חישוביות וסיבוכיות תשפ"ה סמסטר א'
שיעור 5
בעיות NP שלמות

תוכן העניינים

5.1 הגדרת חישוב יעיל

עד כה כל הבעיות החישוביות שעסקנו בהן הניחו שהמשאבים שעומדים לרשות מכונת הטיורינג שפותרת אותן הם **בלתי מוגבלים**. כעת נעבור לעסוק בשאלה מה קורה כאשר אנחנו מגבילים חלק ממשאבים אלו. יש סוגים רבים של משאבים שניתן לעסוק בהם, אבל שני הנפוצים ביותר בתיאוריה של מדעי המחשב הם

- **זמן החיושב**
- **הזיכרון שנדרש לצורך החיושב**.

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

אבל במחשבים שונים האלגוריתם ירוץ זמנים שונים בשל

- יעילות המעבד,
- אופטימיזציות שמתבצעות ברמת המעבד,
- אופטימיזציות בזמן הקומפליציה,

וכיוצא בהן.

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

מכונת טיורינג היא סביבה טבעית להגדרה כזו:

הגדרה 5.1: זמן הריצה

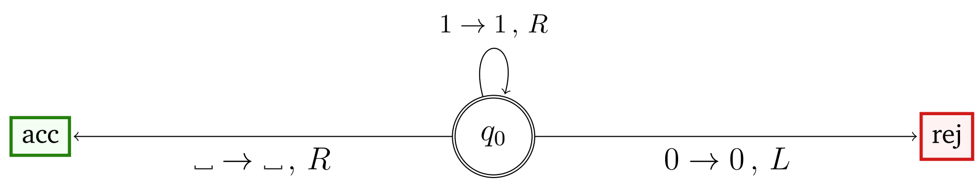
זמן הריצה של מכונת טיורינג M על קלט w הוא מספר צעדי החישוב ש- M מבצעת על w.

נשים לב לכך שמספר צעדי החישוב עשוי להיות אינסופי, אבל כמובן שסיטואציה כזו אינה רלוונטית לנו אם אנו מעוניינים להגביל את זמן הריצה.

בעיה נוספת היא שעל פי רוב, זמן הריצה של אלגוריתם תלוי ב **גודל הקלט** $|w|$ שמוזן אליו.

דוגמה 5.1

נתבונן על מ"ט $M = (Q, q_0, \Sigma, \Gamma, \delta, \text{acc}, \text{rej})$ כאשר $\Sigma = \{0,1\}$ ו- $\Gamma = \{0,1,\sqcup\}$ שמכריעה את השפה $L = \{1^n | n \geq 1\}$ של מחרוזות האוניריות.



- על קלט w, המכונה פשוט עוברת סדרתית על כל תווי w.
- אם אחד מהם 0 היא דוחה,
- ואם הגיעה אל $\sqcup$ שבסוף הקלט היא מקבלת.
- ככל שהקלט ארוך יותר, כך M תבצע צעדי חישוב רבים יותר.

ברור כי המספר הצעדים המקסימלי הוא במקרה שבקלט w יש רק תווי 1 ולכך המ"ט תבצעת $n = |w|$ צעדי חישוב. בכל מקרה אחר היא תבצעת $< n$ צעדים.

אנחנו אומרים כי "זמן הריצה של M הוא n" כאשר n אורך הקלט, בגלל שמספר הצעדים המקסימלי הוא n.

באופן כללי, אם מכונה על קלט w מבצעת פחות מ- $|w|$ צעדי חישוב, המשמעות היא המכונה כלל לא קראה את כל הקלט, וזה אינו מקרה נפוץ במיוחד (אם כי הוא בהחלט קיים). אם כן ברור שמדידת זמן הריצה היא תמיד **ביחס לאורך הקלט**.

הגדרה 5.2: סיבוכיות זמן ריצה

תהי M מ"ט דטרמיניסטית אשר עוצרת על כל קלט. **הזמן הריצה** או **הסיבוכיות זמן** של M היא פונקציה $f : \mathbb{N} \to \mathbb{N}$, כאשר $f(n)$ המספר צעדי חישוב המקסימלי ש- M מבצעת על קלט w של אורך n.

אם $f(n)$ זמן הריצה של M, אומרים כי M רץ בזמן $f(n)$ וש- M היא $f(n)$ זמן מכונת טיורינג

אנחנו נייצג את הזמן הריצה **בסימון אסימפטוטי** או **סימון O גדולה.**

למשל, נתונה הפונקציה $f : \mathbb{N} \to \mathbb{N}$ שמוגדרת $f(n) = 6n^3 + 2n^2 + 20n + 45$. בסימון $O(f)$ אנחנו רושמים רק

החזקה הכי גדולה ללא המקדם, כלומר

$$f(n) = 6n^3 + 2n^2 + 20n + 45 \quad \Rightarrow \quad f(n) = O\left(n^3\right) \ .$$

הגדרה 5.3: סימון אסימפטוטי

תהיינה f, g פונקציות

$$f : \mathbb{N} \to \mathbb{R}^+ \ , \qquad g : \mathbb{N} \to \mathbb{R}^+$$

כאשר $\mathbb{R}^+$ הממשיים הלא שליליים.
אומרים כי

$$f(n) = O\left(g(n)\right)$$

אם קיימים שלמים c ו- n_0 עבורם לכל $n \geq n_0$ מתקיים

$$f(n) \leq cg(n) \ .$$

אם $f(n) = O\left(g(n)\right)$ אורמים כי $g(n)$ חסם עליון אסימפטוטי של $f(n)$.

דוגמה 5.2

תהי $f : \mathbb{N} \to \mathbb{R}^+$ פונקציה שמוגדרת

$$f(n) = 6n^3 + 2n^2 + 20n + 45 \ .$$

הוכיחו כי $f(n) = O\left(n^3\right)$.

