

שיעור 9

מבוא לסיבוכיות זמן

9.1 הגדרה של סיבוכיות זמן

עד כה כל הבעיות החישוביות שעשכנו בהן הניחו שהמשאים שעומדים לרשות מכונת הטיורינג שפותרת אותן הם **בלתי מוגבלים**. כתע נ עבור לעסוק בשאלת מה קורה כאשר אנחנו מוגבלים חלק ממשאים אלו. יש סוגים רבים של ממשאים שנייתן לעסוק בהם, אבל שני הנפוצים ביותר בתיאוריה של מדעי המחשב הם

- **זמן חישוב**,

- **הזיכרון שנדרש לצורך החישוב**.

אתה מהבעיות שבהן נתקלים:
 כשמעוניינים למדוד את צרכית המשאים הללו של אלגוריתם מסוים היא שלא ברור כיצד למדוד אותם.
 האם זמן חישוב נמדד בשניות?
 אם כן, כיצד ניתן לחשב את זמן החישוב עבור אלגוריתם נתון?
 האם علينا לקודד ולהריץ אותו על מחשב מסוים?

אבל במחשבים שונים האלגוריתם ירוץ זמן זנים שונים בשל

- **יעילות המעבד**,

- **אופטימיזציות שמתבצעות ברמת המעבד**,

- **אופטימיזציות בזמן הקומפליציה**,

וכיווץ בהן.

אפיו תנאים חיצוניים כמו החום בסביבת המעבד עשויים להשפיע על זמן הריצה. מכאן הרצון למצוא הגדרה **תיאורטיבית** של זמן ריצה, שאינה תלולה בחומרה זו או אחרת.

הערה 9.1

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

הגדרה 9.1 זמן הריצה של מכונת טיורינג

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

הגדרה 9.2 סיבוכיות זמן של בעיה/שפה

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

דוגמה 9.1 סיבוכיות זמן של השפה של מחרוזות האוניריות

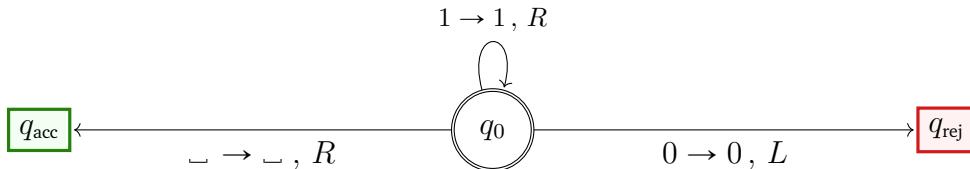
נתבונן על השפה של מחרוזות האוניריות הבאה:

$$L = \{1^n \mid n \geq 1\}.$$

בנייה מכונית טיורינג הבאה שמכריעה אותה:

$$M = (Q, q_0, \Sigma, \Gamma, \delta, q_{acc}, q_{rej})$$

כאשר $\Sigma = \{0, 1\}$ ו- $\Gamma = \{0, 1\}$. המ מצבים והמעברים מתוארים בהתרשים מצבים של מטפה:



בכדי לחשב את הסיבוכיות זמן של L בהתאם למוגנה בפסאודוקוד:

M על כל קלט w :

- (1) • אם המילה היא מילת הריקה תדחה.
- אחרת ממשיכה לשלב (2).
- (2) • אם התו הנקרא 0 תדחה.
- אחרת אם התו הנקרא הוא \sqcup מקבל.
- אחרת חוזרת לשלב (2).

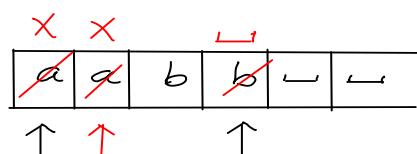
כל שהקלט ארוך יותר, כך M תבצע צעדי חישוב נוספים יותר. בפרט המספר הצעדים המקסימלי הוא במקרה שקלט w יש רק תווי 1 ולכון המ"ט תבצע $|w| = n$ צעדי חישוב. בכל מקרה אחר היא תבצע לפחות מ- n צעדים.

$$\begin{aligned} &\Leftarrow \text{חסם העליון של מספר צעדי חישוב של } M \text{ על קלט } w \text{ הוא } n \text{ כאשר } |w| = n. \\ &\Leftarrow M \text{ עוצרת בזמן } O(n). \\ &\Leftarrow L \text{ כריעה בזמן } O(n). \\ &\Leftarrow L \in TIME(n). \end{aligned}$$

באופן כללי, אם מכונה על קלט w מבצעת פחותה מ- $|w|$ צעדי חישוב, המשמעות היא המכונה כלל לא קראה את כל הקלט, וזה אינו נדיר במיוחד (אם כי הוא בחילוט קיים). אם כן ברור שמידות זמן חריצת היא תמיד **ביחס לאורך הקלט**.

