

שיעור 9

מבוא לסיבוכיות זמן

9.1 הגדרה של סיבוכיות זמן

הגדרה 9.1 זמן הריצה של מבנות טיריניג

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

הערה 9.1

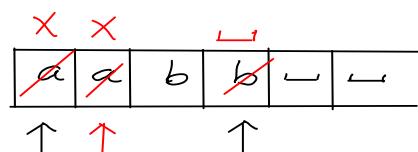
זמן הריצה של מ"ט M על קלט w , נמדד ביחס לגודל הקלט w , כלומר $f(|w|)$.

הגדרה 9.2 סיבוכיות זמן של בעיה/שפה

בاهינתן קלט w באורך $|w| = n$. אומרים כי ניתן להכריע שפה L בזמן $f(n)$ אם קיימות מ"ט M המכrijעה את L כך שלכל $w \in \Sigma^*$, זמן הריצה של M על w חסום ע"י $f(|w|)$.

דוגמה 9.1 (דוגמה של סיבוכיות זמן של שפה)

نبנה מ"ט M עם סרט ייחיד שמכrijעה 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 שמאליה עד התו הראשון מימין לו $- X$ וחוזרת $- (1)$.

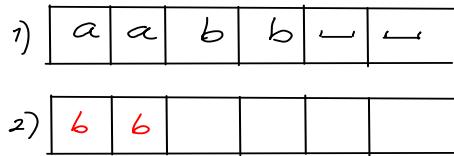
זמן הריצה

- M מבצעת $\frac{|w|}{2}$ איטרציות.
- בכל איטרציה M סורקת את הרצף פעמיים זהה עליה ($O(|w|)$).
- לכן סה"כ זמן הריצה של M חסום ע"י

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

דוגמה 9.2 (דוגמה של סיבוכיות זמן של שפה)

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



התאזר 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 שהע הראשים ימינה וחוזרת לשלב (3).

שלבים (3-5): $O(|w|)$

זמן הריצה

זמן הריצה של M' הוא $O(|w|)$.

הגדרה 9.3 תחילה

תהי $f : \mathbb{N} \rightarrow \mathbb{R}^+$ פונקציה מהטבועים אל הממשיים הא-שליליים. תחילה ($TIME(f(n))$) היא האוסף של כל השפות ש刻画ות ע"י מכונת טירינג $O(f(n))$.

דוגמה 9.3 (דוגמה של מחלוקת-זמן של שפה)

עבור השפה $L \in TIME(n^2)$ בדוגמה 9.1

דוגמה 9.4 (דוגמה של מחלוקת-זמן של שפה)עבור השפה $L \in TIME(n)$ בדוגמה 9.2:**9.2 יחס בין הסיבוכיות של מ"ט סרט יחיד ומטמ"ס****משפט 9.1**

לכל מ"ט מרובה סרטים M הרצה בזמן $f(n)$ קיימת מ"ט סרט יחיד M' השකולה לו- M ורצה בזמן $O(f^2(n))$.

הוכחה:

בhinntן מ"ט מרובה 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 שלו (עם הפרדה ע"י $\#$), ובכל צעד חישוב, M' סורקת את הסרט שלו כדי לאזות שת האותיות שמתחת הראשים (משמעות ב- $\hat{\alpha}$) ואחרי זה, משתמש בפונקציית המעברים של M , וسورקת את הסרט פעמי' נספה 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 לו- M' לסרוק את הסרט שלו? 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 היררכיה של M' לסדרת שלה היא $O(f(n))$ וזה עלות של צעד חישוב ביררכיה של M' על הקלט. מכיוון ש- M ריצה בזמן $f(n)$, זמן היררכיה של M' חסום ע"י $f(n) \cdot O(f(n)) = O(f^2(n))$.

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

הגדרה 9.4

בاهינתן מכונת טיורינג אי-דטרמיניסטית M , זמן היררכיה של M על קלט w , היא פונקציה $f(|w|)$ השווה למספר הצעדים בחישוב המקסימלי של M על w .

משפט 9.2

לכל מכונת טיורינג א-דטרמיניסטית N הריצה בזמן $f(n)$, קיימת מכונת טיורינג דטרמיניסטית D השקולה ל- N שריצה בזמן $2^{f(n)}$.

הוכחה:

בاهינתן מכונת טיורינג א-דטרמיניסטית N הריצה בזמן $f(n)$ מכונת טיורינג דטרמיניסטית D באותו אופן כמו בהוכחת השקילות במשפט 4.1.