פתרון:

$f(n) = 6n^3 + 2n^2 + 20n + 45$. לכל $n \in \mathbb{N}$ מתקיים $n^2 \leq n^3$, $n \leq n^3$, ו- $1 \leq n^3$. לכן

$$f(n) = 6n^3 + 2n^2 + 20n + 45 \leq 6n^3 + 2n^3 + 20n^3 + 45n^3 = 73n^3 \ .$$

נגדיר $g(n) = n^3$. מצאנו $n_0 = 1$ ו- $c = 73$ כך שלכל $n \geq n_0$ מתקיים

$$f(n) \leq cg(n) \ .$$

לכן $f(n) = O\left(g(n)\right) = O\left(n^3\right)$.

משפט 5.1:

לכל $a, b, n \in \mathbb{R}$,

$$\log_a n = \frac{\log_b n}{\log_b a} \ .$$

ז"א מעבר מבסיס a לבסיס b משנה את הערך של הלוגריתם עד פקטור של $\dfrac{1}{\log_b a}$. מכיוון ששינוי של המקדם לא משנה את החסם עליון אסימפטוטי, במידה שההתנהגות האסימפטוטית של פונקציה כלשהי היא $\log_a n$ אנחנו פשוט רושמים $O(\log n)$ ללא הבסיס.

דוגמה 5.3

נתונה הפונקציה $f : \ \to \mathbb{R}^+$ שמוגדרת

$$f(n) = 3n \log_2 n + 5n \log_2 \log_2 n + 2 \ .$$

הוכיחו:

$$f(n) = O(n\log n) \ .$$

פתרון:

לכל $n\geq 2$ מתקיים

$$\log_2(n)\leq n \ , \qquad 2\leq n\log_2 n$$

לפיכך

$$\begin{aligned} f(n) =& 3n\log_2(n) + 5n\log_2(\log_2(n)) + 2 \\ \leq& 3n\log_2(n) + 5n\log_2(n) + 2 \\ \leq& 3n\log_2(n) + 5n\log_2(n) + 2n\log_2(n) \\ =& 10n\log_2(n) \end{aligned}$$

נגדיר $g(n)=n\log_2(n)$. מצאנו $n_0=2$ ו- $c=10$ כך שלכל $n\geq n_0$ מתקיים

$$f(n)\leq cg(n) \ .$$

לכן $f(n)=O(g(n))=O(n\log n)$.
לעתים אנחנו רושמים פונקציות כסכום של התנהגויות אסימפטוטיות, לדוגמה הפונקציה

$$f(n) = 6n^2 + 2n$$

ניתנת לרשום בצורה

$$f(n) = O\left(n^2\right) + O(n) \ .$$

כל O בביטוי זה מייצג מקדם כלשהו מודחק. מכיוון שה- $O(n^2)$ שולטת על ה- $O(n)$ ביטוי זה שקול ל- $f(n)=O(n^2)$.

אנחנו ראינו כי הסימון $f(n)=O(g(n))$ אומר שהפונקציה $f(n)$ שווה אסימפטוטי ל- $g(n)$ לכל היותר. הסימון $f(n)=o(g(n))$ אומר שהפונקציה $f(n)$ פחות אסימפטוטי מ- $g(n)$. פורמלי:

הגדרה 5.4:

תהיינה f,g פונקציות

$$f:\mathbb{N}\to\mathbb{R}^+ \ , \qquad g:\mathbb{N}\to\mathbb{R}^+ \ .$$

אומרים כי

$$f(n) = o(g(n))$$

אם

$$\lim_{n\to\infty}\frac{f(n)}{g(n)} = 0 \ .$$

במילים פשוטות, $f(n)=o(g(n))$ אם לכל מספר ממשי $c>0$ קיים מספר ממשי n_0 כך ש- $f(n)<cg(n)$ לכל $n\geq n_0$.

דוגמה 5.4

א) $\sqrt{n}=o(n)$

ב) $n=o(n\log\log n)$

ג) $n\log\log n = o(n\log n)$

ד) $n\log n = o\left(n^2\right)$

ה) $n^2 = o\left(n^3\right)$

דוגמה 5.5

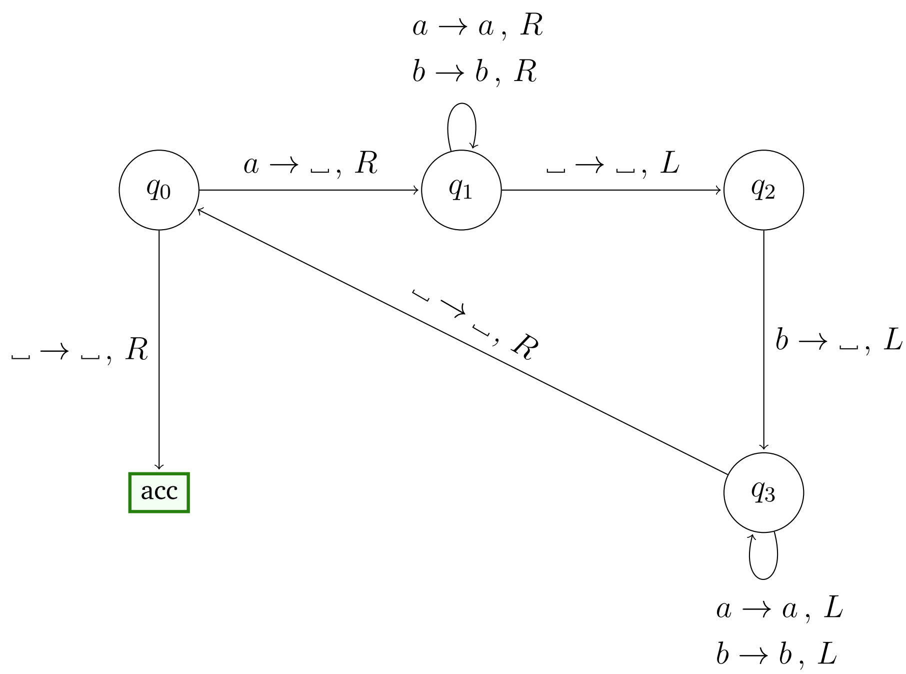
תהי M_1 המ"ט שמכריעה את השפת המילים

$$A = \left\{ \mathrm{a}^n \mathrm{b}^n \;\middle|\; n \geq 0 \right\} .$$

חשבו את הזמן הריצה של M_1.

