<u>תזכורת:</u>
f ניתנת לחישוב אם קיימת מ"ט M כך ש $f_M = f$
איך מראים שפונקציה לא ניתנת לחישוב? קשר לשפות.

$$L_f = \{(x,y) \mid y = f(x)\}$$
f ניתנת לחישוב אם ורק אם $L_f \in RE$

שיטה שניה להוכחה שפונקציה לא ניתנת לחישוב: הוכחה ישירה.
<u>דוגמה:</u>
אם M עוצרת על x אז $f_1(\langle M\rangle, x) = 1$
ואחרת $f_1(\langle M\rangle, x) = 0$

אם M עוצרת על x אז $f_2(\langle M\rangle, x) = 1$
ואחרת f_2 לא מוגדרת

אם M עוצרת על x אז f_3 לא מוגדרת
ואחרת $f_3(\langle M\rangle, x) = 0$

f_1 לא ניתנת לחישוב - (אחרת $HP \in R$).
f_2 ניתנת לחישוב - נריץ את M על x ואם היא תעצור נחזיר 1.
f_3 לא ניתנת לחישוב (אחרת $\overline{HP} \in RE$)

<u>דוגמה:</u>
סיבוכיות קולמגורוב
מה זה סדרה אקראית? ההפך מסדרה שיש בה חוקיות?
נקבע: $\Sigma = \{0,1\}$
$\Gamma = \{0,1,b\}$
סיבוכיות קולמגורוב של מחרוזת $x \in \Sigma^*$ הוא המספר m הקטן ביותר כך שקיימת מ"ט בעלת m מצבים של הקלט הריק (ε) פולטת את x. נסמן אותו ב $k(x)$.
<u>משפט:</u> k היא פונקציה שלא ניתנת לחישוב.
<u>אבחנה 1:</u> $k(x) \le |x| + 1$ (בפרט k היא פונקציה מלאה).
הסבר: אם $x = x_1 x_2 \ldots x_n$
נתאר מ"ט מתאימה בעלת המצבים: $q_1, q_2, \ldots, q_{n+1}$
q_1 מצב התחלתי, q_{n+1} מצב סופי
$f(q_i, b) = (q_{i+1}, x_i, R)$

<u>אבחנה 2:</u> k לא חסומה: לכל l טבעי קיימת מחרוזת x כך ש $h(x) > l$
הוכחה: יש מספר סופי של מ"ט בעלות l מצבים. לא יותר מ $(3\cdot 3\cdot l)^{3l}$.
לכל מ"ט יש פלט יחיד על הקלט ε. נבחר $(3\cdot 3\cdot l)^{3l} + 1$ מחרוזות x שונות ונקבל שעבור אחת מהן $k(x) > l$.

<u>הוכחת המשפט:</u>

נניח בשלילה שקיימת מ"ט M_k המחשבת את הפונקציה k.

k מלאה ולכן M_k עוצרת תמיד.

נתאר M_1: הקלט הוא מספר טבעי l.

הפלט הוא x - המחרוזת הראשונה כך ש $k(x) \geq l$. (על פי האבחנה השניה, קיימת מחרוזת x כזו).

M_1 על קלט l: עבור על המחרוזות x ע"פ הסדר הלקסיקוגרפי. לכל x חשב את $k(x)$ באמצעות M_k המובטחת. אם $k(x) > l$ עצור עם פלט x ואחרת עבור ל x הבא.

נסמן ב t את מספר המצבים של M_1.

נבחר n "גדול מספיק": $2^n - n \geq t+3$

נתאר מכונה חדשה: M_2 על קלט ε

1. כותבת על הסרט את המספר 2^n נראה משהו כמו ...10000 עם n אפסים.
2. מחזירה את הראש שמאלה לתחילת הסרט.
3. מריצה את M_1 ומקבלת כפלט את x הפלט של M_1.

מתקיים: $k(x) > 2^n$ ע"פ נכונות M_1 והבניה.

מספר המצבים של $k(x) \leq M_2$

לביצוע משימה 1 נצטרך לכל היותר $|n|+2$ מצבים

לביצוע משימה 2 נצטרך לכל היותר מצב אחד

לביצוע משימה 3 נצטרך לכל היותר t מצבים.

לכן קיבלנו: $2^n < k(x) \leq n+3+t \leq 2^n$ וזו כמובן סתירה.

<u>בעיות חיפוש:</u>

$\Sigma = \{0,1\}$

יחס דו מקומי $S \subseteq \Sigma^* \times \Sigma^*$

<u>הגדרה:</u> בעיית החיפוש של יחס דו מקומי S, ניתנת לפתרון אם קיימת מ"ט M_s:

על קלט x מוציאה כפלט y (כלשהו) כך ש $(x,y) \in S$.

אם אין y כזה אז M_S לא עוצרת על x.

דוגמה: לכל פונקציה f, נגדיר יחס $S_f = \{(x, f(x)) \mid x \in \Sigma^*\}$

בעיית החיפוש של S_f שקולה לבעיית החישוב של f.

$L_S = \{(x,y) \mid (x,y) \in S\}$

בעיית הזיהוי של S: $L_S \in RE$

האם זיהוי שקול לחיפוש?

