

שיעור 9

מבוא לסיבוכיות

9.1 הגדרה של סיבוכיות

9.1 הערה

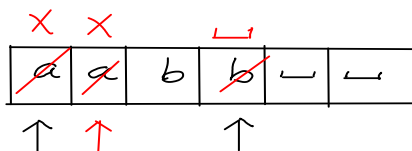
זמן ריצה של מ"ט M על קלט w , נמדד ביחס לגודל הקלט w , כלומר $f(|w|)$.

9.1 הגדרה

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

9.1 דוגמה

נבנה מ"ט M המכריעה השפה $L = \{a^n b^n \mid n \geq 0\}$.



התאור של M :

על קלט w :

- (1) אם התו שמתחת לראש הוא $_$ \Leftarrow מקבלת.
 - (2) אם התו שמתחת לראש הוא b \Leftarrow דוחה.
 - (3) מוחקת את התו שמתחת לראש ע"י X .
 - (4) מזיזה את הראש ימינה עד התו הראשון משמאל ל- $_$.
- אם התו הוא a או X \Leftarrow דוחה.
 - מוחקת את התו שמתחת לראש ע"י $_$, מזיזה את הראש שמאלה עד התו הראשון מימין ל- X וחוזרת ל- (1).

זמן הריצה

• $\frac{|w|}{2}$ איטרציות.

• בכל איטרציה מבצעים $O(|w|)$ צעדים.

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

הגדרה 9.2 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 9.2

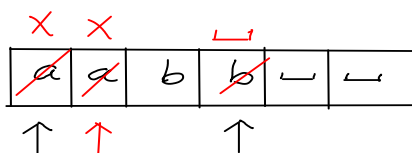
זמן הריצה של מ"ט נמדד ביחס לגודל הקלט $|w|$.

הגדרה 9.3

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

דוגמה 9.2

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



התאור של M :

על קלט w :

(1) אם התו שמתחת לראש הוא $_$ מקבלת.

(2) אם התו שמתחת לראש הוא b דוחה.

(3) מוחקת את התו שמתחת לראש ע"י X .

(4) מזיזה את הראש ימינה עד התו הראשון משמאל ל- $_$.

• אם התו הוא a או X דוחה.

• מוחקת את התו שמתחת לראש ע"י $_$, מזיזה את הראש שמאלה עד התו הראשון מימין ל- X וחוזרת ל- (1).

זמן הריצה

• M מבצעת $\frac{|w|}{2}$ איטרציות.

• בכל 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 9.3

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

1)

a	a	b	b	␣	␣
---	---	---	---	---	---

2)

6	6				
---	---	--	--	--	--

התאור של M' :

על קלט w :

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

(2) מזיזה את הראשים לתחילת הסרטים. $O(|w|)$

(3) אם שני הראשען מצביעים על ␣ מקבלת.

(4) אם אחד הראשים מצביע על ␣ והשני לא ␣ לא.

(5) מזיזה את שהע הראשים ימינה וחוזרת לשלב (3). שלבים (3-5): $O(|w|)$.

זמן הריצה

זמן הריצה של M' הוא $O(|w|)$.

9.2 יחס בין הסיבוכיות של מ"ט סרט יחיד ומטמ"ס

משפט 9.1

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

הוכחה:

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

כלומר, M' שומרת את התוכן של k סרטים של M על הסרט היחיד שלה (עם הפרדה ע"י #), ובכל צעד חישוב, M' סורקת את הסרט שלה כדי לזהות שת האותיות שמתחת לראשים (שמסומנות ב- \hat{a}) ואחרי זה, משתמשת בפונקצית המעברים של M , וסורקת את הסרט פעם נוספת כדי לעדכן את התוכן בכל אחד מהסרטים ואת מיקום הראש בכל אחד מהסרטים.

1) 2)

⋮

k)

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

כמה לוקח ל- 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

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

העלות של הסריקה של M' לסרט שלה היא $O(f(n))$ וזה עלות של צעד חישוב בריצה של M' על הקלט.