דוגמה 9.2

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



התאור של M

על קלט *w*:

- (1) אם הינו שמתוחת לראש הוא \perp מקבלת.
 - (2) אם הינו שמתוחת לראש הוא $b \perp$ דוחה.
 - (3) מוחקמת את הינו שמתוחת לראש ע"י X .
 - (4) מזיהה את הראש ימינה עד הינו הראשון משמאלו ל- \perp .
 - אם הינו הוא a או $X \perp$ דוחה.
 - מוחקמת את הינו שמתוחת לראש ע"י \perp , מזיהה את רוחזורתת ל- (1).

זמן הרצאה

- M מבצעת $\frac{|w|}{2}$ איטרציות.
 - בכל איטרציה M סורקת את הסרט פעמיים וזה עולה $O(|w|)$.
 - לבו מה"כ זמו הריצה של M חסום ע"י

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

9.3 דוגמה

.L = {aⁿbⁿ | n ≥ 0} נבנה מ"ט מרובת סרטיים' M שמכריעת את השפה

1)	a	a	b	b	—	—
2)	6	6				

התאור של M'

על קלט *w*:

זמן הריצה

זמן הריצה של M' הוא $O(|w|)$.

הגדרה 9.3 $TIME(f(n))$

נגיד הקבוצת השפות $L \in TIME(f(n))$ כך שלכל שפה L קיימת מכונת טיריניג דטרמיניסטיבית שמכריעה את L בזמן לכל היותר $f(n)$, כאשר n הוא האורך של הקלט:

$$TIME(f(n)) = \{L \mid O(f(n)) \text{ בזמן } L \text{ המכrichtה } f(n)\}.$$

דוגמה 9.4

עבור השפה בדוגמה 9.2:

$$L \in TIME(n^2).$$

דוגמה 9.5

עבור השפה בדוגמה 9.3:

$$L \in TIME(n).$$

9.2 יחס בין הסיבוכיות של מכונת טיריניג עם סרט יחיד ומכונת טיריניג מרובת סרטים

משפט 9.1

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

הוכחה:

בבהינתן 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 הסרטו שלו כדי לזהות שת האותיות שמתחאת הראשים (משמעות ב- \hat{a}) ואחרי זה, משתמשת בפונקציית המעברים של M , וسورקת 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

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

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

מכיוון ש- M רצה בזמן $(f(n), f)$, 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 דטרמיניסטי ומ"ט א"ד

משפט 9.2

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

הוכחה:

בහינתן מ"ט א"ד N ריצה בזמן (n, f) מ"ט דטרמיניסטי D באותו אופן כמו בהוכחת השקילות המשפט 4.1.

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

בהינתן קלט w באורך n :

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

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

נתיחס כאן לשני החסמים הבאים:



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

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

9.4 החלוקת P

הגדרה 9.4 בעיית הכרעה

בעיית הכרעה מוגדרת באופן הבא:

"בהינתן קלט כלשהו, האם הקלט מקיים תנאי מסוים "

דוגמה 9.6

בהינתן מספר n , האם n ראשוני?

כל בעיית הכרעה ניתן לתאר כפשה שකולה:

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

משפט 9.3

. שפה \equiv בעיית הכרעה

הגדרה 9.5 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 9.4 התזה של צירץ' (Church Thesis)

אם קיים אלגוריתם המכריע בעיה בזמן פולינומיAli, אז קיימת מכונת טיורינג דטרמיניסטיבית המכריע את השפה השקולה לבעיה זו בזמן פולינומיAli.