משפט: לכל יחס דו מקומי S, אם $L_S \in RE$ אז בעיית החיפוש של S ניתנת לפתרון.

(ההוכחה כמעט זהה למשפט אנלוגי עבור פונקציות)

האם חיפוש גורר זיהוי? לא!

דוגמה: $L_{eq}=\{\langle M_1\rangle,\langle M_2\rangle \mid L(M_1)=L(M_2)\}$

בעיית הזיהוי כאן היא קשה כי השפה הזאת לא שייכת ל RE.

מצד שני בעיית החיפוש היא קלה - נתון לנו קלט מכונה $\langle M_1\rangle$ וצריך למצוא מכונה השקולה לה - נבחר ב $\langle M_1\rangle$ או במכונה אחרת הדומה לה כפלט.

<u>מבוא לחלק ב' של הקורס</u>

נדבר על יעילות מבחינת זמן, וקצת על יעילות מבחינת זיכרון.

איך מודדים זמן?

לא מודדים זמן אמיתי אלא צעדי חישוב.

הגדרה: סיבוכיות החישוב של מ"ט M היא פונקציה (חלקית) $t_M:\Sigma^*\to\mathbb{N}$

אם M עוצרת על x אז $t_M(x)=x$ מספר צעדי החישוב של M על x

ואחרת לא מוגדר $t_M(x)$.

$t(M)$ ניתנת לחישוב.

מספיקים לנו חסמים על הסיבוכיות:

- אסימפטוטיקה
- ניתוח של המקרה הרע

$T:\mathbb{N}\to\mathbb{N}$ נקראת חסם סיבוכיות עבור מ"ט M אם לכל $x\in\Sigma^*$ מתקיים: $t_M(x)\le T(|x|)$.

איזה חסם סיבוכיות ייחשב יעיל?

$$\underbrace{O(\log n),O(\sqrt{n})}_{*},O(n),O(n^2),O(n^3),\underbrace{O(2^n),O(2^{2^n})}_{**}$$

* - למעט בעיות טריוויאליות, נחוץ תמיד $T(n)\ge n$.

** - מקבלות ערכים גבוהים מאוד כבר ל n מאוד קטן.

קריטריונים להגדרה מוצלחת ליעילות:

- התאמה למציאות
- נוחות מתמטית

<u>הגדרה:</u> למכונת טיורינג M יש סיבוכיות פולינומית אם קיים פולינום $p(n)=o(n^c)$ עבור c קבוע כלשהו המהווה חסם סיבוכיות עבורה.

מ"ט כזו תיקרא יעילה.

<u>יתרונות:</u>

1. כמעט כל האלגוריתמים שאנשים משתמשים בהם במציאות עומדים בהגדרה:
- מיון
- אלגברה לינארית
- אלגוריתמים בסיסיים בגרפים - חיפוש, זרימה...

2. עמידות - הגדרה לא רגישה לבחירת המודל - כל בעיה הניתנת לפתרון פולינומיאלי במודל מ"ט / מ"ט רב סרטית / מכונת RAM, ניתנת לפתרון פולינימיאלי גם בשאר המודלים הנ"ל.

(מ"ט 2 סרטים - n^c $\Leftarrow$ מ"ט עם סרט אחד n^{2c})

(מכונת RAM n^c $\Leftarrow$ מ"ט עם סרט אחד n^{2c})
תזה מורחבת של צ'רצ' (תזת $edmonds$):
אוסף הפונקציות הניתנות לחישוב יעיל בכל מודל סביר וכללי הוא זהה.

3. "תכונות סגור"
<u>הרכבה:</u> אם f,g הן פונקציות הניתנות לחישוב יעל אז $h(x) \triangleq g(f(x))$ ניתנת גם כן לחישוב יעיל.
<u>הוכחה:</u> f ניתנת לחישוב יעיל ולכן קיימת מ"ט M_f המחשבת את f תוך $O(n^c)$ צעדים
g ניתנת לחישוב יעיל ולכן קיימת מ"ט M_g המחשבת את f תוך $O(n^d)$ צעדים
צ"ל: קיימת M_h המחשבת את h בסיבוכיות פולינומיאלית.
1. M_h תריץ את M_f על x ותקבל פלט y. $O(n^c)$. הגודל של y הוא גם $O(n^c)$
2. ותריץ על y את M_g. הקלט הוא בגודל $O(n^c)$ ולכן הסיבוכיות היא $O\left(\left(n^c\right)^d\right)=O\left(n^{cd}\right)$
בכל מקרה, קיבלנו שהסיבוכיות הכללית היא פולינומיאלית.

<u>חסרונות ההגדרה:</u>
1. לפעמים סיבוכיות אסימפוטטית גבוהה היא בכל זאת עדיפה:
על פי ההגדרה n^{1000} נחשב יעיל ו $n^{\log n}$ לא יעיל, אף על פי שלרוב זה יהיה להפך.

2. יש אלגוריתמים שימושיים שאינם עומדים בהגדרה.
למשל אלגוריתם $SIMPLEX$ - פתרון בעיות אופטימיזציה לינאריות.