פתרון:

המכונה שמכריעה את הפשה מתוארת בתרשים למטה. המכונה, באופן איטרטיבי, עוברת על הקלט ובכל מעבר מורידה a מתחילת המילה ומורידה b מסוף המילה ומחליפה אותן ברווח.
אם לאחר מספר מעברים כאלו הסרט ריק, המכונה מרבלת, וזה יתקיים לכל מילה ורק מילים בשפה $\left\{ \mathrm{a}^n \mathrm{b}^n \;\middle|\; n \geq 0 \right\}$.



האלגוריתם של המכונה מפורט להלן:

1) הראש מתחיל בסימן הראשון של הקלט. q_0:

- אם תו הנקרא b, ← rej.
- אם תו הנקרא ␣ ← acc.
- אם תו הנקרא a, כותבים עליה ␣, זז לסוף הקטלט ועוברים לשלב 2).

2)
- אם תו הנקרא a או ␣, ← rej.
- אם תו הנקרא b כותבים עליה ␣, זז לתחילת הקלט ועוברים לשלב 3).

3) חוזרים על שלבי 1) ו- 2) שוב ושוב עד שהמ"ט מגיע למצב acc או rej.

בסבב הראשון, בשלב 1) המספר הצעדים המקסימלי שהמכונה מבצעת הוא $n+1$:
n צעדים כדי לזוז לסוף המילה ועוד צעד נוסף כדי להחזיר את הראש למשבצת האחרונה של הקלט.
בשלב 2) המכונה מבצעת n צעדים:
$n-1$ צעדים כדי לחזור לתו רווח הראשון ועוד צעד אחד כדי לשים את הראש בתו הראשון שאינו תו רווח.

לכן אחרי הסבב הראשון המספר הצעדים המקסימלי הוא $2n+1$.

בסבב השני יש $n-2$ תווים שאינם תוי רווחים.
לכן בסבב השני המכונה תבצע $2n-3$ צעדים לכל היותר.

בסבב השלישי, יהיו $n-4$ סימנים לסרוק והמכונה תבצע $2n-9$ צעדים לכל היותר.

בכללי, בסבב ה- k -ית המכונה מבצעת $2n-4k+5$ צעדים לכל היותר.
בסה"כ יהיו $\frac{n}{2}$ סבבים מקסימלי.

לכן המספר הצעדים המקסימלי הוא

$$\sum_{k=1}^{n/2}(2n+5-4k)=\frac{n^2}{2}+\frac{3n}{2}$$

לפיכך הזמן הריצה של M_1 הוא

$$O\left(n^2\right)+O\left(n\right)=O\left(n^2\right)\ .$$

דוגמה 5.6

תהי M_{L_2} המ"ט שמכריעה את השפת המילים

$$L_2=\{\mathtt{a}^n \mid n=2^k\ ,k\geq 0\}\ .$$

חשבו את הזמן הריצה של M_{L_2}.

פתרון:

1) <u>סבב $k=1$</u>

נתון הקלט למשל

␣	␣	a	a	a	a	a	a	a	a	␣	␣

$\uparrow$

נתחיל בתו הראשון ונעבור על סרט הקלט משמאל לימין ומבצעים מחיקה לסירוגין של האות a, כלומר אות אחת נמחק ואות אחת נשאיר וכן הלאה.

␣	␣	✓	a	✓	a	✓	a	✓	a	␣	␣

$\uparrow$

אחרי סבב הראשון

- אם יש ✓ בתו האחרון ⇐ יש מספר אי-זוגי אותיות a אחרי חילוק ב- 2 ⇐ אין חזקת 2 אותיות a. ← rej.
- אם יש a בתו האחרון ⇐ יש מספר זוגי אותיות a אחרי חילוק ב- 2 ונמשיך לשלב 2).

2) הראש חוזר לתו הראשון של הקלט

␣	␣	✓	a	✓	a	✓	a	✓	a	␣	␣
		↑									

3) חוזרים על שלבים 1) ו- 2), עד שהמכונה תגיע למצב rej או למצב שנשאר רק אות אחת של a, ואז המכונה עוברת למצב acc.

<u>סבב $k = 2$</u>

1')

␣	␣	✓	✓	✓	a	✓	✓	✓	a	␣	␣
									↑		

2')

␣	␣	✓	✓	✓	a	✓	✓	✓	a	␣	␣
		↑									

<u>סבב $k = 3$</u>

1'')

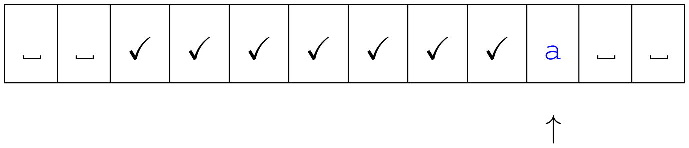
␣	␣	✓	✓	✓	✓	✓	✓	✓	a	␣	␣
									↑		

2'')

