<u>תזכורת:</u> חישוב יעיל שקול לחישוב ע"י מכונה פולינומית, זאת אומרת, קיים פולינום $p(n)=\theta(n^c)$ כך שלכל x, זמן הריצה של M על x חסום ע"י $p(|x|)$ צעדים.

<u>הגדרות:</u>

1. $P=\{$קיימת M כך ש $L(M)=L$ ו M פולינומית$\}$
2. $Poly=\{f:\Sigma^*\to R \mid f_M=f$ קיימת מ"ט M פולי' כך ש$\}$

הערות:

1. $P\subseteq R$.
2. אם $f\in Poly$ אז f מלאה.

* $|f(x)\le p(|x|)|$ - אורך הפלט קטן מהחסם על זמן חישוב הפלט (כי בכל צעד המכונה יכולה לכתוב לכל היותר אות אחת לפלט)

<u>הגדרה:</u> פונקציה המקיימת את * נקראת פונקציה חסומה פולינומית.

<u>תזכורת:</u> אם f מלאה אז $L_f=\{(x,y)\mid y=f(x)\}$.

<u>משפט:</u> f ניתנת לחישוב $\Leftrightarrow L_f\in R$.

(אותה ההוכחה בכיוון $\Leftarrow$ מוכיחה גם שאם f ניתנת לחישוב <u>יעיל</u> אז $L_f\in P$)

הכיוון $\Rightarrow$ לא מתאים להוכחת יעילות (כי הטענה "$L_f\in P\Leftarrow f$ ניתנת לחישוב יעיל" לא נכונה).

<u>למשל:</u> $f(x)=1^{(2^{|x|})}$.

בהינתן $(x,1^{(2^{|x|})})$ זהו קלט שאורכו הוא $n=|x|+2^{|x|}$ ולכן קל לזהות ב $O(n)$ האם הזוג הזה שייך ל L_f ולכן $L_f\in P$.

אבל f לא ניתנת לחישוב יעיל כי גודל הפלט הוא אקספוננציאלי ביחס לגודל הקלט.

נגביל את עצמנו לדיון על f חסומה פולינומית.

טיעון לא פורמאלי לאי נכונות המשפט: $E(m)$ היא פונקצית הצפנה, שכמובן ניתנת לחישוב יעיל.

$f=E^{-1}$ כמובן לא ניתנת לחישוב יעיל (אחרת ההצפנה לא שווה הרבה).

L_f ניתנת לחישוב יעיל - היא מקבלת כקלט (m,n) ובודקת ע"י הצפנה של m האם $n=E(m)$.

נגדיר: $L_f' = \{(x,y) \mid f(x)$ רישא של $y\}$

<u>משפט:</u> $f \in Poly \Leftrightarrow f$ חסומה פולינומית (1) וגם $L_f' \in P$ (2).

<u>הוכחה:</u> $\Leftarrow$

$f \in Poly \Leftarrow f$ חסומה פולינומית. (1)

$f \in Poly \Leftarrow$ קיימת M_f המחשבת את f ועוצרת תוך $p(n)$ צעדים לכל קלט באורך n.

נבנה מ"ט פולי' M עבור השפה L_f': (2)

M על קלט (x,y):

1. תחשב את $f(x)$ באמצעות המכונה M_f המובטחת.
2. תבדוק האם y היא רישא של $f(x)$.

הנכונות מיידית.

סיבוכיות: $O(|x|^c + |y|) = O((|x|+|y|)^c)$. הסבר:

1. $p(|x|) = O(n^c)$ צעדים.
2. לכל היותר $|y|$ צעדים.

כיוון $\Rightarrow$: f חסומה פולי' ולכן קיים פולי p כך ש $|f(x)| \le p(|x|)$ לכל x.

$L_f' \in P$: קיימת M, מ"ט פולי' הרצה זמן $q(n)$ ומכריעה את L_f'.

נתאר מ"ט M_f שעל קלט x מחשבת <u>ביעילות</u> את $f(x)$.

