגדר $RE = \{L \subseteq \Sigma^* \mid \text{קיימת מ"ט המקבלת את } L\}$.
- אוסף השפות שהמשלימה שלהן קבילה מסומן R ומוגדר $Co\,RE = \{L \subseteq \Sigma^* \mid \bar{L}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

משפט 3: סגירות של השפות הכריעות והשפות הקבילות

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

משפט 4: 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 17: 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.

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

3 אי-כריעות

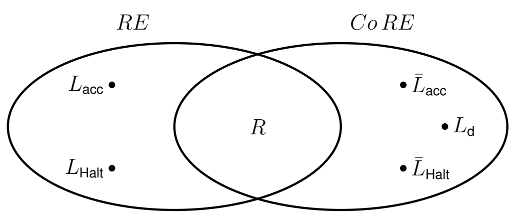
משפט 5: סיווג שפות ידועות - חישוביות

- $L_{acc} = \{\langle M, w\rangle \mid w \in L(M)\}$ — $\in RE\backslash R$
- $L_{halt} = \{\langle M, w\rangle \mid M \text{ עוצרת על } w\}$ — $\in RE\backslash R$
- $L_M = \{\langle M\rangle \mid\mid \langle M\rangle \text{ המקבלת את } M\}$ — $\in RE\backslash R$
- $L_d = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$ — $\in Co\,RE\backslash R$
- $L_E = \{\langle M\rangle \mid L(M) = \varnothing\}$ — $\in Co\,RE\backslash R$
- $L_{EQ} = \{\langle M_1, M_2\rangle \mid L(M_1) = L(M_2)\}$ — $\notin RE\backslash R, \notin Co\,RE\backslash R$
- $L_{REG} = \{\langle M\rangle \mid L(M) \text{ רגולרית}\}$ — $\notin RE\backslash R, \notin Co\,RE\backslash R$
- $L_{NOTREG} = \{\langle M\rangle \mid L(M) \text{ לא רגולרית}\}$ — $\notin RE\backslash R, \notin Co\,RE\backslash R$

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

משפט 6:

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

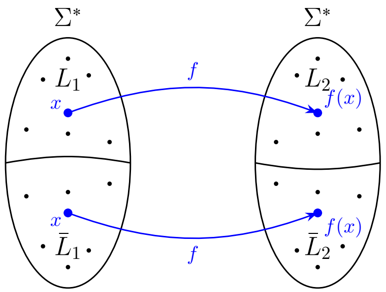


4 רדוקציות

הגדרה 18: 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 19: מ״ט המחשבת פונקציה
בהינתן פונקציה $f:\Sigma^*\to\Sigma^*$ אומרים כי f חשיבה אם קיימת מ״ט המחשבת את f.

הגדרה 20: 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 7: משפט הרדוקציה
לכל שתי שפות $L_1,L_2\subseteq\Sigma^*$, אם קיימת רדוקציה $L_1\leqslant L_2$ אזי
$$\begin{aligned}
L_1\in R &\quad\Leftarrow\quad L_2\in R\\
L_1\in RE &\quad\Leftarrow\quad L_2\in RE\\
L_1\in Co\,RE &\quad\Leftarrow\quad L_2\in Co\,RE\\
L_1\notin R &\quad\Rightarrow\quad L_2\notin R\\
L_1\notin RE &\quad\Rightarrow\quad L_2\notin RE\\
L_1\notin Co\,RE &\quad\Leftarrow\quad L_2\notin Co\,RE
\end{aligned}$$

חישוביות וסיבוכיות דף נוסחאות למבחן סמסטר א׳, תשפ״ו

משפט 8: 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 9: 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 $S\neq\varnothing$.
- $L_S=\{\langle M\rangle \mid L(M)=S\}$.

5 סיבוכיות

משפט 10:
לכל מ״ט מרובת סרטים M הרצה בזמן $f(n)$, קיימת מ״ט סרט יחיד M' השקולה ל- M ורצה בזמן $O\left(f^2(n)\right)$.

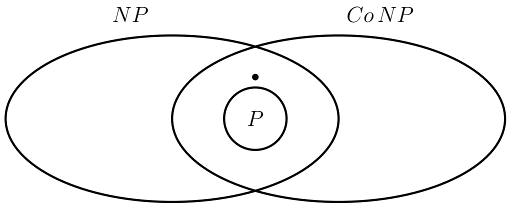
משפט 11:
לכל מ״ט א״ד N הרצה בזמן $f(n)$, קיימת מ״ט דטרמיניסטית D השקולה ל- N ורצה בזמן $2^{(f(n))}$.

הגדרה 21: 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 22:
- $P=$ 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.
- $Co\,NP=$ קבוצת כל השפות שהמשלימה שלהן שייכת ל- NP $\quad$ $Co\,NP=\{A \mid \bar{A}\in NP\ .\}$.