␣	␣	✓	✓	✓	✓	✓	✓	✓	a	␣	␣
		↑									

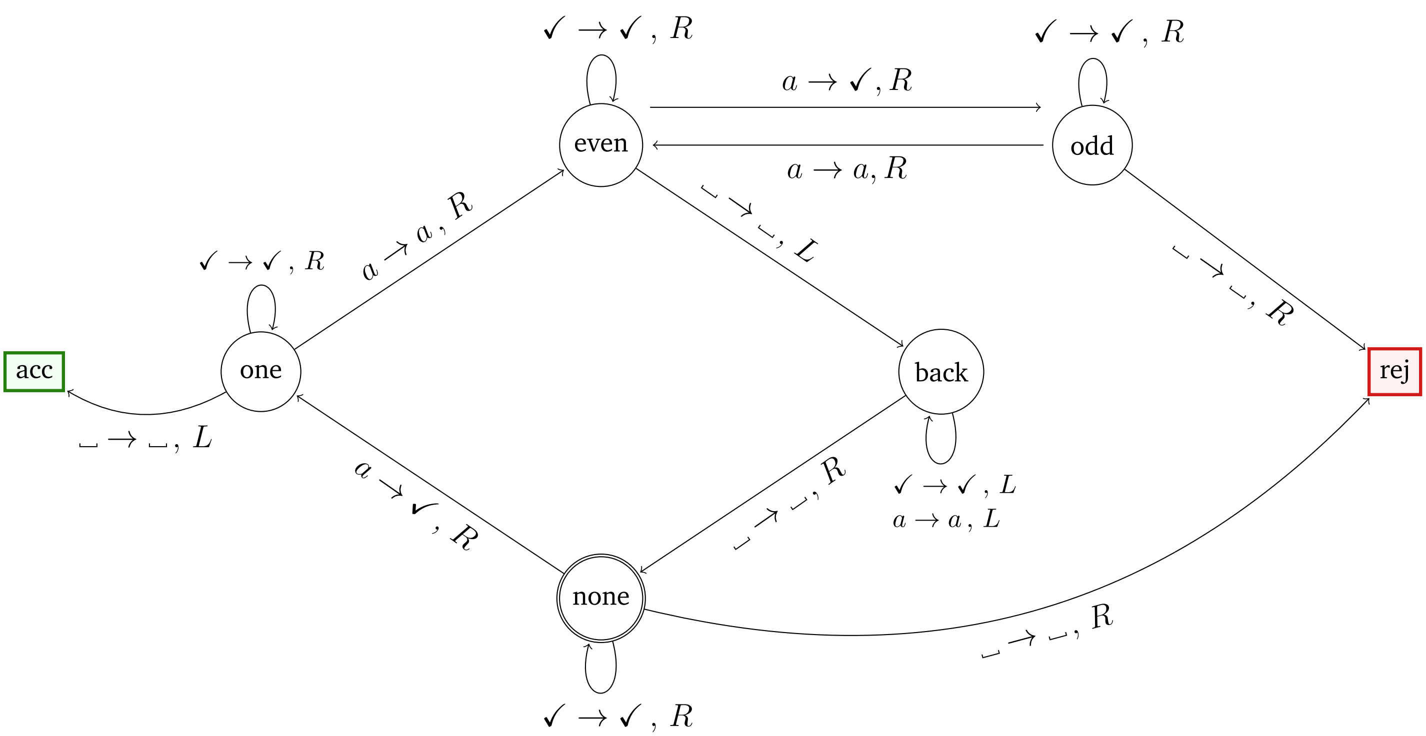
<u>סבב $k = 4$</u>

ב"')



נשאר בדיוק אות a והמכונה ← acc.

המכונת טיורינג אשר מקבלת מילים בשפה זו מתוארת למטה.



בכל סבב, בסריקה מקצה השמאלי לקצה הימני המכונת טיורינג מבצעת $n+1$ צעדים לכל היותר: n צעדים לזוז לסוף הקלט וצעד אחד להחזיר את הראש לתו האחרון של הקלט.
אחרי זה המכונה מבצעת $n+1$ צעדים כדי להחזיר את הראש לתו הראשון של הקלט: n צעדים לתו רווח הראשון וצעד אחד להחזיר את הראש לתחילת הקלט.

המכונה חוזרת על התהליך הזה עד שנשאר אות a אחת בלבד. בכל סבב המכונה מבצעת חילוק ב- 2, לכן ידרשו $\log_2(n)$ סבבים עד שנשאר אות a אחת בלבד.

בשלב האחרון המכונה בודקת האם יש בדיוק אות a אחת, אשר דורש n צעדים בשביל הסריקה מקצה השמאל לקצה הימין, ועוד צעד אחד לתו רווח הראשון אחרי התו האחרון של הקלט.

לפיכך, בסה"כ יהיו לכל היותר

$$2(n+1)\log_2(n)+n+1=2n\log_2(n)+2\log_2 n+n+1$$

צעדים. לכן זמן הריצה הוא

$$O\left(n\log n\right)+O\left(\log n\right)+O\left(n\right)+O\left(1\right)=O\left(n\log n\right)\ .$$

נקודה עדינה שנובעת מהגדרת סיבוכיות זמן ריצה בתור פונקציה של אורך הקלט היא שיש חשיבות **לאופן הייצוג** של הקלט כשאנו מנסים לקבוע אם אלגוריתם הוא יעיל או לא. דוגמה קלאסית היא האלגוריתם הנאיבי לבדיקת ראשוניות:

עבור מספר n ניתן לבדוק אם n ראשוני או לא על ידי מעבר סדרתי על כל המספרים $1 < k < n$ ובדיקה האם k מחלק את n.

- אם כן $\leftarrow$ rej.
- אם לכל k הבדיקה נכשלה $\leftarrow$ acc.

אלגוריתם זה מבצע $O(n)$ פעולות חלוקה ולכן הוא לכאורה יעיל, כי "זמן ריצה לינארי הוא יעיל". אך בפועל זה אלגוריתם לא יעיל מאוד.
הסיבה לכך היא שכדי לייצג את המספר n אנחנו צריכים רק ל- $\log n$ ביטים, והאלגוריתמים שלנו לחיבור, כפל וכו' של מספרים פועלים בסיבוכיות $O\left(\log n\right)$ ו- $O\left(\log^2 n\right)$ וכדומה.
כלומר אם n מיוצגבבסיס בינארי אז האלגוריתם שראינו דורש זמן אקספוננציאלי **בגודל ייצוג** n.
לעומת זאת, אם n מיוצג בבסיס אונרי, כלומר בתור 1^n, אז האלגוריתם לבדיקת ראשוניות אכן יהיה $O(n)$.

הגדרה 5.5: מחלקה של סיבוכיות זמן

המחלקת הסיבוכיות זמן מסומנת $\mathrm{TIME}\left(t(n)\right)$ ומוגדרת להיות אוסף של כל השפות אשר ניתנות להכרעה על ידי מכונת טיורינג בזמן $O\left(t(n)\right)$.