M_f על קלט x:

אתחול: $y = \varepsilon$

איטרציה i: בודקים באמצעות M המובטחת לכל $a \in \Sigma$ האם $(x, ya) \in L_f'$.

אם כן, נחליף את y ב ya ונתחיל באיטרציה חדשה.

אם לא: נעבור לאות הבאה ב Σ.

אם עברנו על כל האותיות, נחזיר את y.

<u>נכונות:</u> נסמן: $f(x) = y_1 y_2 ... y_t$. $t \le p(|x|)$.

אם בתחילת איטרציה i מתקיים $y = y_1 ... y_{i-1}$ אז בסוף האיטרציה יתקיים $y = y_1 ... y_{i-1} y_i$ (מהבניה).

באתחול ε רישא של $f(x)$ תמיד ולכן בסוף האיטרציה ה t יתקיים: $y = y_1 y_2 ... y_t = f(x)$ ואז נעצור עם פלט y כי לא נצליח להוסיף אותיות כי M תדחה את כל המילים מהצורה $f(x)a$.

סיבוכיות: $(t+1)$ איטרציות $\cdot q(|x|+|y|) \cdot |\Sigma|$

$|y| \le t \le p(|x|)$ $(t+1) = O(p(|x|))$

לכן סה"כ:

$= O(p(|x|) \cdot q(|x| + p(|x|))) = r(|x|)$ פולינום.

<u>הקשר בין שפות לבעיות חיפוש:</u> $S \subseteq \Sigma^* \times \Sigma^*$

בעיית חיפוש - נתון x ורוצים למצוא y כך ש $(x,y) \in S$.

בעיית זיהוי - נתון (x,y) ורוצים לדעת האם $(x,y) \in S$.

<u>זיהוי יעיל:</u> האם $S \in P$? אם כן אז הזיהוי של S יעיל (מפעילים את הפונקציה על x ורואים האם התוצאה היא y) ואחרת לא.

<u>חיפוש יעיל:</u>

<u>הגדרה:</u> בעיית החיפוש של יחס S ניתנת לפתרון יעיל אם קיימת מ"ט פולי M כך שלכל x:

אם קיים y כך ש $(x,y) \in S$ אז M עוצרת ב q_A עם פלט y.

אם לא קיים y כנ"ל, אז M עוצרת ב q_R (ומתעלמים מהפלט).

האם חיפוש יעיל $\Leftarrow$ זיהוי יעיל?

<u>לא!</u> דוגמה נגדית: $L_{EQ} = \{\langle M_1 \rangle, \langle M_2 \rangle \mid L(M_1) = L(M_2)\}$

החיפוש יעיל מאוד - בהינתן $\langle M_1 \rangle$ מחזירים את $\langle M_1 \rangle$ בזמן ליניארי.

אבל $L_{EQ} \notin RE$ ולכן בוודאי ש $L_{EQ} \notin P$ ולכן בעיית הזיהוי היא בעיה קשה.

האם זיהוי יעיל $\Leftarrow$ חיפוש יעיל?

לכל יחס S - האם זיהוי יעיל של S גורר חיפוש יעיל של S?

<u>הגדרה:</u> יחס S יקרא חסום פולינומית אם קיים פולינום p כך שלכל $(x,y) \in S$ מתקיים $|y| \le p(|x|)$.

האם לכל יחס חסום פולינומית S, מתקיים שזיהוי יעיל $\Leftarrow$ חיפוש יעיל?

<u>זוהי השאלה פתוחה המרכזית במדעי המחשב (נוסח 1)</u>

<u>מקרים פרטיים חשובים:</u>

<u>לוגיקה:</u> נתון פסוק - האם הוא ספיק? בהינתן השמה, קל למצוא האם היא מספקת אותו, אבל קשה למצוא השמה המספקת אותו.

<u>גרפים:</u> נתון גרף G - האם קיים בו מסלול המילטון? (מסלול שעובר בכל קודקוד פעם אחת בדיוק) קשה לדעת, אבל אם נתון מסלול - קל לבדוק האם הוא מסלול המילטון.

