

## 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

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

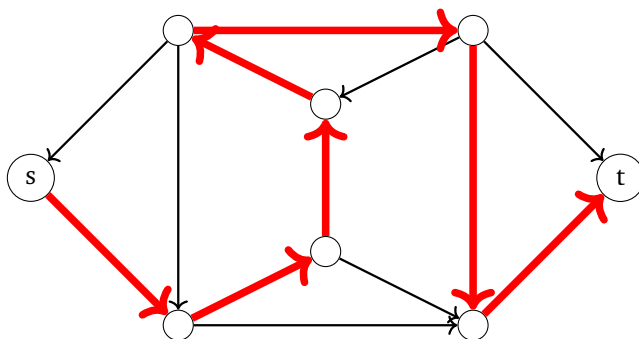
$$RELPRIME = \{ \langle x, y \rangle \mid x \text{ ו-} y \text{ זרים} \} \in P \quad (2)$$

#### 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  $w \in A$   $\Leftrightarrow \exists y : V(w, y) = T$ .

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

### 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- $t$ ?

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

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.

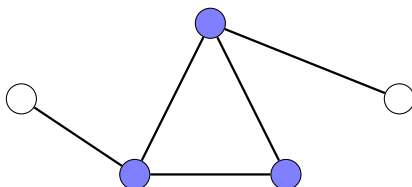
• אם  $\langle G, s, t \rangle \in HAMPATH \Leftarrow G$  מכיל מסלול המילטוני מ- $s$  ל- $t \Leftarrow$  עבור  $y$  שהוא קידוד של מסלול זה,  $V$  יקבל את הזוג  $(\langle G, s, t \rangle, y)$ .

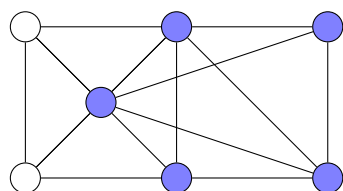
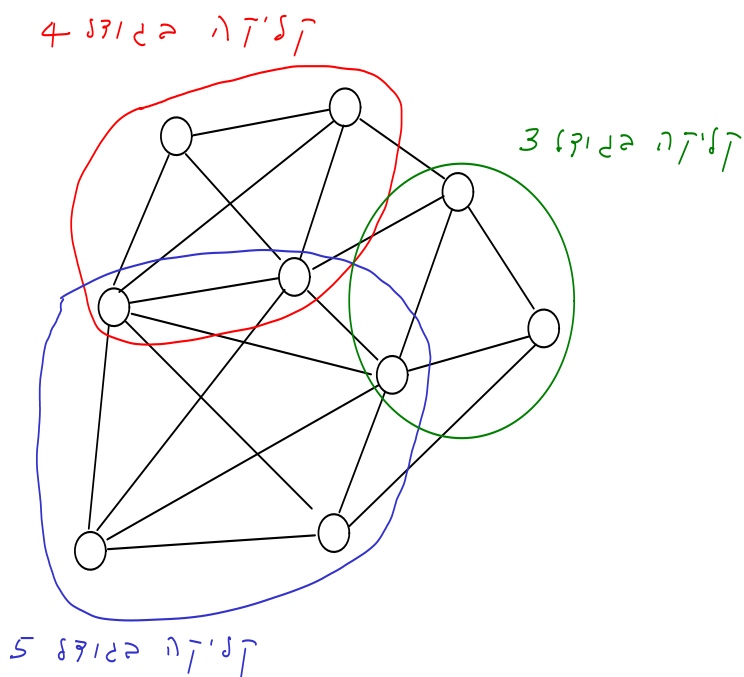
• אם  $\langle G, s, t \rangle \notin HAMPATH \Leftarrow G$  לא מכיל מסלול המילטוני מ- $s$  ל- $t \Leftarrow$  לכל  $y$ , האלגוריתם ידחה את הזוג  $(\langle G, s, t \rangle, y)$ .

## 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  $CLIQUE$ . $V =$  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-  $G$ .

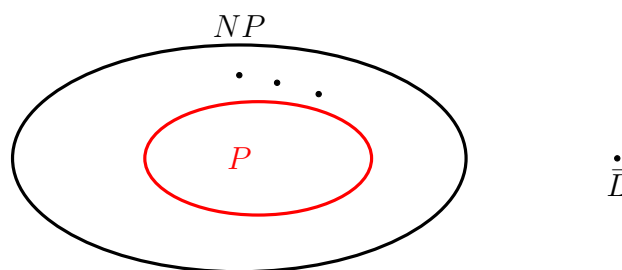
\* אם כן  $\Leftarrow$  מקבלת.\* אחרת  $\Leftarrow$  דוחה.אלגוריתם אימות  $\equiv$  מ"ט א"ד.

## 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:

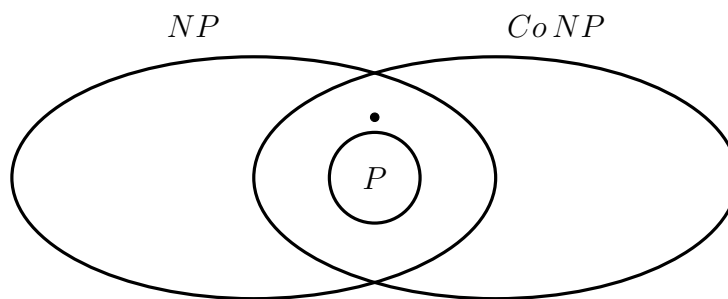
$$\overline{HAMPATH} \in CoNP.$$

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

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  $|w|$ .