דוגמה 5.7

השפה

$$A = \left\{\mathtt{a}^n\mathtt{b}^n \;\middle|\; n \geq 0\right\}$$

המכונת טיורינג M_1 מכריעה את השפה A בזמן $O(n^2)$ לכן $A \in \mathrm{TIME}\left(n^2\right)$.

דוגמה 5.8

קיימת מכונת טיורינג M_2 שמכריעה את השפה A בצורה יותר יעילה, בזמן ריצה $O\left(n\log n\right)$.

האלגוריתם

(1 סורקים את סרט הקלט משמאל לימין.

- אם נמצא $\mathtt{a}$ לצד ימין של $\mathtt{b}$ $\leftarrow$ rej.
- אחרת עוברים לשלב 2).

(2 סורקים את סרט הקלט משמאל לימין ובודקים אם המספר הכולל של אותיות $\mathtt{a}$ ו- $\mathtt{b}$ זוגי או אי-זוגי.

- אם אי-זוגי $\leftarrow$ rej.
- אחרת עוברים לשלב 3).

(3 סורקים את הקלט שוב משמאל לימין.

- מבצעים מחיקה לסירוגין של האות $\mathtt{a}$, (כלומר מתחילים אם האות $\mathtt{a}$ הראשונה, אות אחת נמחק ואות אחת נשאר וכן הלאה.)
- אחר כך מבצעים מחיקה לסירוגין של האות (מתחילים אם האות $\mathtt{b}$ הראשונה, אות אחת נמחק ואות אחת נשאר וכן הלאה.) $\mathtt{b}$.

4) חוזרים על שלבים 2) ו- 3)

- עד שהמכונה מגיעה למצב rej,
- אחרת אם לא נשאר אף אותיות a או b המכונה עוברת ל- acc.

הסיבוכיות

הזמן הריצה של שלב 1) הוא $O(n)$.

גם שלב 2) הוא $O(n)$ וגם שלב 3) הוא $O(n)$.

בכל סבב, בשלב 3) המכונה מורידה לפחות חצי האותיות a ולפחות חצי האותיות b.
לכן המכונה תבצע $\log_2 n + 1$ סבבים לכל היותר.
לפיכך הזמן הריצה של M_2 יהיה

$$O(n) + 2O(n)\left(1 + O\left(\log_2 n\right)\right) = 2O\left(n \log_2 n\right) + 3O(n) = O(n \log n)\ .$$

לפיכך $A \in \text{TIME}\left(n \log n\right)$.

דוגמה 5.9

קיימת מכונת טיורינג M_3 עם שני סרטים שמכריעה את השפה A בצורה יותר יעילה, בזמן ריצה $O\left(n\right)$.
זמן הריצה זה נקרא **זמן ליניארי**.

האלגוריתם

בהתחלה על סרט 1 כתוב את הקלט.
סרט 2 ריק.

1) סורקים את סרט 1 משמאל לימין.

- אם המילה ריקה ← acc.
- אם נמצא a לצד ימין של b ← rej.
- אם תו הנקרא הראשון b ← rej.
- אחרת עוברים לשלב 2).

2) סורקים את סרטים 1 ו- 2 משמאל לימין והעתיקו את כל האותיות a מסרט 1 לסרט 2 צעד צעד.

- אם התו הראשון אחרי האותיות a הוא ␣ "←" rej
- אם התו הראשון אחרי האותיות a הוא b עוברים לשלב 3).

3) אם נקרא אות b בסרט 1 נמחק אות a בסרט 2.

אחר כך הראש של סרט 1 זז ימינה צעד אחד והראש של סרט 2 זז שמאלה צעד אחד וחוזרים על השלב הזה.

- אם לא נשארות אף אותיות a בסרט 2 אבל עדיין נשארות אותיות b בסרט 1 אז ← rej.
- אם כאשר כל האותיות a על סרט 2 נמחקו ולא נשארות אף אותיות b על סרט 1 אז ← acc.

הסיבוכיות

הזמן הריצה של שלב 1) הוא $O(n)$.

הזמן הריצה של שלב 2) ושלב 3) ביחד הוא $O(n)$.
לפיכך הזמן הריצה של M_3 יהיה

$$O(n)+O(n)=2O\left(n\right)=O(n)\ .$$

לפיכך $A\in \text{TIME}\left(n\right)$.

ראינו דוגמה של עקרון חשוב בסיבוכיות:

משפט 5.2:

הגדרת זמן הריצה שנתנו היא תלויה במודל של מכונת הטיורינג שאיתו אנחנו עובדים.

משפט 5.3:

תהי $t:\mathbb{N}\to\mathbb{R}^+$ פונקציה $t(n)$.
אם מתקיים

$$t(n)\geq n$$

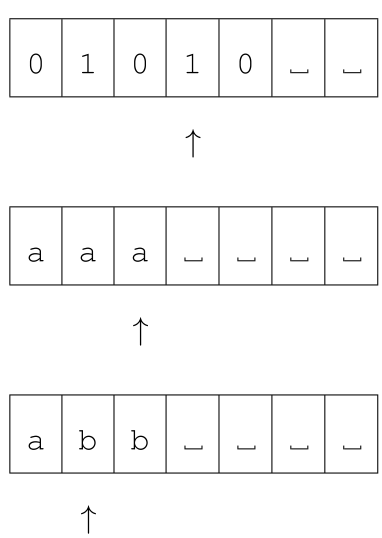
אז לכל מכונת טיורינג $O\left(t(n)\right)$ רב-סרטי קיימת מ"ט $O\left(t^2(n)\right)$ עם סרט אחד.

הוכחה:
תהי M מ"ט k סרטים שרץ בזמן $O\left(t(n)\right)$.

נבנה מ"ט S עם סרט אחד שרץ בזמן $O\left(t^2(n)\right)$.

