שיעור 9
המחלקה P והמחלקה NP

9.1 המחלקה P

- המחלקה P היא אוסף כל הבעיות שקיים עבורן אלגוריתם המכריע אותן בזמן פולינומיאלי.

$$\text{אלגוריתם מכריע} \equiv \text{מ"ט דטרמיניסטית} ,$$
$$\text{בעיית הכרעה} \equiv \text{שפה} ,$$

- אלגוריתם A מכריע בעייה בזמן פולינומיאלי אם קיים קבוע $c > 0$ כך שזמן הריצה של A על כל קלט w חסום ע"י $O\left(|w|^c\right)$.

9.2 דוגמאות לבעיות ב- P

(1

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

(2

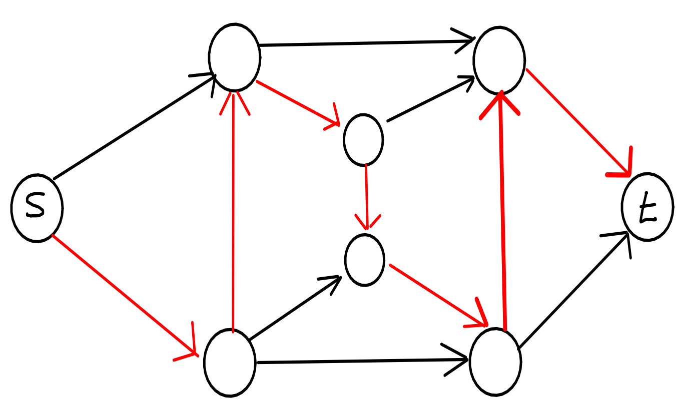
$$RELPRIME = \left\{\langle x, y\rangle \mid \text{ זרים } y \text{ ו- } x \right\} \in P$$

9.3 בעיית המסלול ההמילטוני HAMPATH

הגדרה 9.1 HAMPATH

בהינתן גרף מכוון $G = (V, E)$ ושני קודקודים $s, t \in V$. מסלול המילטוני 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?

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

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 בעייה 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 $w\in A \quad\Leftarrow\quad \exists y\ :\ V(w,y)=T$.
- אם $w\notin A \quad\Leftarrow\quad \forall y\ :\ V(w,y)=F$.

הערה 9.1

- זמן ריצה של אלגוריתום 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?

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

הוכיחו כי $HAMPATH \in NP$.

הוכחה: נבנה אלגוריתם אימות V עבור $HAMPATH$.

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

(1 בודק האם y היא סדרה של

$$u_1, u_2, \quad \ldots \quad u_n$$

השונים זה מזה.

- אם לא $\Leftarrow$ דוחה.

(2 בודק האם $s = u_1$ ו- $u_n = t$.

- אם לא $\Leftarrow$ דוחה.

(3 בודק שכל הצלעות (u_i, u_{i+1}) (לכל $1 \leqslant i \leqslant n$) 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 $(\langle G,s,t\rangle, y)$.

■

משפט 9.2 $HAMPATH \in NP$

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?

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

הוכיחו כי $HAMPATH \in NP$.

הוכחה: נבנה אלגוריתם אימות V עבור $HAMPATH$.

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

1) בודק האם y היא סדרה של

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

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 $1 \leqslant i \leqslant n$) קיימות ב- G.

- אם כן $\Leftarrow$ מקבל.
- אם לא $\Leftarrow$ דוחה.