כלומר, בהינתן קלט w , D תסrox את עץ החישוב של N ו- w לרוחב ותקבל כל אחד החישובים של N המסתויים ב- w .

בاهינתן קלט w באורך n :

- כל מסלול בעץ החישוב של N על w חסום ע"י $f(n)$.
- מסמר 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 היררכיה של D חסום ע"י

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

נתיאחס 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.

הגדירה 9.5 בעיית הכרעה

בעיית הכרעה מוגדרת באופן הבא:

"בhinintן קלט כלשהו, האם הקלט מקיים תנאי מסוים"

דוגמה 9.5

בhinintן מספר n , האם n ראשוני?

כל בעיית הכרעה ניתן לתאר כשפה שקולה:

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

משפט 9.3

. שפה \equiv בעיית הכרעה

הגדירה 9.6 אלגוריתם זמן פולינומיAli

אומרים כי אלגוריתם A מכרייעת בעיה בזמן פולינומיAli אם קיים קבוע $0 < c$ 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 המכרייע בעיה בזמן פולינומיAli, אז קיימת מ"ט דטרמיניסטיבית המכרייע את השפה השקולה לבעיה זו בזמן פולינומיAli.

. מכונת טיורינג \equiv אלגוריתם מכרייע

9.4 המחלקה P **הגדירה 9.7 המחלקה P**

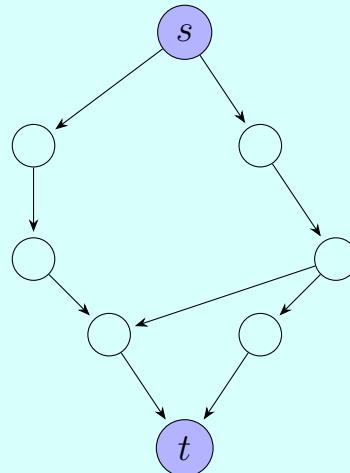
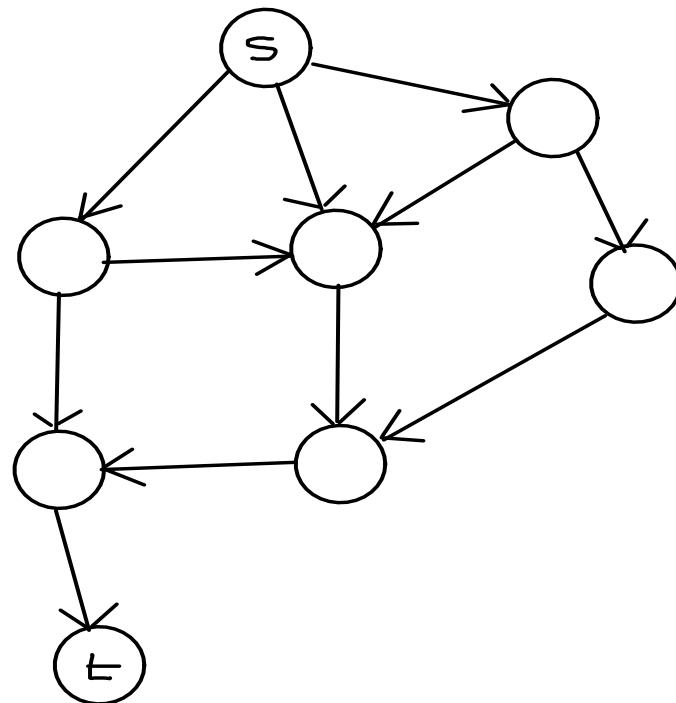
המחלקה P היא אוסף כל הבעיות (השפות) שקיימים עבורן אלגוריתם (מכונת טיורינג דטרמיניסטיבית) המכרייע אותן בזמן פולינומיAli.

דוגמה 9.6

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

9.5 בעיית PATH

הגדירה 9.8 בעיית המסלול בגרף מכובן



קלט: גרף מכובן $G = (V, E)$ 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 9.5

$PATH \in P$.

הוכחה: בניית אלגוריתם A עבור הבעיה $.PATH$

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

(1) צובע 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 נתנות 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 בסיס ביניاري.
- 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 פולינומיAli במספר הקודקודים $|V|$ ירוץ בזמן פולינומיAli בגודל הקידוד $|\langle G \rangle|$.