משפט 12: תכונות של P ו- NP
- $P\subseteq NP$.
- P סגורה תחת משלים: אם $A\in P$ אזי גם $\bar{A}\in P$.
- $P\subseteq NP\cap Co\,NP$.



6 רדוקציה פולינומיאלית

הגדרה 23: 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 24: 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 $w \in \Sigma^*$:
$$w \in A \quad \Leftrightarrow \quad f(w) \in B\ .$$

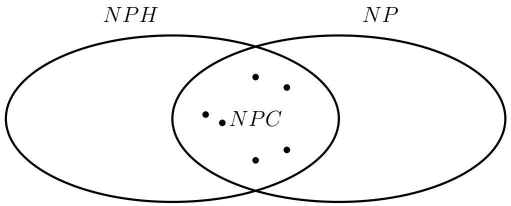
משפט 13: משפט הרדוקציה
לכל שתי בעיות A ו- B, אם $A \leqslant_P B$ אזי

$$\begin{aligned} B \in P &\Rightarrow A \in P \\ B \in NP &\Rightarrow A \in NP \\ A \notin P &\Rightarrow B \notin P \\ A \notin NP &\Rightarrow B \notin NP \end{aligned}$$

7 NP שלמות

הגדרה 25: NP קשה (NP-hard)
בעייה B נקראת NP קשה אם לכל בעייה $A \in NP$ קיימת רדוקציה $A \leqslant_P B$.

הגדרה 26: 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 14: תכונות של רדוקציה פולינומיאלית
- אם קיימת שפה $B \in NPC$ (שלמה NP) 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 $\varnothing, \Sigma^*$ מתקיים $A \leqslant_P B$.

משפט 15:
תהי B בעייה NP- שלמה. אזי לכל בעייה $C \in NP$, אם $C \leqslant_p B$ אזי גם C היא NP שלמה.

8 בעיית הספיקות (SAT)

הגדרה 27: 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:
$$\phi = \overbrace{\left(x_1 \vee \bar{x}_2 \vee x_4 \vee \bar{x}_7\right)}^{C_1} \wedge \overbrace{\left(x_3 \vee x_5 \vee \bar{x}_8\right)}^{C_2} \wedge \quad \cdots$$

הגדרה 28: נוסחת $3CNF$
נוסחת $3CNF$, ϕ היא נוסחה CNF שבה בכל פסוקית יש בדיוק שלוש ליטרלים. לדוגמה:
$$\phi = \overbrace{\left(x_1 \vee \bar{x}_2 \vee x_4\right)}^{C_1} \wedge \overbrace{\left(x_3 \vee x_5 \vee \bar{x}_8\right)}^{C_2} \wedge \quad \cdots$$

הגדרה 29: 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.

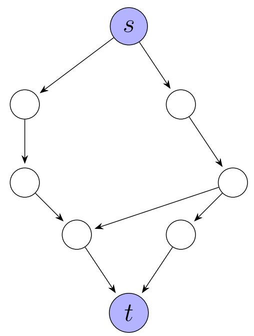
הגדרה 30: בעיית SAT
קלט: נוסחת CNF, ϕ.
פלט: האם ϕ ספיקה?
$$SAT = \{\langle\phi\rangle \mid \text{ספיקה } CNF \text{ נוסחת } \phi\}$$

הגדרה 31: בעיית $3SAT$
קלט: נוסחת $3CNF$ ϕ.
פלט: האם ϕ ספיקה?
$$3SAT = \{\langle\phi\rangle \mid \text{ספיקה } 3CNF \text{ נוסחת } \phi\}$$

משפט 16:
- $SAT \in NP$.
- **משפט קוק לוין:** $SAT \in NPC$.
- $3SAT \in NPC$.
- $P = NP \Leftrightarrow SAT \in P$.

9 סיווג שפות ידיועות - סיבוכיות

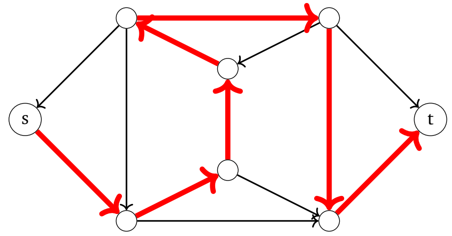
הגדרה 32: בעיית מסלול $PATH$
קלט: גרף מכוון G ושני קודקודים s ו- t.
פלט: האם G מכיל מסלול מקודקוד s לקודקוד t.
$$PATH = \{\langle G, s, t\rangle \mid t \text{ -ל } s \text{ גרף מכוון המכיל מסלול מ- } G \}$$



הגדרה 33: 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 34: 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.