נכונות

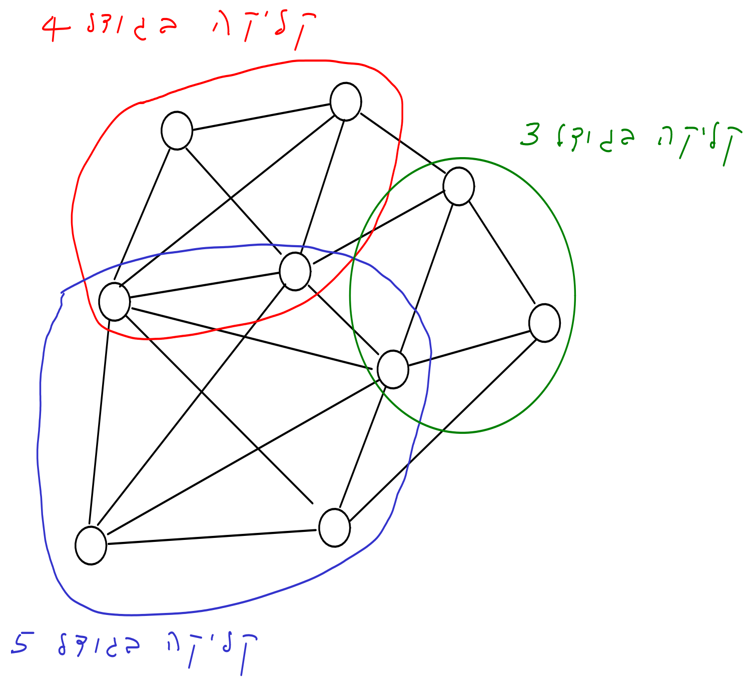
- זמן הריצה של האלגוריתם הוא פולינומיאלי בגודל הקלט.
- אם $\langle G, s, t\rangle \in HAMPATH$ $\Leftarrow$ G מכיל מסלול המילטוני מ- s ל- t $\Leftarrow$ עבור y שהוא קידוד של מסלול זה, V יקבל את הזוג $(\langle G, s, t\rangle, y)$.
- אם $\langle G, s, t\rangle \notin HAMPATH$ $\Leftarrow$ G לא מכיל מסלול 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 $u, \mathrm{v} \in C$ מתקיים $(u, \mathrm{v}) \in E$.

לדוגמה:



הגדרה 9.6 בעיית הקליקה

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

פלט: האם G קליקה בגודל k?

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

משפט 9.3 $CLIQUE \in NP$

$$CLIQUE \in NP \ .$$

הוכחה: נבנה אלגוריתם אימות V עבור $CLIQUE$.

$V =$ 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 $S=\{x_1,x_2, \quad \ldots \quad x_n\}$ 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 9.4 $SubSetSum \in NP$

$$SubSetSum \in NP \ .$$

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 9.5

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 9.6

$$P\subseteq NP \ .$$

שאלה פתוחה: האם $P=NP$?

משפט 9.7

P סגורה תחת משלים.

הוכחה: אם $A\in P$ אזי גם $\bar{A}\in P$. ■

הגדרה 9.8 $CoNP$

$$CoNP=\{A\,\big|\,\bar{A}\in NP \ .\}$$

לדוגמה:

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

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

שאלה פתוחה: האם $NP=CoNP$?

משפט 9.8

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

שאלה פתוחה: האם $P=NP\cap CoNP$?

נדון בשאלה המרכזית: האם $P=NP$?

הגדרה 9.9 פונקציה פולינומיאלית

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

הגדרה 9.10 רדוקציה פולינומיאלית

בהינתן שתי בעיות 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 9.9 משפט הרדוקציה

לכל שתי בעיות A ו- B, אם $B \leqslant_P A$ 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 $B \leqslant_P A$, קיימת פנקציה f חשיבה בזמן פולנומיאלי המקיימת, לכל $w \in \Sigma^*$,

$$w \in A \quad \Leftrightarrow \quad f(w) \in B \ .$$

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 עת B בזמן פולינומיאלי. נבנה אלגוריתם M_A המכריע את A בזמן פולינומיאי.

<u>התאור של M_A</u>

$M_A =$ 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 $w \in A \Leftarrow f(w) \in B \Leftarrow M_B$ מקבל את $f(w) \Leftarrow M_A$ מקבל את w.
- אם $w \notin A \Leftarrow f(w) \notin B \Leftarrow M_B$ דוחה את $f(w) \Leftarrow M_A$ דוחה את w.

נוכיח כי זמן הריצה של M_A הוא פולינומיאי 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

$$P_f\left(|w|\right) + P_B\left(|f(w)|\right)$$

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

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

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

■