

## שיעור 8

# מבוא לסייעות

## 8.1 הגדרה של סיבוכיות

## הערה 8.1

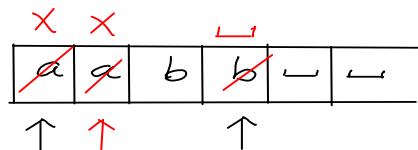
זמן ריצה של מ"ט  $M$  על קלט  $w$ , נמדד ביחס לגודל הקלט  $w$ , קלומר ( $f(|w|)$ )

## 8.1 הגדרה

נאמר כי ניתן להכריע שפה  $L$  בזמן  $(n)^f$ , אם קיימת מ"ט  $M$  המכריעה את  $L$  ולכוון קלט  $\Sigma^*$  בזמנו  $w$ , זמן הריצה של  $M$  על  $w$  חסום ע"י  $|w|^f$ .

### 8.1 דוגמה

**מבנה מ"ט**  $M$  המכריעה השפה



## התאור של $M$

על קלט:

- (1) אם הטו שמתחת לראש הוא  $\perp$   $\Leftarrow$  מקבלת.
  - (2) אם הטו שמתחת לראש הוא  $b$   $\Leftarrow$  דוחה.
  - (3) מוחקת את הטו שמתחת לראש ע"י  $X$ .
  - (4) מזיצה את הראש ימינה עד הטו הראשון משמאלו  $\perp$   $\Leftarrow$ .
    - אם הטו הוא  $a$  או  $X$   $\Leftarrow$  דוחה.
    - מוחקת את הטו שמתחת לראש ע"י  $\perp$ , מזיצה את הראש שמאלה עד הטו הראשון מימין לו  $X$ .

זמו ברכיאב

- $\frac{|w|}{2}$  איטרציות.
  - בכל איטציה מבצעים  $O(|w|)$  צעדים.

**הגדרה 8.2 זמן הריצה**

זמן הריצה של מ"ט  $M$  על קלט  $w$  היא פונקציה  $f(|w|)$  השווה למספר הצעדים הנדרש בחישוב של  $M$  על  $w$ .

**הערה 8.2**

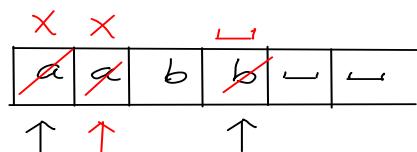
זמן הריצה של מ"ט נמדד ביחס לגודל הקלט  $|w|$ .

**הגדרה 8.3**

אומרים כי ניתן להכריעה שפה  $L$  בזמן  $f(n)$  אם קיימת מ"ט  $M$  המכריעה את  $L$  כך שלכל  $\Sigma^*$ , זמן הריצה של  $M$  על  $w$  חסום ע"י  $f(|w|)$ .

**דוגמה 8.2**

נבנה מ"ט  $M$  עם סרט ייחיד שמכריעה את השפה  $.L = \{a^n b^n \mid n \geq 0\}$



התאור של  $M$ :

על קלט  $w$ :

- (1) אם התו שמתוחת לראש הוא  $\_ \leftarrow$  מקבלת.
- (2) אם התו שמתוחת לראש הוא  $b \leftarrow$  דוחה.
- (3) מוחקת את התו שמתוחת לראש ע"י  $X$ .
- (4) מזיהה את הראש ימינה עד התו הראשון משמאלו  $\_ \leftarrow$ .
  - אם התו הוא  $a$  או  $X \leftarrow$  דוחה.
  - מוחקת את התו שמתוחת לראש ע"י  $\_ \leftarrow$ , מזיהה את הראש שמאלה עד התו הראשון מימין לו  $X$  ו חוזרת  $\_ \leftarrow$  (1).

זמן הריצה

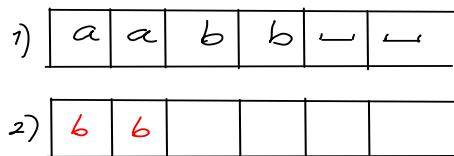
•  $M$  מבצעת  $\frac{|w|}{2}$  איטרציות.