<u>מ"ט אי-דטרמיניסטית (א"ד): (רק בהקשר של שפות)</u>

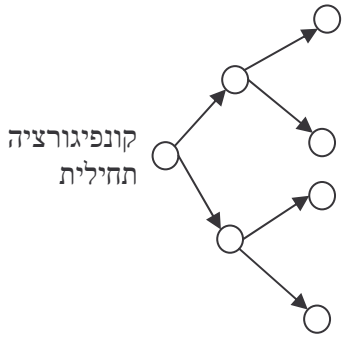
<u>הגדרה:</u> מ"ט א"ד היא שביעיה כמו מ"ט רגילה למעט פונקצית המעברים:

$$\delta:(Q\setminus F)\times\Gamma\to\left(Q\times\Gamma\times\{S,L,R\}\right)^2$$

לדוגמה: $\delta(q,a)=\left((p_0,b_0,d_0),(p_1,b_1,d_1)\right)$

<u>הערה:</u> מ"ט רגילה (דטרמיניסטית) היא מקרה פרטי בו לכל זוג (q,a), שתי האפשרויות למעבר הן זהות. לכל קונפיגורציה יש שתי קונפיגורציות עוקבות.

במקום לדבר על מסלול חישוב יש לנו עץ חישוב (עץ בינארי):



יכול להיות שחלק מהמסלולים יהיו אינסופיים.

מ"ט א"ד מקבלת את הקלט x אם <u>קיים</u> מסלול בעץ החישוב המסתיים ב q_A.

$L(M)\triangleq\{x\mid x$ מקבלת את $M\}$

<u>הערות:</u> מודלים שקולים: מ"ט א"ד עם k סרטים.

מ"ט א"ד שבה: $\delta:(Q\setminus F)\times\Gamma\to 2^{(Q\times\Gamma\times\{S,L,R\})}$

(כמו אוטומט אי דטרמיניסטי מהקורס אש"ף).

<u>דוגמה:</u> $comp=\{x\mid x$ מספר פריק$\}$. זאת אומרת שקיים $y\in\mathbb{N}$ כך ש $y\mid x$ ו $y\neq 1$.

M על קלט x:

1. "תנחש" מחרוזת y באורך כמו המחרוזת x.
2. תבדוק ש $1<y<x$.
3. נבדוק ש y מחלק את x. אם תנאים 2,3 יתקיימו אז נקבל, ואחרת נדחה.

מה זה ניחוש? סדרה של l צעדים אי דטרמיניסטיים שבכל אחד מהם כותבים 0 או 1.

כל אחת מ 2^l המחרוזות שיתקבלו מ $\{0,1\}^l$ נכתבת באחד מ 2^l מסלולי החישוב.

נתאר את הניחוש בצעד מס' 1 עבור M עם שני סרטים:

$$\delta(q_{guess},a,b)=\left((q_{guess},a,0,R,R),(q_{guess},a,1,R,R)\right)\qquad \delta(q_{guess},b,b)=(q_2,\ldots)$$

<u>נכונות:</u>

אם $x\in comp$ אז על פי הגדרת השפה קיים $1<y<x$ המחלק את x.

על פי הבניה יש מסלול חישוב שבו ניחשנו את y ולכן הבדיקה בסעיפים 2,3 תחזיר כן, ולכן במסלול הזה M עוצרת ב q_A ולכן $x\in L(M)$.

אם $x\notin comp$ אז לא קיים y כנ"ל ולכן בכל מסלול (ניחוש) שנבצע, נקבל y שלא מחלק את x או שלא בין 1 ל x. לכן בכל מסלול M תדחה את x ולכן $x\notin L(M)$. לכן $L(M)=comp$

<u>משפט:</u> המודל של מ"ט דטרמיניסטי שקול למודל האי דטרמיניסטי - זאת אומרת: אוסף השפות הניתנות לקבלה זהה בשני המודלים.