Logika és számításelmélet

10. előadás

Rice tétel

Rekurzíve felsorolható nyelvek tulajdonságai

Tetszőleges $\mathcal{P} \subseteq RE$ halmazt a rekurzívan felsorolható nyelvek egy **tulajdonságának** nevezzük. $\mathcal{P}$ **triviális**, ha $\mathcal{P} = \emptyset$ vagy $\mathcal{P} = RE$.

$L_{\mathcal{P}} = \{\langle M \rangle \mid L(M) \in \mathcal{P}\}$.

Rice tétele

Ha $\mathcal{P} \subseteq RE$ egy nem triviális tulajdonság, akkor $L_{\mathcal{P}} \notin R$.

Rice tétel

Bizonyítás

Bizonyítás:

1. eset $\emptyset \notin \mathcal{P}$.

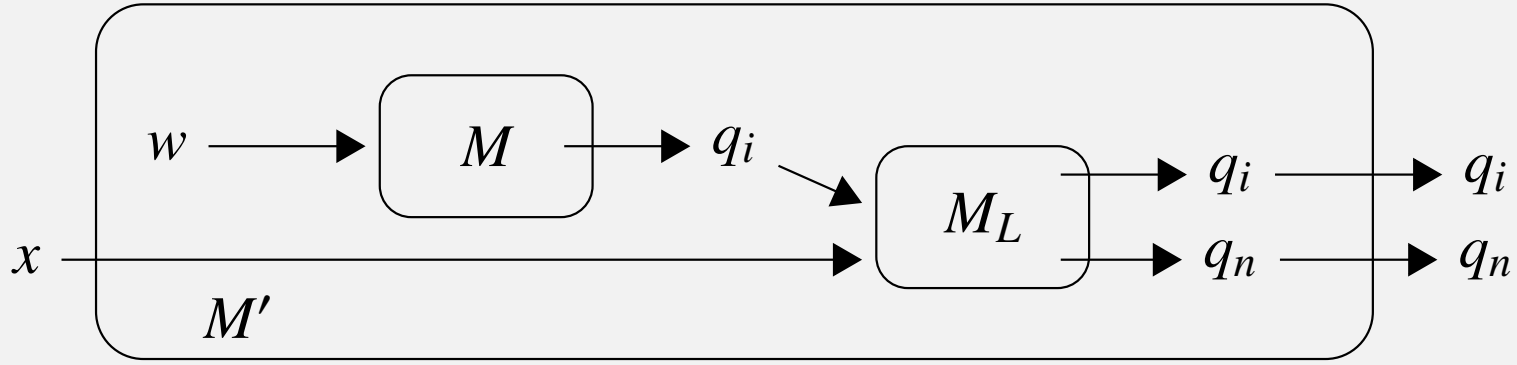
Mivel tudjuk, hogy $L_u \notin R$, elég belátni, hogy $L_u \leq L_{\mathcal{P}}$.
Mivel $\mathcal{P}$ nem triviális, ezért létezik $L \in \mathcal{P}$. ($L \neq \emptyset$).
$L \in RE$, ezért van olyan M_L TG, melyre $L(M_L) = L$.

Egy tetszőleges $\langle M, w \rangle$ TG – bemenet páros hoz elkészítünk egy M' (valójában $M'_{\langle M,w \rangle}$) kétszalagos TG-t, mely egy x bemenetén a következőképpen működik:

1. Bemenetétől függetlenül először szimulálja M-et w-n
2. Így, ha M nem áll meg w-n, M' se áll meg semelyik inputján $\Rightarrow L(M') = \emptyset$.
3. Ha M elutasítja w-t, akkor M' q_n-be lép és leáll (azaz nem fogadja el x-et $\Rightarrow L(M') = \emptyset$.
4. Ha M elfogadja w-t, akkor M' szimulálja M_L -et x-en (azaz $L(M') = L$).

Rice tétel

Bizonyítás



Összefoglalva

- $\langle M, w\rangle \in L_u \Rightarrow L(M') = L \Rightarrow L(M') \in \mathcal{P} \Rightarrow \langle M'\rangle \in L_{\mathcal{P}}$.
- $\langle M, w\rangle \notin L_u \Rightarrow L(M') = \emptyset \Rightarrow L(M') \notin \mathcal{P} \Rightarrow \langle M'\rangle \notin L_{\mathcal{P}}$.

Azaz:
$\langle M, w\rangle \in L_u \Leftrightarrow \langle M'\rangle \in L_{\mathcal{P}}$, tehát $L_u \leq L_{\mathcal{P}}$ és így $L_{\mathcal{P}} \notin R$.