■
ולכן A רץ בזמן פולינומיAli בגודל הקלט.

9.6 הביעית RELPRIME

הגדרה 9.9 מספרים זרים (Relatively prime)

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

הגדרה 9.10 ביעית RELPRIME

קלט: שני מספרים x ו- y .

פלט: האם x ו- y זרים?

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

הוכחנו נכון להכריע את $RELPRIME \in P$ בזמן פולינומי, כלומר נוכחה במשפט 9.8 למטה. לפניכן נסביר את האלגוריתם של אוקלידס למציאת ה- \gcd של שני שלמים, ומתוך זה נוכל לחשב את הסיבוכיות זמן של $RELPRIME$. ראשית נזכיר משפט שלמדנו בקורסים קודמים:

משפט 9.6 המשפט של האלגוריתם של אוקלידס

אם x, y שלמים אז

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

הוכחה: ההוכחה היא לא חלק של הקורס ומופיע בסעיף האחרון "הוכחות של משפטי שימושיים" בדף 103.

האלגוריתם של אוקלידס הוא אלגוריתם, שמקבל כקלט שני מספרים y, x ופולט את $\gcd(x, y)$. הוא מתבסס על המשפט 9.6. האלגוריתם עצמו הוא כדלקמן:

על קלט $\langle x, y \rangle$ כאשר y, x מספרים שלמים בבסיס בינארי:

(1) כל עוד $y \neq 0$:

(2) $x \leftarrow x \bmod y$

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

(כלומר מחליפים בין x ו- y).

(4) מחזירים את x .

לדוגמה:

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

כדי להוכיח כי $RELPRIME \in P$ נדרש למשפט עזר הבא:

משפט 9.7 (משפט עזר)

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

הוכחה: ההוכחה היא לא חלק של הקורס ומופיע בסעיף האחרון "הוכחות של משפטי שימושיים" בדף 104.

משפט 9.8

$$RELPRIME \in P.$$

הוכחה:

נבנה אלגוריתם A המכريع את $RELPRIME$ בזמן פולינומילי. $RELPRIME$ היא השפה של הבעיה שמקבלת כקלט שני מספרים שלמים x, y ומחייבת תשובה לשאלת, האם x, y זרים. כלומר:

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

לכן A משתמש באלגוריתם של אוקלידס $EUCLID(x, y)$ כדי לחשב $\gcd(x, y)$.

בנייה האלגוריתם A המכريع

"על קלט $\langle x, y \rangle$ כאשר x, y שלמים בסיסיים ביןaries: A מרייך את $EUCLID$ על x ו- y .

- אם $\gcd(x, y) = 1$ אז A מקבל.

- אחרת A דוחה."

הוכחת הנכונות

הנכונות של A מנובעת ישירות מהנכונות של האלגוריתם האוקלידס, $EUCLID$.

סיבוכיות זמן

נראה כי A רץ בזמן פולינומילי בגודל הקלט $\langle x, y \rangle$.

- לפי משפט עזר 9.7: $x < \frac{x}{2} \bmod y$.
- בכל איטרציה, בשלב (2) המשתנה x מקבל את הערך החדש $x \leftarrow x \bmod y$.
- לכן בכל איטרציה הערך החדש של x קטן ממש מחצי של הערך הקודם של x .
- לכן אחרי כל איטרציה, x קטן לפחות חצי.
- בשלב (3), A מחליף בין x ו- y , אז אחרי כל 2 איטרציות, גם x קטן לפחות חצי וגם y קטן לפחות חצי.
- לכן המספר הפעמים המקסימלי שאפשר לבצע שלבי (2) ו- (3) היא $m = \min(2 \lfloor \log_2 x \rfloor, 2 \lfloor \log_2 y \rfloor)$.
- לכן המספר האיטרציות המקסימלי של $EUCLID$ הוא $m = \min(2 \lfloor \log_2 x \rfloor, 2 \lfloor \log_2 y \rfloor)$.
- יהי n האורך של הקלט. כלומר $n = \text{האורך של המחרוזות של השלמים } x \text{ ו- } y \text{ בסיסיים ביןaries}$.

$$m \leq n$$

- לכן A דורש $O(n)$ צעדים.
- כל איטרציה של $EUCLID$ מתבצע בזמן פולינומילי.
- clone קיים טבעי k עבורו כל איטרציה של $EUCLID$ מתבצע בזמן $O(n^k)$.
- לכן $A \in TIME(n^{k+1})$ ($EUCLID \in TIME(n^{k+1})$ (ראו הגדרה 9.3) ולכן $RELPRIME \in P$.