רושמים את התוכן של ה- k סרטים והמיקום של הראש של כל אחד הסרטים של M על הסרט היחיד של S.
להלן יש דוגמה לכך של מכונת טיורינג עם 3 סרטים:

המכונת טיורינג M



<u>המכונת טיורינג S</u>

#	0	1	0	1 ↑	0	#	a	a	a ↑	#	a	b ↑	b

כדי לסמלץ צעד אחד של M במ"ט S:

1) בהתחלה, S מאתחלת את הסרט שלה על ידי לכתוב את התוכן של כל אחד של ה- k סרטים על הסרט היחיד שלה, עם תו # להפריד בין שני סרטים של M כמתואר בדוגמה למעלה.

2) כדי לסמלץ צעד אחד של M על המכונה S, המכונה S מבצעת סריקה אחת מה- # הראשון בקצה השמאלי ל- # ה- $k+1$ -ית בקצה הימין.

בסריקה זו S זוכרת את הסימנים במיקומים של ה- k ראשים של M באמצעות k תאי זכרון.

3) אחר כך S מבצעת סריקה שנייה של הסרט. בסריקה זו, לפי הפונקצית המעברים S מבצעת

- כתיבה של הסימן החדש בסרט ה-i במיקום של כל ראש של סרט ה-i,
- תזוזה של הראש של סרט ה- i

לכל $1 \leq i \leq k$.

במקרה שכל אחד של הראשים של M זז ימינה לתו רווח בקצה הימין של הסרט שלו, כלומר למשבצת ריקה שטרם לא נקרא, S מוסיפה משבצת עם תו רווח לצד שמאל של ה- # ומזיזה את כל המשבצות מקום אחד ימינה.

האורך של הסרט של S שווה לסכום של הארכים של ה- k סרטים של M.
הזמן הריצה של M הוא $t(n)$.
ז"א M משתמשת ב- $t(n)$ משבצות לכל היותר ב- $t(n)$ צעדים.
לכן בהכרח האורך של הסרט של S הוא $t(n)$ לכל היותר,
לכן סריקה אחת של S דורשת $O(t(n))$ צעדים לכל היותר.

כדי לדמות צעד אחד של M, המכונה S מבצעת שתי סריקות.
כל סריקה לוקחת זמן $O(t(n))$.
לכן S לוקחת זמן $O(t(n))$ כדי לבצע צעד אחד של M.

בשלב האתחול S מבצעת $O(n)$ צעדים.

S מסמלצת כל אחד של ה- $t(n)$ צעדים של M, בזמן $O(t(n))$.

לפיכך הזמן הכולל הנדרש של S לבצע $t(n)$ צעדים של M הוא

$$t(n) \times O(t(n)) = O\left(t^2(n)\right) \ .$$

הסימלוץ הכולו לוקח

$$O(n) + O\left(t^2(n)\right) \ .$$

אנחנו הנחנו כי $t(n) \geq n$ לכן הזמן הריצה של S הוא

$$O\left(t^2(n)\right) \ .$$

■

הגדרה 5.6: זמן הריצה של מ"ט לא דטרמיניסטית

צהי N מכונת טיורינג לא דטרמיניסטית.
הזמן הריצה של N מוגדרת להיות הפונקיצה $f:\mathbb{N}\to\mathbb{N}$ כאשר $f(n)$ הוא המספר הצעדים המקסימלי אשר N מתוך כל הענפים של החישוב שלה על קלט של אורך n.

משפט 5.4:

תהי $t(n)$ פונקציה המקיימת $t(n)\geq n$. כל מ"ט $O\left(t(n)\right)$ לא דטרמיניסטית N סרט אחד, שקולה למכונת טיורינג $2^{O(t(n))}$ דטרמיניסטית סרט אחד.

הוכחה:

■

5.2 המחלקה P

הגדרה 5.7: מכונת טיורינג פולינומית

מכונת טיורינג M תיקרא **פולינומית** או **יעילה** אם קיים $c\in\mathbb{N}$ כך ש- M פועלת בסיבוכיות זמן ריצה $O\left(n^c\right)$.

הגדרה 5.8: המחלקה P

המחלקה P היא אוסף השפות שקיימת מכונת טיורינג פולינומית M המקבלת אותן. כלומר:

$$P=\bigcup_k \text{TIME}\left(n^k\right)\ .$$

הגדרה 5.9: המחלקה $POLY$

המחלקה $POLY$ היא אוסף הפונקציות שקיימת מכונת טיורינג פולינומית M המקבלת אותן.

דוגמה 5.10 גרף מכוון

נתון גרף G עם קדקודים s ו- t.
נגדיר בעיה $PATH$ להיות הבעיה לקבוע האם קיים מסלול בין s לבין t.

$$PATH=\left\{\langle G,s,t\rangle\,\middle|\,\text{גרף מכוון המכיל מסלול מכוון מ- } s \text{ ל- } t\ G\right\}$$

הוכיחו כי

$$PATH\in P\ .$$

פתרון:

נבנה אלגוריתם M פולינומי בשביל בעיה $PATH$ כמפורט להלן.

עבור הקלט $\langle G,s,t\rangle$ כאשר G הגרף המכוון עם קדקודים s ו- t:

1) נסמן את הקדקוד s.

2) חוזרים על שלב 3) עד שלא נשארים קדקודים לא מסומנים בקצוות של אף צלע של G:

3) סורקים את כל הצלעות של G.

- אם נמצע צלע (a,b) מקדקוד מסומן לקדקוד לא מסומן, נסמן את הקדקוד b.

4) אם קדקוד t מסומן, $\leftarrow$ acc.
אחרת $\leftarrow$ rej.

שלב 1) מבוצע פעם אחת בלבד, ושלב 4) מבוצע פעם אחת בלבד.

אם ל- G יש n קדקודים אז שלב 3) מבוצע n פעמים לכל היותר.

לכן מספר הצעדים המבוצעים הוא $n+1+1$ לכל היותר.

לכן $M=O(n)$.

דוגמה 5.11

תהי $RELPRIME$ הבעיה לבדור אם שני שלמים x,y זרים.

$$RELPRIME=\Big\{\{x,y\}\in\mathbb{N}\;\Big|\;\gcd(x,y)=1\Big\}$$

הוכיחו כי $RELPRIME\in P$.

