

שיעור 10

המחלקה P והמחלקה NP

10.1 המחלקה P

- המחלקה P היא אוסף כל הבעיה שקיים עboroן אלגוריתם המכרייע אותה בזמן פולינומיAli.
- אלגוריתם מכרייע \equiv מ"ט דטרמיניסטי , בעית הכרעה \equiv שפה ,
- אלגוריתם A מכרייע בעיה בזמן פולינומיAli אם קיים קבוע $c > 0$ כך שזמן הריצה של A על כל קלט w חסום ע"י $O(|w|^c)$.

10.2 דוגמאות לבעיות ב- P

$$PATH = \{ \langle G, s, t \rangle \mid \text{גרף } G \text{ מכיל מסלול מ- } s \text{ ל- } t \} \in P \quad (1)$$

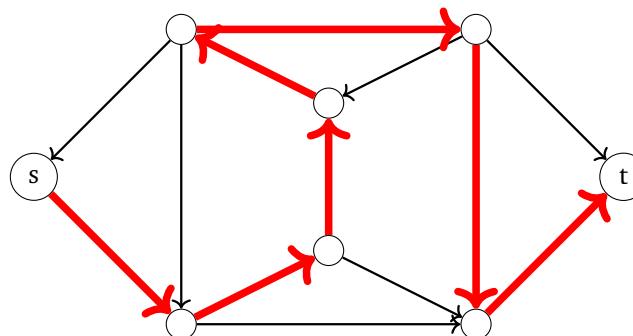
$$RELPRIME = \{ \langle x, y \rangle \mid x \text{ ו- } y \text{ זרים} \} \in P \quad (2)$$

10.3 בעית המסלול המילטוני HAMPATH

הגדרה 10.1 HAMPATH

בහינתן גרף מכון (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 בדיקוק פעם אחת.

לדוגמה:



הגדרה 10.2 בעית HAMPATH

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

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

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

נשאל שאלת: האם $HAMPATH \in P$?

לא ידוע האם קיים אלגוריתם המכריע את $HAMPATH$ בזמן פולינומיAli (שאלת פתוחה).

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

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

- ניתן לבדוק האם y היא מסלול המילוטוני מ- s ל- t ב- G בזמן פולינומיAli ולענות בהתאם.
- במקרה זה, אומרים כי $HAMPATH$ ניתנת לאיומות בזמן פולינומיAli.

10.4 אלגוריתם איומות

הגדרה 10.3 אלגוריתם איומות

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

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

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

הערה 10.1

- זמן ריצה של אלגוריתום איות נמדד ביחס לגודל הקלט $|w|$.
- אלגוריתם איות פולינומיAli אם הוא רץ בזמן פולינומיAli.

10.5 המחלקה NP

הגדרה 10.4 המחלקה NP

המחלקה NP היא אוסף כל הבעיה שקיים עבורן אלגוריתם איות פולינומיAli.

משפט 10.1 $HAMPATH \in NP$

בעיית המסלול המילוטוני : $HAMPATH$

קלט: גраф מכון $G = (V, E)$ ושני קודקודים $s, t \in V$

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

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

הוכחה כי $HAMPATH \in NP$

הוכחה: בניית אלגוריתם אimotoת V עבור $HAMPATH$.

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

1) בודק האם y היא סדרה של

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

השונים זה מזוהה.

- אם לא \Leftarrow דוחה.

2) בודק האם $u_n = t$ ו- $u_1 = s$

- אם לא \Leftarrow דוחה.

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

- אם כן \Leftarrow מקבל.

- אם לא \Leftarrow דוחה.

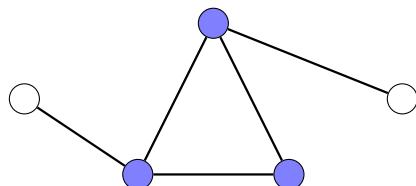
נכונות

- זמן הריצה של האלגוריתם הוא פולינומילי בגודל הקלט.
- אם G מכיל מסלול המילטוני מ- s ל- t \Leftarrow עבור y שהוא קידוד של מסלול זה, V קיבל את הזוג $(\langle G, s, t \rangle, y)$.
- אם G לא מכיל מסלול המילטוני מ- s ל- t \Leftarrow לכל y , האלגוריתם ידחה את הזוג $(\langle G, s, t \rangle, y)$.

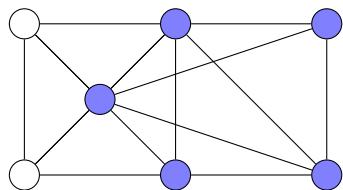


הגדרה 10.5 קליקה

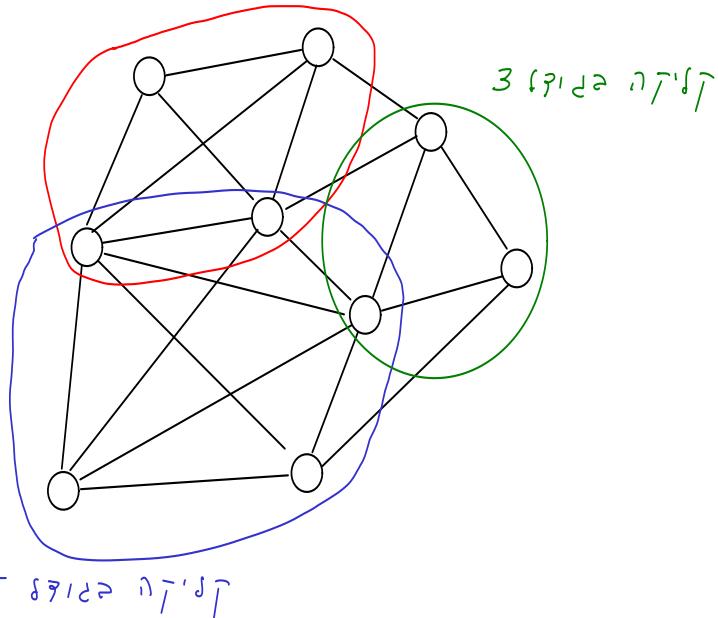
בහינתנו גראף לא מכוכן $G = (V, E)$, קליקה ב- G היא תת-קובוצה של קודקודים $C \subseteq V$ כך שלכל שני קודקודים $u, v \in C$ מתקיים $(u, v) \in E$.