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

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

■

9.3 יחס בין הסיבוכיות של מ"ט דטרמיניסטית ומ"ט א"ד

הגדרה 9.4

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

משפט 9.2

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

הוכחה:

בהינתן מ"ט א"ד N הרצה בזמן $f(n)$ מ"ט דטרמיניסטית D באותו אופן כמו בהוכחת השקילות במשפט 4.1.

כלומר, בהינתן קלט w , D תסרו' את עץ החישוב של N ו- w לרוחב ותקבל כל אחד החישובים של N המסתיים ב- q_{acc} .

בהינתן קלט w באורך n :

- כל מסלול בעץ החישוב של N על w חסום ע"י $f(n)$.
- מספר החישובים ש- D מבצעת 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

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

נתייחס כאן לשני החסמים הבאים:

■

(1) חסם פולינומיאלי הוא חסם מהצורה n^c עבור $c > 0$ כלשהו.

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

הגדרה 9.5 בעיית הכרעה

בעיית הכרעה מוגדרת באופן הבא:

"בהינתן קלט כלשהו, האם הקלט מקיים תנאי מסוים"

דוגמה 9.4

בהינתן מספר n , האם n ראשוני?

כל בעיית הכרעה ניתן לתאר כפשה שקולה:

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

משפט 9.3

. שפה \equiv בעיית הכרעה

הגדרה 9.6 אלגוריתם זמן פולינומיאלי

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

משפט 9.4 התזה של צירץ' (Church Thesis)

אם קיים אלגוריתם המכריע בעייה בזמן פולינומיאלי, אז קיימת מ"ט דטרמיניסטית המכריעה את השפה השקולה לבעייה זו בזמן פולינומיאלי.

. מכונת טיורינג \equiv אלגוריתם מכריעה

9.4 המחלקה P **הגדרה 9.7 המחלקה P**

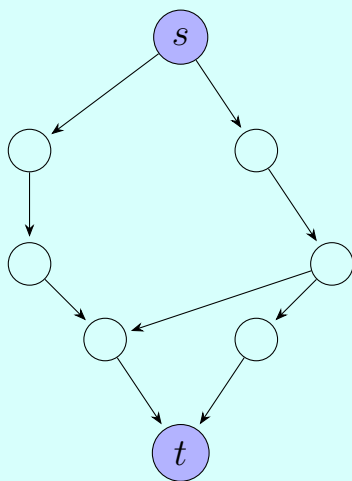
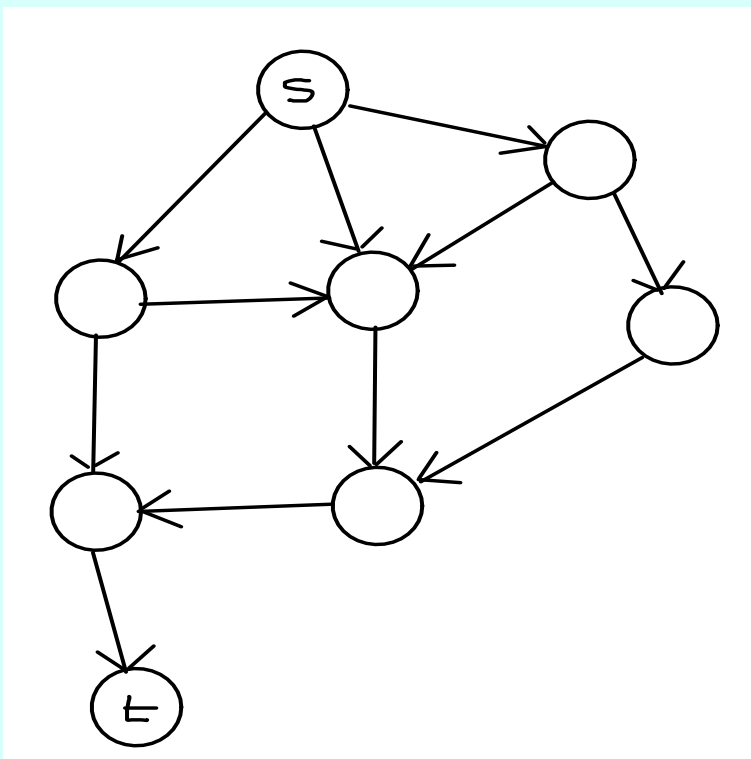
המחלקה P היא אוסף כל הבעיות (השפות) שקיים עבורן אלגוריתם (מכונת טיורינג דטרמיניסטית) המכריע אותן בזמן פולינומיאלי.