- בכלל איטרציה  $M$  סורקת את הסרט פעמיים וזה עולה  $O(|w|)$ .
- לכן סה"כ זמן הריצה של  $M$  חסום ע"י

$$\frac{|w|}{2} \cdot O(|w|) = O(|w|^2).$$

**דוגמה 8.3**

נבנה מ"ט מרובת סרטים'  $M'$  שמכריעת את השפה  $\{a^n b^n \mid n \geq 0\}$ .



התאור של  $M'$ :

על קלט  $w$ :

(1) מעתיקת את ה-  $b$  -ים לסרט 2 (ותוך כדי בודקת האם  $w$  מהצורה  $a^* b^*$ ).

(2) מזיהה את הראשים לתחילת הסרטים.

(3) אם שני הראשים מצביעים על  $\_ \leftarrow$  מקבלת.

(4) אם אחד הראשים מצביע על  $\_ \leftarrow$  והשני לא  $\leftarrow$  לא.

(5) מזיהה את שע הראשים ימינה וחוזרת לשלב (3).

**שלבים (3-5):**  $O(|w|)$

זמן הריצה

זמן הריצה של  $M'$  הוא  $O(|w|)$ .

## 8.2 יחס בין הסיבוכיות של מ"ט סרט יחיד ומטמ"ס

### משפט 8.1

לכל מ"ט מרובת סרטים  $M$  הריצה בזמן  $f(n)$  קיימת מ"ט סרט יחיד'  $M'$  השקולה לו-  $M$  ורצה בזמן  $O(f^2(n))$ .

**הוכחה:**

בhinתן מ"ט מרובת סרטים  $M$ , הריצה בזמן  $f(n)$ , נבנה מ"ט עם סרט יחיד'  $M'$  באותו אופן כמו בהוכחת השקילות במשפט 3.1.

כולומר,  $M'$  שומרת את התוכן של  $k$  סרטים של  $M$  על הסרט היחיד שלו (עם הפרדה ע"י '#), ובכל צעד חישוב,  $M'$  סורקית את הסרט שלו כדי להזיהות שת האותיות שמתחאת הראשים (שמסומנות ב-  $\hat{\alpha}$ ) ואחרי זה, משתמשת בפונקציית המעברים של  $M$ , וسورקית את הסרט פעמי נספה כדי לעדכן את התוכן בכל אחד מהסרטים ואת מיקום הראש בכל אחד מהסרטים.

1)

2)

⋮  
⋮  
⋮

κ)

#	$\hat{\alpha}_1$	#	$\hat{\alpha}_2$	#	$\hat{\alpha}_3$	#	
---	------------------	---	------------------	---	------------------	---	--

כמה לוקח לנו  $M'$  לסרוק את הסרט שלה? מכיוון שהסרט של  $M'$  מכיל את התוכן של  $k$  הסרטים של  $M$ , והגודל של כל אחד מהסרטים של  $M$  חסום ע"י  $f(n)$ , גודל הסרט של  $M'$  חסום ע"י

$$k \cdot f(n) = O(f(n)) .$$

הוצאות של הסקירה של  $M'$  לסרט שלה היא  $O(f(n))$  וזה עלות של צעד חישוב בדיקה של  $M'$  על הקלט.

מכיוון ש-  $M$  רצה בזמן  $f(n)$ , זמן היזהה של  $M'$  חסום ע"י

$$f(n) \cdot O(f(n)) = O(f^2(n)) .$$

## 8.3 יחס בין הסיבוכיות של מ"ט דטרמיניסטי ומ"ט א"ד

### הגדרה 8.4

בהתנחת מ"ט א"ד  $M$ , זמן הריצה של  $M$  על קלט  $w$ , היא פונקציה  $f(|w|)$  השווה במספר הצעדים בחישוב המקסימלי של  $M$  על  $w$ .