פתרון:

נבנה אלגוריתם שמתבסס על האלגוריתם אוקלידס למצוא את ה- gcd. נסמן את האלגוריתם שמבצע האלגוריתם אוקלידס ב- E.
הקלט הוא הצמד שלמים $\{x,y\}$ בבסיס בינארי:

1) משימים $x\leftarrow x \mod y$

2) מחליפים x ו- y.

3) מחזירים x.

4) חוזרים על השלבים 1) - 3) עד שנקבל $y=0$.

```
x = 625;
y = 75;

a=x;
b=y;

while y!=0:
    x = x % y

    y1 = x
    x = y
    y = y1

print("gcd(%d,%d) = %d" % (a,b,x))
```

האלגוריתם R פותר את הבעיה $RELPRIME$ על ידי שימוש של E כתת-אלגוריתם:
הקלט של R הוא הצמד שלמים $\{x,y\}$ בבסיס בינארי:

1) מריצים E על $\{x,y\}$.

2) אם הערך חזרה של E הוא 1 אז $\text{acc} \leftarrow$
אחרת $\text{rej} \leftarrow$.

אם E רץ בזמן פולינומי אז גם R ירוץ בזמן פולינומי אז מספיק לבדוק את הסיבוכיות זמן הריצה של E בלבד.

ללא הגבלת כלליות נניח ש- $x > y$. (המקרה של $x = y$ לא מעניין אותנו כי התשובה $\gcd(x,x) = x$ טריוויאלית).
משפט החילוק של אוקלידס אומר שלכל x, y שלמים קיימים שלמים q, r עבורם

$$x = qy + r \ ,$$

כאשר $y < x$ ו- $r < y$. השלם $q = \left\lfloor \frac{x}{y} \right\rfloor$ נקרא המנה ו- $r = x \mod y$ נקרא השארית.

אחרי ביצוע של שלב 1), שבו אנחנו משימים $x = x \mod y$, אז יהיה $x < y$.

אחרי ביצוע של שלב 2), שבו מחליפים x ו- y, אז יהיה $x > y$.

כעת יש שתי אפשרויות:

- אם אחרי שלב 2) יוצא כי $y \geq \frac{x}{2}$ אז $x \mod y < y \leq \frac{x}{2}$.

  לכן $x \mod y \leq \frac{x}{2}$.

  מכאן אנחנו רואים כי x יקטן לפחות בחצי.

- מצד שני נניח שאחרי שלב 2) יוצא כי $y < \frac{x}{2}$.

  אז $x \mod y < y \geq \frac{x}{2}$.

  לכן $x \mod y \leq \frac{x}{2}$.

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

  לפיכך
  $$x \mod y = x - y < \frac{x}{2} \ .$$
  לכן גם במקרה זה x יקטן לפחות בחצי.

x ו- y מתחלפים כל פעם ששלב 2) מתבצע, לכן אחרי 2 סבבים של האלגוריתם, הערך של x יקטן לפחות בחצי וגם הערך של y יקטן בחצי.

לפי זה מספר הפעמים המקסימלי ששלבים 1) ו- 2) מתבצעים הוא המינימום בין מספר פעמים שאפשר לחלק x ב- 2 לבין מספר פעמים שאפשר לחלק y בחצי. ז"א המימימום בין $2\log_2 x$ לבין $2\log_2 y$. כלומר, מספר הסבבים המקסימלי של האלגוריתם הוא

$$\min\left(2\log_2 x, 2\log_2 y\right) \ .$$

מכיוון ש- x ו- y נתונים בבסיב בינארי אז

$$\log_2 x = n_x - 1 \ , \qquad \log_2 y = n_y - 1$$

כאשר n_x אורך המספר x בבסיס בינארי ו- n_y אורך המספר y.

לכן מספר הצעדים המקסימלי של האלגוריתם E הוא

$$\min(n_x - 1, n_y - 1) \ .$$

זמן הריצה מוגדר להיות המספר הצעדים המקסימלי של האלגוריתם, לכן

$$E = O(n)$$

כאשר n אורך הקלט.

5.3 המושג של אלגוריתם אימות

הגדרה 5.10: מעגל המילטוני

כלומר מעגל המילטוני (Hamiltonian cycle) בגרף מכוון $G = (V, E)$ הוא מעגל אשר עובר כל קדקוד בדיוק פעם אחת.

גרף המכיל מעגל המילטוני מכונה **גרף המילטוני** (Hamiltonian). אחרת, הגרף מכונה **לא המילטוני** (non-Hamiltonian).

הגדרה 5.11: הבעיית מעגל המילטוני

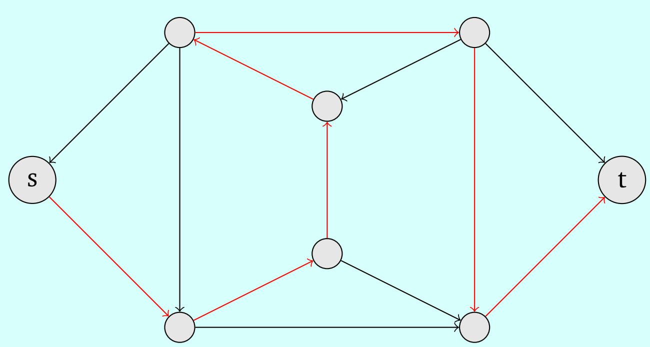
הבעיית המעגל ההמילטוני the hamiltonian cycle problem היא הבעיה:

" האם לגרף G יש מעגל המילטוני?"

ניתן להגדיר כשפה פורמלית:

$$HAMPATH = \left\{ \langle G, s, t \rangle \ \middle| \ \text{G הוא גרף מכוון המכיל מעגל המילטוני מ- s ל- t.} \right\}$$

התרשים למטה מראה דוגמה של מעגל המילטוני בגרף מכוון.



נשאל שאלה: מהו הסיבוכיות זמן הריצה של הבעיה $HAMPATH$? כעת זה לא ידוע האם הבעיה הזו ניתנת לפתור בזמן פולינומי, כלומר האם $HAMPATH \in P$.

