

# שיעור 10

## המחלקה P והמחלקה NP

### 10.1 המחלקה P

#### הגדרה 10.1 בעיית הכרעה

בעיית הכרעה מוגדרת באופן הבא:

"בhinatan קלט כלשהו, האם הקלט מקיים תנאי מסוימים ? "

#### דוגמה 10.1 דוגמה של בעיית הכרעה

לדוגמה, בהינתן מספר  $n$ , האם  $n$  ראשוני?

#### משפט 10.1 שקיים בין בעיה לשפה

כל בעיה הכרעה ניתן לתאר כשפה שוקולה:

. בעיה הכרעה  $\equiv$  שפה

### דוגמה 10.2

לדוגמה, הבעיה הכרעה הבאה:

"בhinatan מספר  $n$ , האם  $n$  ראשוני? "

ניתנת לרשום כשפה הבאה:

$$L_{\text{prime}} = \{ \langle n \rangle \mid n \text{ ראשוני} \}.$$

#### הגדרה 10.2 אלגוריתם זמן פולינומייאלי

אומרים כי אלגוריתם  $A$  מכרייע בעיה בזמן פולינומייאלי אם קיימים קבוע  $c > 0$  כך שזמן הריצה של  $A$  על קלט  $w$  חסום ע"י  $O(|w|^c)$ .

התזה של צרצ' טיורינג אומר שאם קיימים אלגוריתם המכרייע בעיה בזמן פולינומייאלי, אז קיימת מכונת טיורינג דטרמיניסטיבית המכרייע את השפה השוקולה בעיה או בזמן פולינומייאלי.

. אלגוריתם מכרייע  $\equiv$  מכונת טיורינג דטרמיניסטיבית

#### הגדרה 10.3 המחלקה P

המחלקה  $P$  היא אוסף כל הבעיה (השפות) שקיימים עבורן אלגוריתם (מכונת טיורינג דטרמיניסטיבית) המכרייע אותן בזמן פולינומייאלי.

## 10.2 דוגמאות לבעיות ב- $P$

(1)

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

(2)

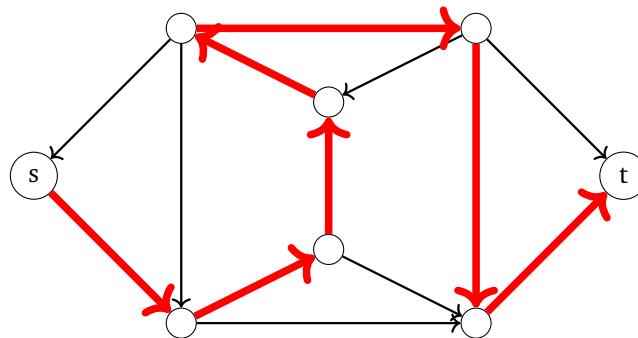
$$RELPRIME = \{\langle x, y \rangle \mid x \text{ ו- } y \text{ זרים}\} \in P$$

## 10.3 בעיית המסלול המילטוני $HAMPATH$

### הגדירה 10.4 $HAMPATH$

בاهינתן גרף מכון  $G = (V, E)$  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 בדיקת פעם אחת.

לדוגמה:



### הגדירה 10.5 בעיית $HAMPATH$

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

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

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

נשאל שאלת: האם  $HAMPATH \in P$ ?

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

- בהינתן קלט  $\langle G, s, t \rangle \in HAMPATH$ , האם  $\langle G, s, t \rangle \in ?$

• נעה על שאלת אחרת:

בהתאם קלט  $\langle G, s, t \rangle \in HAMPATH$ , ומהריזת  $y$ , האם  $\langle G, s, t \rangle \in ?$

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

## 10.4 אלגוריתם אימות

### הגדרה 10.6 אלגוריתם אימות

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

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

- אם  $w \in A$  קיים  $y$  כך ש:  $V(w, y) = T$   $\Leftarrow$
- אם  $w \notin A$  לכל  $y$  מתקיים  $V(w, y) = F$   $\Leftarrow$

### הערה 10.1

זמן ריצה של אלגוריתום אימות נמדד ביחס לגודל הקלט  $|w|$ .