### משפט 8.2

לכל מ"ט א"ד  $N$  הריצה בזמן  $f(n)$ , קיימת מ"ט דטרמיניסטי  $D$  השකלה ל-  $N$  ורצה בזמן  $.2^{(f(n))}$ .

**הוכחה:**

בhinתן מ"ט א"ד  $N$  הרצה בזמן  $f(n)$  מ"ט דטרמיניסטי  $D$  באותו אופן כמו בהוכחת השקלות במשפט 4.1. כלומר, בהינתן קלט  $w$ ,  $D$  תשרו את עץ החישוב של  $N$  ו-  $w$  לרוחב ותקבל כל אחד החישובים של  $N$  המסתויים כולם, בהינתן קלט  $w$ ,  $D$  מבצע חסום ע"י מספר הקודקודים בעץ החישוב של  $N$  ו-  $w$ . ב-  $q_{\text{acc}}$ .

בhinתן קלט  $w$  באורך  $n$ :

- כל מסלול בעץ החישוב של  $N$  על  $w$  חסום ע"י  $f(n)$ .
- מסגר החישובים ש-  $D$  מבצע חסום ע"י מספר הקודקודים בעץ החישוב של  $N$  ו-  $w$ .
- מכיוון שמספר הבנים של כל קודקוד בעץ החישוב חסום ע"י

$$C = 3|Q| \cdot |\Gamma|$$

מספר הקודקודים בעץ החישוב חסום ע"י

$$C^0 + C^2 + \dots C^{f(n)} \leq C^{f(n)+1} = C \cdot C^{f(n)}.$$

ולכן זמן הריצה של  $D$  חסום ע"י

$$f(n) \cdot C \cdot C^{f(n)} \leq C^{f(n)} \cdot C^{f(n)} = C^{2f(n)} = (C^2)^{f(n)} = 2^{C' \cdot f(n)} = 2^{O(f(n))}.$$

נתיחס כאן לשני החסמים הבאים:

1) חסם פולינומיAli הוא חסם מהצורה  $n^c$  עבור  $c > 0$  כלשהו.2) חסם אקספוננציאלי הוא חסם מהצורה  $2^{n^c}$  עבור  $c > 0$  כלשהו.

### הגדרה 8.5 בעיית הברעה

בעיית הברעה מוגדרת באופן הבא:

"בהינתן קלט כלשהו, האם הקלט מקיים תנאי מסוים "

### דוגמה 8.4

בhinתן מספר  $n$ , האם  $n$  ראשוני?

כל בעיית הברעה ניתנת לתאר כפשה שකולה:

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

### משפט 8.3

. שפה  $\equiv$  בעיית הברעה

**הגדרה 8.6 אלגוריתם זמן פולינומיAli**

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

**משפט 8.4 התזה של צירץ' (Church Thesis)**

אם קיים אלגוריתם המכריע בעיה בזמן פולינומיAli, אז קיימת מ"ט דטרמיניסטית המכריע את השפה השכללה לבעיה זו בזמן פולינומיAli.