דוגמה 9.5

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

9.5 בעיית PATH

הגדרה 9.8 בעיית המסלול בגרף מכוון



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

פלט: האם קיים מסלול ב- G מ- s ל- t ?

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

משפט 9.5

$$PATH \in P.$$

הוכחה: נבנה אלגוריתם A עבור הבעיה $PATH$.

$A = \langle G, s, t \rangle$ על קלט

(1) צובע את s .

(2) מבצע $|V| - 1$ פעמים:

• לכל $(u, v) \in E$ צלע

* אם u צבוע \Leftarrow צבע את v .

(3) • אם t צבוע \Leftarrow החזיר "כן".

• אחרת \Leftarrow החזיר "לא".

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

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

איך נקודד את G ?

• נניח כי $|V| = n$ ו- $V = \{1, 2, 3, \dots, n\}$.

• 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 בבסיס ביניארי.

• אזי 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 פולינומיאלי במספר הקודקודים $|V|$ ירוץ בזמן פולינומיאלי בגודל הקידוד $|\langle G \rangle|$.



ולכן A רץ בזמן פולינומיאלי בגודל הקלט.

9.6 בעיית RELPRIME

הגדרה 9.9 מספרים זרים (Relatively prime)

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

הגדרה 9.10 בעיית RELPRIME

קלט: שני מספרים x ו- y .

פלט: האם x ו- y זרים?

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

משפט 9.6

$$RELPRIME \in P.$$

הוכחה: נבנה אלגוריתם A המכריע את $RELPRIME$ בזמן פולינומיאלי.

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 $d = \gcd(x, y)$. אזי קיימים שלמים s, t כך ש- $dx + ty = d$. נסמן $r = x \bmod y$. אז $x = qy + r$.
לכן

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

לדוגמה:

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

האלגוריתם האוקלידי:

על קלט x ו- y :

(1) כל עוד $y \neq 0$

$$x \bmod y \rightarrow x$$

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

(כלומר מחליפים בין x ו- y).

(2) מחזירים את x .

האלגוריתם A המכריע $RELPRIME$:

$A = \text{על קלט } \langle x, y \rangle$

(1) מריץ את האלגוריתם האוקלידי על x ו- y .

• אם האלגוריתם האוקלידי החזיר 1 מקבל.

• אחרת דוחה.

נכונות האלגוריתם נובעת מנכונות האלגוריתם האוקלידי.

נוכיח כי A רץ בזמן פולינומיאלי בגודל הקלט.

טענת עזר:

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

הוכחה:

יש שתי אפשרויות:

• אם $y \leq \frac{x}{2}$ אזי

$$x \bmod y < y \leq \frac{x}{2}.$$

• נניח ש- $\frac{x}{2} < y < x$

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

לפיכך

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

■

לפי טענת העזר, אחרי כל איטרציה x קטן בלפחות חצי.מכיוון שבכל איטרציה מחליפים בין x ו- y , אחרי כל שתי איטרציות גם x וגם y קטנים בלפחות חצי.ולכן לאחר $\log_2 x + \log_2 y$ איטרציות לפחות x או y שווים ל-0.ולכן מספר האיטרציות באלגוריתם האוקלידי חסום ע"י $\log_2 x + \log_2 y$, וזה בדיוק זמן הריצה של האלגוריתם A .ולכן A רץ בזמן פולינומיאלי בגודל הקלט.

ולכן

$$RELPRIME \in P.$$

■