אלגוריתם אימות פולינומיAli אם הוא רץ בזמן פולינומיAli.

## 10.5 המחלקה NP

### הגדרה 10.7 המחלקה NP

המחלקה NP היא אוסף כל הבעיות שקיים עבורן אלגוריתם אימות פולינומיAli.

### משפט 10.2 $HAMPATH \in NP$

בעיית המסלול ההAMILTONI :  $HAMPATH$

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

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

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

הוכחה: הוכחנו כי  $HAMPATH \in NP$

הוכחה: נבנה אלגוריתם אימות  $V$  עבור  $HAMPATH$ .

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

1) בודק האם  $y$  היא סדרה של

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

השונים זה מזה.

- אם לא  $\Leftarrow$  דוחה.

2) בודק האם  $u_n = t$  ו-  $u_1 = s$ .

- אם לא  $\Leftarrow$  דוחה.

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

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

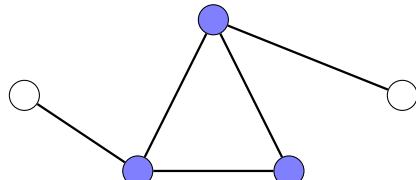
### נכונות

- 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,  $V$  יקבל 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  $(\langle G, s, t \rangle, y)$ .

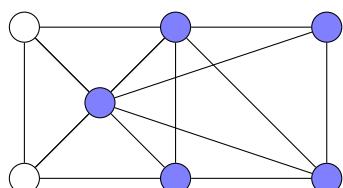
■

### הגדרה 10.8 קליקה

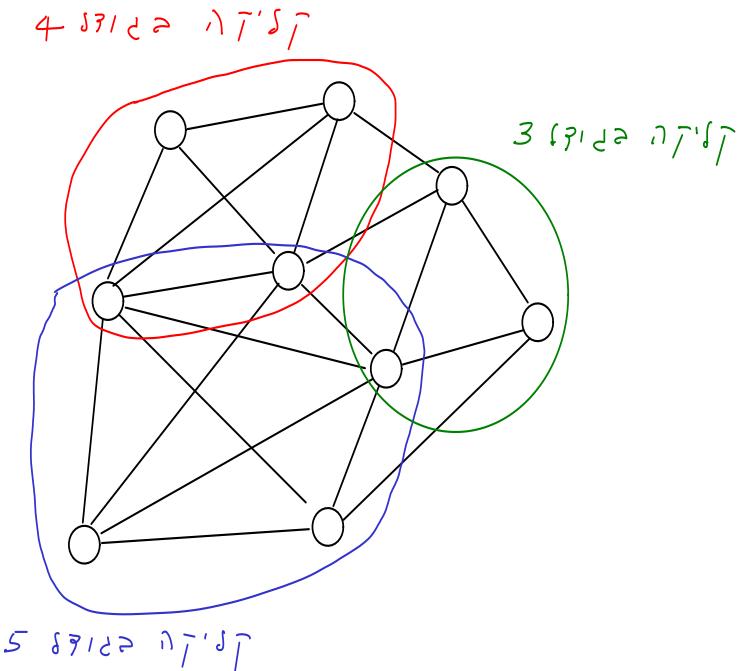
בහינתן גרף לא מכוון  $G = (V, E)$ , קליקה ב- $G$  היא תת-קובוצה של קודקודים  $C \subseteq V$  כך שלכל שני קודקודים  $u, v \in C$  מתקיים  $(u, v) \notin E$ .



קליקה בגודל 3



קליקה בגודל 5

**הגדרה 10.9 בעיית הקליקה**

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

פלט: האם  $G$  קליקה בגודל  $k$ ?

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

**משפט 10.3**  $\text{CLIQUE} \in NP$

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

**הוכחה:** נבנה אלגוריתם אimotoת  $V$  עבור  $\text{CLIQUE}$ .

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

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 10.10 בעיית  $\text{SubSetSum}$** 

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

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

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

**משפט 10.4**  $\text{SubSetSum} \in NP$

$\text{SubSetSum} \in NP$ .