. מכונת טיורינג ≡ אלגוריתם מכריע

**8.4 המחלקה  $P$** **הגדרה 8.7 המחלקה  $P$** 

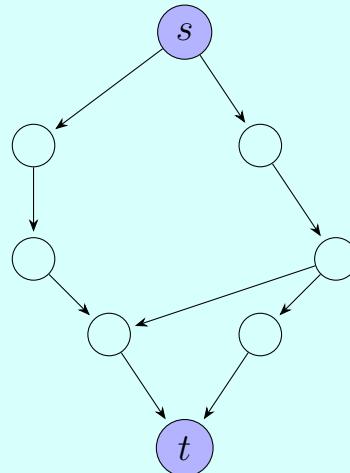
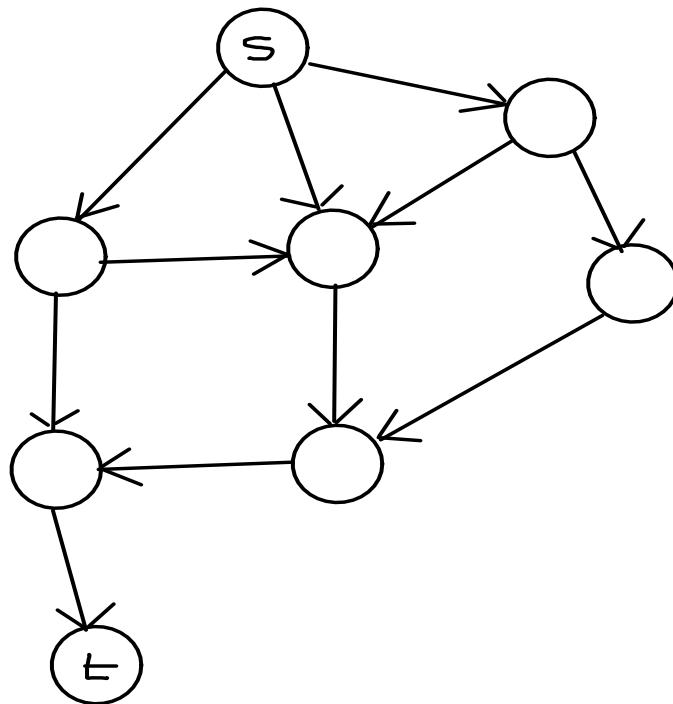
המחלקה  $P$  היא אוסף כל הבעיות (השפות) שקיים עבורן אלגוריתם (מכונת טיורינג דטרמיניסטית) המכריע אותן בזמן פולינומיAli.

**דוגמה 8.5**

$$L = \{a^n b^n \mid n \geq 0\} \in P .$$

**8.5 בעיית PATH**

## הגדרה 8.8 בעיית המסלול בגרף מכוען



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

פלט: האם קיים מסלול ב-  $G$  מ-  $s$  ל-  $t$  ?

$$PATH = \{\langle G, s, t \rangle \mid \text{קיים מסלול ב- } G \text{ מ- } s \text{ ל- } t\}$$

## משפט 8.5

$$PATH \in P .$$

**הוכחה:** בניית אלגוריתם  $A$  עבור הבעיה  $PATH$

$\langle G, s, t \rangle = A$

(1) צבע את  $s$ .

(2) מבצע  $|V| - 1$  פעמים:

- לכל צלע  $(u, v) \in E$
- \* אם  $u$  צבוע  $\Leftarrow$  צבע את  $v$ .
- אם  $t$  צבוע  $\Leftarrow$  החזיר "כן".
- אחרת  $\Leftarrow$  החזיר "לא".

זמן ריצה של האלגוריתם הוא  $O(|V| \cdot |E|)$  פולינומיAli במספר הקודקודים  $|V|$ .

האם זה פולינומיAli בגודל הקלט  $|\langle G \rangle|$ ?

איך נקודד את  $G$ ?

- נניח כי  $n = |V| = 1, 2, 3, \dots, n$ .
- נניח כי הצלעות נתונות ע"י מטריצה  $M$  בגודל  $n \times n$  כך ש-

$$M_{ij} = \begin{cases} 1 & (i, j) \in E \\ 0 & (i, j) \notin E \end{cases}.$$

- נניח כי מספרים מקודדים בסיסי ביניארי.

- איז גודל הקידוד של  $G$  שווה  $n^2 + n \log_2 n$ , כלומר

$$|\langle G \rangle| = \Omega(|V|^2) \Rightarrow |V| = O(|\langle G \rangle|).$$

ולכן כל אלגוריתם הרץ בזמן פולינומיAli במספר הקודקודים  $|V|$  ירוץ בזמן פולינומיAli בגודל הקידוד  $|\langle G \rangle|$ .

■  
ולכן  $A$  רץ בזמן פולינומיAli בגודל הקלט.

## RELPRIME 8.6 בעית

### הגדרה 8.9 מספרים זרים (Relatively prime)

שני מספרים  $x, y$  זרים אם המחלק המשותף הגדול ביותר, מסומן  $\text{gcd}(x, y)$ , שווה 1.