קליקה בגודל 3 : $k = 3$

קliquה בגודל 5 : $k = 5$

ליניאר חישובים 4

**הגדרה 10.6 בעיית הקלliquה**קלט: גרף לא מכוון $G = (V, E)$ ומספר k .פלט: האם G קלliquה בגודל k ?

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

משפט 10.2 CLIQUE $\in NP$

$$\text{CLIQUE} \in NP.$$

הוכחה: בניית אלגוריתם אימות V עבור $.CLIQUE$ 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 10.7 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 ?

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

משפט 10.3 $SubSetSum \in NP$

$SubSetSum \in NP$.

הוכחה: נבנה אלגוריתם אimotoת V עבור $.SubSetSum$

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

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.

10.6 הקשר בין NP למ"ט א"ד

NP=Non-deterministic polynomial-time.

משפט 10.4

לכל בעיה A :

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

דוגמה 10.1

نبנה מ"ט א"ד M המכריעה את $CLIQUE$ בזמן פולינומיAli.

: על קלט $\langle G, k \rangle = M$

- 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 אimoto \equiv מ"ט א"ד.

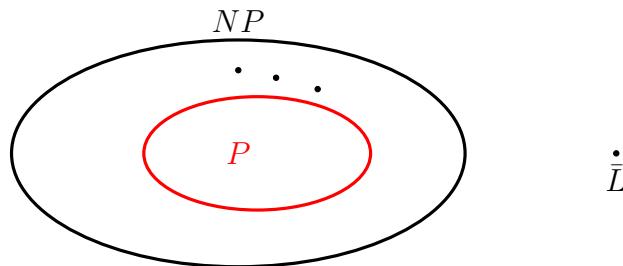
10.7 הקשר בין המחלקה P ו- NP

P = כל הבעיות שניתן להכרייה בזמן פולינומיAli.

NP = כל הבעיות שניתן לאמת בזמן פולינומיAli.

משפט 10.5

$$P \subseteq NP .$$



שאלה פתוחה: האם $P = NP$

משפט 10.6

P סגורה תחת משלים.

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

הגדרה 10.8

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

לדוגמה:

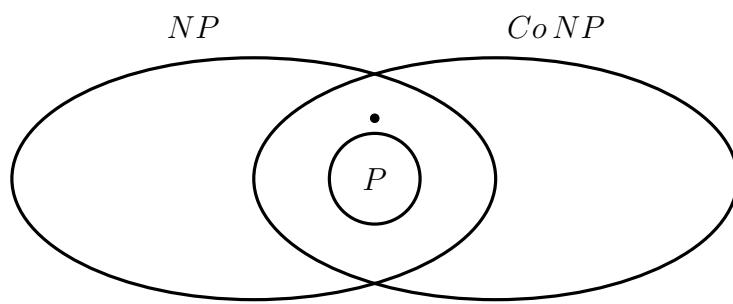
$$\overline{HAMPATH} \in CoNP .$$

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

שאלה פתוחה: האם $NP = CoNP$

משפט 10.7

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



שאלה פתוחה: האם $P = NP \cap Co\ NP$?

נדון בשאלה המרכזית: האם $P = NP$?

הגדרה 10.9 פונקציה פולינומיאלית

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

הגדרה 10.10 רדוקציה פולינומיאלית

בහינתן שתי הבעיות A ו- B . אומרים כי A ניתנת לרדוקציה פולינומיאלית ל- B , ומסמנים $A \leqslant_P B$, אם קיימת פונקציה $\Sigma^* \rightarrow \Sigma^*$ המקיים:

(1) חסיבה בזמן פולינומיאלי

(2) לכל $w \in \Sigma^*$:

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

משפט 10.8 משפט הרדוקציה

לכל שתי בעיות A ו- B , אם $A \leqslant_P B$ אז $A \in P$

(1) אם $A \in P$ אז $B \in P$.

(2) אם $A \in NP$ אז $B \in NP$.

מסקנה מ- (1) ו- (2):

(3) אם $A \notin P$ אז $B \notin P$.

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

הוכחה: מכיוון שקיימת רדוקציה $B \leqslant_P A$, קיימת פונקציה f חסיבה בזמן פולינומיאלי המקיים, לכל $w \in \Sigma^*$,

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

יהי M_f האלגוריתם שמחשבת את f בזמן פולינומיאלי.

(1) נוכחות כי אם $B \in P$ אז $.A \in P$.

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

התאור של M_A

= על כל קלט w : M_A

1. מחשב את $f(w)$ ע"י M_f
2. מרים את M_B על ($f(w)$ ועונה כמוות).

נוכיח כי M_A מכריע את A בזמן פולינומיAli:

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

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

- 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

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

מכיוון ש- $|f(w)|$ 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 פולינומיAli בגודל $|w|$.