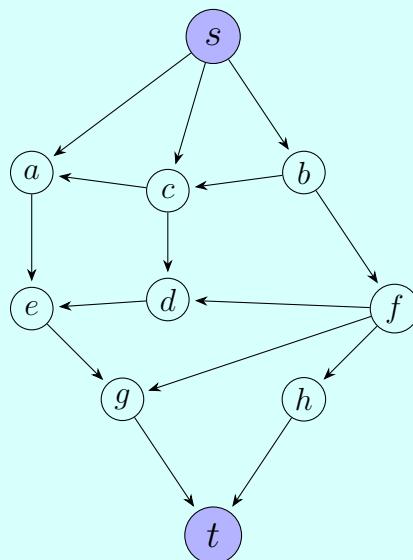
מכונת טיורינג \equiv אלגוריתם מכריע.

הגדרה 9.6 המחלקה P

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

דוגמה 9.7

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

9.5 בעיית PATH**הגדרה 9.7 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 ?

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

$PATH \in P$.

הוכחה: נבנה 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 $\langle G \rangle$?

- 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 בבסיס בינארי.

• 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.

9.6 הביעית RELPRIME

הגדרה 9.8 מספרים זרים (Relatively prime)

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

הגדרה 9.9 בעית RELPRIME

קלט: שני מספרים x ו- y .

פלט: האם x ו- y זרים?

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

אנחנו נוכיח כי ניתן להכريع את $RELPRIME \in P$ בזמן פולינומיAlg, כלומר נוכיח נוכחה במשפט 9.8 למטה. לפניכן נסביר את האלגוריתם של אוקלידס למציאת ה- \gcd של שני שלמים, ומתווך זה נוכל לחשב את הסיבוכיות זמן של $RELPRIME$. ראשית נזכיר משפט שלמדו 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 משפטיים שימושיים" בדף 104. האלגוריתם של אוקלידס הוא אלגוריתם, שמקבל קלט שני מספרים y, x ופלט את $\gcd(x, y)$. הוא מtabוסס על המשפט 9.6. האלגוריתם עצמו הוא כדלקמן:

: x, y על קלט = EUCLID

(1) כל עוד $0 \neq y$:

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

(3) 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 $P \in RELPRIME$ 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 משפטיים שימושיים" בדף 105.

משפט 9.8

$$RELPRIME \in P .$$

הוכחה:

نبנה אלגוריתם A המכريع את $RELPRIME$ בזמן פולינומיAli. $RELPRIME$ היא השפה של ה בעיה, שמקבלת כקלט שני מספרים שלמים x, y ומחזירה תשובה לשאלת, האם y , x זרים. ככלומר:

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

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

בנייה האלגוריתם A המכሩע

"על קלט $\langle x, y \rangle$: מרים את $EUCLID$ על x ו- y . $= A$

- אם $\gcd(x, y) = 1$ מחזיר A $EUCLID(x, y)$ מתקבל.
- אחרת A דוחה."

הוכחת הנכונות

הנכונות של A מנובעת ישיר מהנכונות של האלגוריתם האוקלידי, $EUCLID$.

סיבוכיות זמן

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

- לפי משפט עזר 9.7: $x \mod y < \frac{x}{2}$
- בכל איטרציה, בשלב (2) המשטנה x מקבל את הערך החדש $x \mod y$.
- 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 המקסימלי של פעמים שאפשר לבצע שלבי (2) ו- (3) היה $\min(2 \lfloor \log_2 x \rfloor, 2 \lfloor \log_2 y \rfloor)$.
- לכן המספר המקסימלי של האיטרציות ש $EUCLID$ מבצע הוא $m = \min(2 \lfloor \log_2 x \rfloor, 2 \lfloor \log_2 y \rfloor)$.
- זה בדיקן זמן הריצה של האלגוריתם A .

ולכן A רץ בזמן פולינומיAli בגודל הקלט.

ולכן

$$RELPRIME \in P.$$



9.7 *הוכחות של משפטיים 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- $r = qy + r = \left\lfloor \frac{x}{y} \right\rfloor y + (x \text{ mod } y)$.

$$\text{בפרט } r < y \text{ ו- } \frac{x}{2} \leq y \text{ לפיכך } x \leq \frac{3x}{2} \text{ ו- } 0 \leq r < y$$

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 $y > \frac{x}{2}$

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