### הגדרה 8.10 בעית RELPRIME

קלט: שני מספרים  $x$  ו-  $y$ .

פלט: האם  $x$  ו-  $y$  זרים?

$$\text{RELPRIME} = \{\langle x, y \rangle \mid \text{gcd}(x, y) = 1\}.$$

## משפט 8.6

$$RELPRIME \in P .$$

**הוכחה:** נבנה אלגוריתם  $A$  המכרייע את  $RELPRIME$  בזמן פולינומייאלי.

האלגוריתם מבוסס על העובדה ש-

$$\gcd(x, y) = 1 \iff \langle x, y \rangle \in RELPRIME .$$

ולכן נשתמש באלגוריתם האוקלידי לחישוב  $\gcd$ :

$$\gcd(x, y) = \begin{cases} x & y = 0 \\ \gcd(y, x \bmod y) & y \neq 0 \end{cases} .$$

**הוכחה:** נסמן  $(qy + r) \text{ נסמן } r = x \bmod y \text{ ו } d = \gcd(x, y)$ . אזי קיימים שלמים  $s, t$  כך ש-  $sx + ty = d$ .

לכן

$$s(qy + r) + ty = d \Rightarrow sr + (t + sq)y = d \Rightarrow \gcd(x, y) = d = \gcd(y, r) .$$

לדוגמא:

$$\gcd(18, 32) = \gcd(32, 18) = \gcd(18, 14) = \gcd(14, 4) = \gcd(4, 2) = \gcd(2, 0) = 2 .$$

האלגוריתם האוקלידי:

על קלט  $x$  ו-  $y$ :

**(1)** כל עוד  $y \neq 0$ :

$$x \bmod y \rightarrow x \bullet$$

$$\text{swap}(x, y) \bullet$$

(כלומר מחליפים בין  $x$  ו-  $y$ ).

**(2)** מחזירים את  $x$ .

האלגוריתם  $A$  המכרייע  $RELPRIME$ 

על קלט  $\langle x, y \rangle = A$ :

**(1)** מרים את האלגוריתם האוקלידי על  $x$  ו-  $y$ .

- אם האלגוריתם האוקלידי החזר  $1 \Leftarrow$  מקבל.

- אחרת  $\Leftarrow$  דוחה.

נכונות האלגוריתם נובעת מנכונות האלגוריתם האוקלידי.

נוכיח כי  $A$  רץ בזמן פולינומייאלי בגודל הקלט.

טענת עזר:

$$\text{אם } x \bmod y < \frac{x}{2} \text{ אזי } x > y$$

הוכחה:

יש שתי אפשרויות:

$$\begin{aligned} & \bullet \text{ אם } y \leq \frac{x}{2} \\ x \mod y < y \leq \frac{x}{2}. \end{aligned}$$

$$\bullet \text{ נניח ש- } x < y < \frac{x}{2}.$$

מכיוון ש-  $(y - x) < 2y$ , וגם  $x = qy + (x \mod y)$  אז בהכרח  $2 < q$  ולכן  $x = qy + (x \mod y)$  ולכן  $y = x \mod y$ .

לפיכך

$$x \mod y = x - y < \frac{x}{2}.$$



לפי טענת העזר, אחרי כל איטרציה  $x$  קטן לפחות חצי.

מכיוון שבכל איטרציה מחליפים בין  $x$  ו-  $y$ , אחרי כל שתי איטרציות גם  $x$  וגם  $y$  קטנים לפחות חצי.

ולכן לאחר  $\log_2 y + \log_2 x$  איטרציות לפחות  $x$  או  $y$  שווים ל- 0.

ולכן מספר האיטרציות באlgorigithm האוקלידי חסום ע"י  $\log_2 x + \log_2 y$ , זה בדוק זמן הריצה של האlgorigithm  $A$ .  
ולכן  $A$  רץ בזמן פולינומילי בגודל הקלט.

ולכן

$$RELPRIME \in P.$$