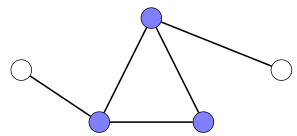
הגדרה 35: בעיית מסלול המילטוני - $HAMPATH$
קלט: גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$.
פלט: האם G מכיל מסלול המילטוני מ- s ל- t?
$$HAMPATH = \{\langle G, s, t\rangle \mid \text{?}t \text{ -ל } s \text{ גרף מכוון המכיל מסלול המילטוני מ- } G \}$$

הגדרה 36: מעגל המילטוני
בהינתן גרף מכוון $G = (V, E)$.
מעגל המילטוני הוא מסלול מעגלי שעובר כל קודקוד ב- G בדיוק פעם אחת.

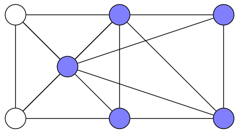
הגדרה 37: בעיית מעגל המילטוני - $HAMCYCLE$
קלט: גרף מכוון $G = (V, E)$.
פלט: האם G מכיל מעגל המילטוני?
$$HAMCYCLE = \{\langle G\rangle \mid \text{.גרף מכוון המכיל מעגל המילטוני } G \}$$

הגדרה 38: 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 39: בעיית הקליקה - $CLIQUE$

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

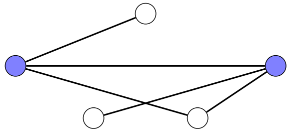
פלט: האם G קליק בגודל k?

$$CLIQUE = \left\{ \langle G, k \rangle \;\middle|\; \text{גרף לא מכוון המכיל קליק בגודל } k \text{ } G \right\}$$

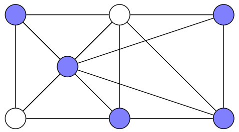
הגדרה 40: כיסוי בקודקודים

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 $v \in C$.

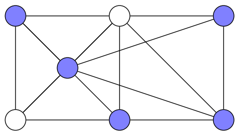
כיסוי בקודקודים בגודל $k = 2$:



כיסוי בקודקודים בגודל $k = 5$:



כיסוי בקודקודים בגודל $k = 5$:



הגדרה 41: בעיית VC

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

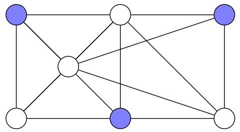
פלט: האם קיים כיסוי בקודקודים ב- G בגודל k?

$$VC = \left\{ \langle G, k \rangle \;\middle|\; \text{גרף לא מכוון המכיל כיסוי בקודקודים בגודל } k \text{ } G \right\}$$

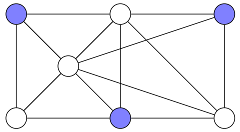
הגדרה 42: קבוצה בלתי תלויה

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 תלוייה בגודל $k = 3$:



הגדרה 43: בעיית IS

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

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

$$IS = \left\{ \langle G, k \rangle \;\middle|\; \text{גרף לא מכוון המכיל קבוצה בלתי תלויה בגודל } k \text{ } G \right\}$$

הגדרה 44: בעיית $PARTITION$

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

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

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

הגדרה 45: בעיית $SubSetSum$

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

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

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

משפט 17:

$\in P$	$PATH = \{\langle G,s,t\rangle \mid$ גרף מכוון המכיל מסלול מ- s ל- t $G\}$
$\in P$	$RELPRIME = \{\langle x,y\rangle \mid \gcd(x,y)=1\}$
$\in NP, \in NPC$	$SAT = \{\langle \phi\rangle \mid$ היא נוסחת CNF ספיקה $\phi\}$
$\in NP, \in NPC$	$3SAT = \{\langle \phi\rangle \mid$ היא נוסחת $3CNF$ ספיקה $\phi\}$
$\in NP, \in NPC$	$IS = \{\langle G,k\rangle \mid$ גרף לא מכוון המכיל קליקה בגודל k $G\}$
$\in NP, \in NPC$	$CLIQUE = \{\langle G,k\rangle \mid$ גרף לא מכוון המכיל קליקה בגודל k $G\}$
$\in NP, \in NPC$	$VC = \{\langle G,k\rangle \mid$ גרף לא מכוון המכיל כיסוי בקודקודים בגודל k $G\}$
$\in NP, \in NPC$	$HAMPATH = \{\langle G,s,t\rangle \mid$ גרף מכוון המכיל מסלול המילטוני מ- s ל- t $G\}$
$\in NP$	$HAMCYCLE = \{\langle G\rangle \mid$ גרף מכוון המכיל מעגל המילטוני $G\}$
$\in NP$	$SubSetSum = \left\{\langle S,t\rangle \mid\right.$ קיימת $Y \subseteq S$ כך ש- $\left.\sum_{x\in Y} x = t\right\}$
$\in CoNP$	$\overline{HAMPATH}$
$\in CoNP$	$\overline{CLIQUE}$

משפט 18: בעיות פתוחות בתורת הסיבוכיות

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

10 רדוקציות זמן פולינומיאליות

משפט 19: רדוקציות פולינומיאליות

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