לכן A רץ בזמן פולינומילי בגודל הקלט. לכן

$$RELPRIME \in P.$$



9.7 *הוכחות של משפטי שימושיים

משפט 9.9 המשפט של האלגוריתם של אוקלידסאם x, y שלמים אז

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

הוכחה: (להעשרה בלבד)

המטרה של ההוכחה זו היא רק להוסיף הבנה להוכחה של משפט 9.8 לסיבוכיות זמן של *RELPRIME* למטרה. היא לא הוכחה שאותם תיבחנו עלייה ואפשר לדלג עליה.

נתחיל אם משפט החלוק של אוקלידס, שאומר שאם x, y שלמים אז קיימים שלמים q ו- $r \leq 0$ כך ש:

$$x = qy + r = \left\lfloor \frac{x}{y} \right\rfloor y + (x \bmod y). \quad (1*)$$

נגיד $d \triangleq \gcd(x, y)$.
מכיוון ש- d הוא מחלק משותף של x ו- y אז $d \mid x$ ו- $d \mid y$ וגם $d \mid (x \bmod y)$. לכן בaczות מסוואה (1*):

$$(d \mid x) \wedge (d \mid y) \xrightarrow{\text{משוואת (1*)}} d \mid (x \bmod y)$$

וז"א וגם $d \mid (x \bmod y)$ אז בהכרח:

$$d \mid \gcd(y, x \bmod y). \quad (2*)$$

כעת נגיד $\bar{d} \triangleq \gcd(y, y \bmod x)$.
מכיוון ש- \bar{d} הוא מחלק משותף של y ו- $y \bmod x$ אז $\bar{d} \mid y$ ו- $\bar{d} \mid y \bmod x$. לכן בaczות מסוואה (1*):

$$(\bar{d} \mid y) \wedge (\bar{d} \mid x \bmod y) \xrightarrow{\text{משוואת (1*)}} \bar{d} \mid x$$

וז"א וגם $\bar{d} \mid x$ אז בהכרח:

$$\bar{d} \mid \gcd(x, y). \quad (3*)$$

לסיכום, לפי משוואות (2*) ו- (3*):
 $d \mid \bar{d} \wedge \bar{d} \mid d$.

מכיוון ש- $\gcd(x, y) = \gcd(y, x \bmod y)$ אז בהכרח $d = \bar{d}$, $d > 0$.

משפט 9.10 (משפט עזר)אם $x \bmod y < \frac{x}{2}$ אז $x > y$.**הוכחה:** יש שני מקרים:

$$y \leq \frac{x}{2} \quad (1)$$

$$y > \frac{x}{2} \quad (2)$$

נווכיח את הטענה עבור שני המקרים.

מקרה 1: $y \leq \frac{x}{2}$

לפי משפט החלוק של אוקלידס אם x, y שלמים Überom $x > y$ אז קיימים $q = x \text{ mod } y$ ו- $r = qy + r = \left\lfloor \frac{x}{y} \right\rfloor y + (x \text{ mod } y)$.

$x \text{ mod } y < y \leq \frac{x}{2}$ לפיכך $y \leq \frac{x}{2}$ ובפרט $r < y$ וגם $0 \leq r < y$.

מקרה 2: $y > \frac{x}{2}$

לפי משפט החלוק של אוקלידס אם x, y שלמים Überom $x > y$ אז קיימים $q = x \text{ mod } y$ ו- $r = qy + r = \left\lfloor \frac{x}{y} \right\rfloor y + (x \text{ mod } y)$.

בפרט אם $q = \left\lfloor \frac{x}{y} \right\rfloor$ ו- $x > y$ אז $x < 2y$. מכיוון ש- $q < 2$. אז בהכרח המינימלי של q הוא 1. לכן אם $q < 2$ בהכרח $q = 1$. לכן יש לנו

$$x = qy + r = (1)(y) + ry + (x \text{ mod } y).$$

מכאן

$$x - y = x \text{ mod } y.$$

כעת נציב את ההנחה ההתחלטית $x - y < \frac{x}{2}$ ונקבל $y > \frac{x}{2}$

$$x \text{ mod } y < \frac{x}{2}.$$