בכל זאת, נניח שחבר מספר לך כי גרף נתון G הוא המילטוני. אפשר לאמת את הטענה ע"י כך שנמנה את הקדקודים על פי סדרם לאורך המעגל ההמילטוני, ונבדוק אם קדקודיו הם תמורה של קדקודי V של G, ואם כל אחת מן הקשתות העוקבות לאורך המעגל אכן קיימת בגרף. בהמשך אנחנו נוכיח כי האלגוריתם האימות הזה ניתן לממש כך שירוץ בזמן $O\left(n^2\right)$, כאשר n הוא אורך הקידוד של G. ז"א הוכחה שגרף מכיל מעגל המילטוני ניתנת לאימות בזמן פולינומיאלי.

אף על פי שלא בהכרח יש לנו אלגוריתם שרץ בזמן פולינומיאלי שבדוק האם גרף מכיל מעגל המילטוני, בכל זאת במקרה שמעגל המילטוני היה נגלה, קל למדי לאמת את המעגל על ידי האלגוריתם לעיל.

הדוגמה הזאת היא מקרה שבה הביעה של לאמת פתרון לבעיה נתונה קלה יותר מהבעיה של למצוא פתרון לבעיה זו.

הגדרה 5.12: מספר פריק

משפר שלם x נקרא **פריק** (composite) אם קיימים שלמים $p>1, q>1$ כך ש-

$$x=pq\ .$$

במילים אחרות, x פריק אם ורק אם x לא ראשוני.

הגדרה 5.13: הבעיית $COMPOSITES$

הבעיית $COMPOSITES$ היא הבעיה:

" האם השלם x פריק? "

ניתן להגדיר כשפה פורמלית:

$$COMPOSITES=\left\{x\ \middle|\ x=pq \text{ כך ש- } p,q>1 \text{ קיימים שלמים } \right\}$$

קל למדי לאמת כי שלם x פריק: בהינתן הפתרון ש- $p\mid x$, אלגוריתם אימות הוא אלגוריתם אשר מחלק x ב- p ובודק שאין שארית והמנה המתקבל הוא שלם וגדול מ- 1. כעת ניתן הגדרה פורמלית של אלגוריתם אימות

הגדרה 5.14: אלגוריתם אימות

אלגוריתם אימות של שפה A הוא אלגוריתם V כך ש-:

$$A=\left\{w\ \middle|\ c \text{ על פי } \langle w,c\rangle \text{ מקבל } V\right\}$$

במילים, **אלגוריתם אימות** הוא אלרגוריתם V אשר מאמת כי הקלט w שייך לשפה A על פי התנאי c, שנקרא **אישור** (certification).

אנחנו מגדירים את זמן הריצה של V על פי האורך של w. לכן **אלגוריתם אימות זמן-פולינומיאלי** רץ בזמן פולינומיאלי $O\left(n^k\right)$ כאשר n האורך של w.

5.4 המחלקה NP

הגדרה 5.15: מחלקת הסיבוכיות NP

היא מחלקת השפות שניתן לאמתן באמצעות אלגוריתם זמן-פולינומיאלי.

מן הדיון שלעיל, בבעיית המעגל ההמילטוני עולה כי $HAMPATH \in NP$.
יתר על כן,

משפט 5.5:

אם $L \in P$ אז $L \in NP$

רעיון ההוכחה: אם קיים אלגוריתם זמן-פולינומיאלי המכריע את L, ניתן להפוך אותו בקלות לאלגוריתם אימות בעל שני קלטים שפשוט מתעלם מכל אישור ומקבל בדיוק אותן מחרוזות שלגביהן הוא קובע כי הן שייכות ל- L.
לכן

$$P \subseteq NP \ .$$

דוגמה 5.12

הוכיחו כי

$$HAMPATH \in NP \ .$$

פתרון:

כזכור הזמן הריצה של מ"א לא דטרמיניסטית מוגדר לפי הזמן הריצה של הענף הכי הארוך (הגדרה 5.6 שלעיל).
נבנה מ"ט אי-דטרמיניסטית N_1 אשר מכריעה את $HAMPATH$ -בזמן-פולינומיאלי אי דטרמיניסטי.

יהיו m מספר הקדקודים של G ו- n מספר הקשתות של G:

$$m = |V| \ , \qquad n = |E| \ .$$

$N_1 =$ על הקלט $\langle G,s,t\rangle$ כאשר G גרף מכוון ו- s,t קדקודים של G:

(1 רושמים רשימה של m מספרים, $p_1,p_2,\ldots,p_m$ כאשר m מספר הקדקודים ב- G.
כל מספר נבחר בצורה אי-דטרמיניסטית מ- 1 עד m.

(2 בודקים אם יש חזרות ברשימה זו.
אם יש חזרות $\leftarrow$ rej.

(3 בודקים אם $s=p_1$ ו- $t=p_m$.
אם לא $\leftarrow$ rej.

(4 לכל $1 \leq i \leq m-1$ בודקים אם הקשת (p_i,p_{i+1}) שייך לקבוצת הקשתות E של G.

- אם אף קשת לא שייכת ל- E $\leftarrow$ rej.
- אם כל הקשתות שייכות ל- E $\leftarrow$ acc.

כעת נבדוק עת הסיבוכיות של האלגוריתם הזה.

שלב 1) דורש m צעדים ולכן מתבצע בזמן פולינומיאלי.

שלב 2) דורש m צעדים לכל היותר, ולכן מתבצע בזמן פולינומיאלי.

שלב 3) דורש m צעדים לכל היותר, ולכן מתבצע בזמן פולינומיאלי.

עבור שלב 4) לכל קשת (p_i, p_{i+1}), N_1 בודקת אם יש קשת תואמת בקבוצת הקשתות E של G.
לכן ידרשו n צעדים לכל היותר לכל i.
לכן שלב 4) דורש $n(m-1)$ צעדים לכל היותר בסה"כ.
לכן הסיבוכיות זמן הריצה של N_1 היא

$$O(m) + O(m) + O\left(n(m-1)\right) = O\left(n(m-1)\right)$$