**הוכחה:** נבנה אלגוריתם אimotoות  $V$  עבור  $\text{SubSetSum}$ .

$V$  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.

## 10.6 הקשר בין NP למוכנות טיריניג א-דטרמיניסטיבית

NP=Non-deterministic polynomial-time.

**משפט 10.5**

לכל בעיה  $A$ :

אם ורק אם קיימת מוכנות טיריניג א-דטרמיניסטיבית המכ裏עה את  $A$  בזמן פולינומילי.

### דוגמה 10.3

نبנה מוכנות טיריניג א-דטרמיניסטיבית  $M$  המכ裏עה את  $CLIQUE$  בזמן פולינומילי.

$\langle G, k \rangle$  על קלט  $= M$ :

- בוחרת באופן א-דטרמיניסטי 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 אimotoות  $\equiv$  מ"ט א"ד.

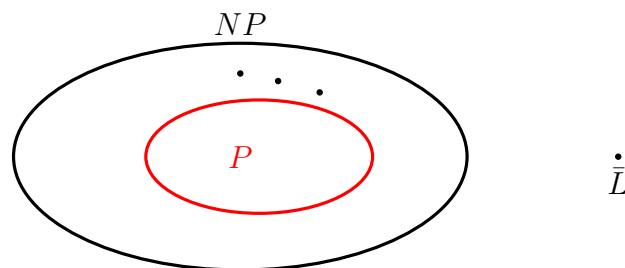
## 10.7 הקשר בין המחלקה $P$ ו- $NP$

$P$  = כל הבעיות שניתן להכריע בזמן פולינומיאלי.

$NP$  = כל הבעיות שניתן לאמת בזמן פולינומיאלי.

### משפט 10.6

$$P \subseteq NP .$$



שאלה פתוחה: האם  $?P = NP$

### משפט 10.7

$P$  סגורה תחת משלים.

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

### הגדרה 10.11

$$Co\,NP = \{A \mid \bar{A} \in NP .\}$$

לדוגמה:

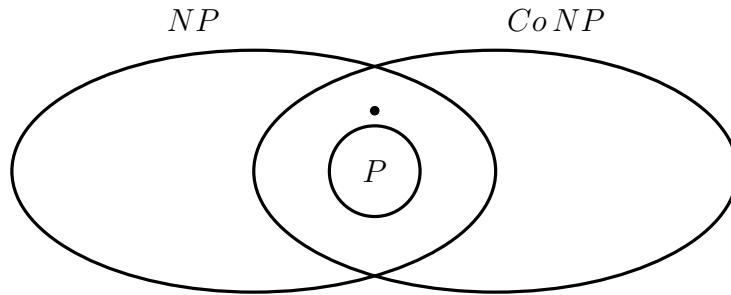
$$\overline{HAMPATH} \in Co\,NP .$$

$$\overline{CLIQUE} \in Co\,NP .$$

שאלה פתוחה: האם  $?NP = Co\,NP$

### משפט 10.8

$$P \subseteq NP \cap Co\,NP .$$



שאלה פתוחה: האם  $?P = NP \cap Co\,NP$

נדון בשאלה המרכזית: האם  $?P = NP$

**הגדרה 10.12 פונקציה פולינומיאלית**

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

**הגדרה 10.13 רדוקציה פולינומיאלית**

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

(1)  $f$  חסיבה בזמן פולינומיאלי

(2) לכל  $w \in \Sigma^*$ :

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

**משפט 10.9 משפט הרדוקציה**

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

(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  $B \notin P$  אז  $A \notin P$ .

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

**הוכחה:** מכיוון שקיימת רדוקציה  $D$   $B \leqslant_P A$ , 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) נוכח כי אם  $B \in P$  אז  $A \in P$ .

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

התאור של  $M_A$

= על כל קלט  $w$ :

1. מחשב את  $f(w)$  ע"י  $M_f$ .

2. מריץ את  $M_B$  על  $f(w)$  ועונה כמותה.

nocich כי  $M_A$  מכrüע את  $A$  בזמן פולינומיאלי:

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

nocich 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-  $|f(w)| \leq P_f(|w|)$ , הזמן 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 פולינומייאלי בגודל  $|w|$ .