Rice tétel

Bizonyítás

2. eset $\emptyset \in \mathcal{P}$.

- Alkalmazhatjuk az 1. eset eredményét $\overline{\mathcal{P}} = RE \setminus \mathcal{P}$-re, hiszen ekkor $\overline{\mathcal{P}}$ szintén nem triviális és $\emptyset \notin \overline{\mathcal{P}}$.
- Azt kapjuk, hogy $L_{\overline{\mathcal{P}}} \notin R$.
- $\overline{L_{\mathcal{P}}} \notin R$, hiszen ha R-beli lenne akkor a nem TG-kódokat elutasítva $L_{\overline{\mathcal{P}}}$-t eldöntő TG-t kapnánk.
- $\overline{L_{\mathcal{P}}} \notin R \Rightarrow L_{\mathcal{P}} \notin R$ (tétel volt).

Rice tétel

Alkalmazások

Következmények:
Eldönthetetlen, hogy egy M TG

- az üres nyelvet ismeri-e fel. ($\mathcal{P} = \{\emptyset\}$)
- véges nyelvet ismer-e fel ($\mathcal{P} = \{L \mid L \text{ véges }\}$)
- környezetfüggetlen nyelvet ismer-e fel
  ($\mathcal{P} = \{L \mid L \text{ környezetfüggetlen }\}$)
- elfogadja-e az üres szót ($\mathcal{P} = \{L \in RE \mid \varepsilon \in L\}$)
- ...

Post Megfelelkezési Probléma

Legyenek $u_1, \ldots, u_n, v_1 \ldots, v_n \in \Sigma^+$ $(n \geq 1)$.
A $D = \{d_1, \ldots, d_n\}$ halmazt **dominókészletnek** nevezzük ha $d_i = \frac{u_i}{v_n}$ $(1 \leq i \leq n)$.
A $d_{i_1} \cdots d_{i_m}$ sorozat $(m \geq 1)$ a D egy **megoldása**, ha $d_{i_j} \in D$ $(1 \leq j \leq m)$ és $u_{i_1} \cdots u_{i_m} = v_{i_1} \cdots v_{i_m}$.

Példa: Az $\left\{\frac{b}{ca}, \frac{a}{ab}, \frac{ca}{a}, \frac{abc}{c}\right\}$ egy megoldása $\frac{a}{ab}\ \frac{b}{ca}\ \frac{ca}{a}\ \frac{a}{ab}\ \frac{abc}{c}$.
Megjegyzés: Tehát a megoldáshoz a dominók többször felhasználhatók és nem kell mindet felhasználni.

Post Megfelelkezési Probléma (PMP):
$L_{\text{PMP}} = \{\langle D \rangle \mid D\text{-nek van megoldása}\}$.

Tétel

$L_{\text{PMP}} \in RE$.

Bizonyítás: Ha D-t egy ábécének tekintjük, akkor éppen a D feletti szavak a potenciális megoldások. Egy TG, mely ezen D feletti szavakat a hosszlexikografikus sorrendben sorra kipróbálja és ha megoldást talál q_i-ben leáll éppen L_{PMP}-t ismeri fel.

Post Megfelelkezési Probléma

Tétel

$L_{\text{PMP}} \notin R$.

Bizonyítás:
Definiáljuk a PMP egy módosított változatát, MPMP-t. Az MPMP probléma igen-példányai olyan (D, d) (dominókészlet,dominó) párok, melyre D-nek van d-vel kezdődő megoldása.
$L_{\text{MPMP}} = \{\langle D, d\rangle \,|\, d \in D \wedge D\text{-nek van } d\text{-vel kezdődő megoldása}\}$.

Először megmutatjuk, hogy $L_{\text{MPMP}} \leq L_{\text{PMP}}$.

Jelölés: ha $u = a_1 \cdots a_n \in \Sigma^+$ és $* \notin \Sigma$ akkor legyen

balcsillag$(u) := *a_1 * a_2 \cdots * a_n$
jobbcsillag$(u) := a_1 * a_2 * \cdots a_n *$.
mindkétcsillag$(u) := *a_1 * a_2 * \cdots a_n *$.

Post Megfelelkezési Probléma

Legyen $D = \{d_1, \ldots, d_n\}$ egy tetszőleges dominókészlet, ahol $d_i = \frac{u_i}{v_i}$ $(1 \leq i \leq n)$.

D' legyen a következő $|D| + 2$ méretű készlet:

$$d'_0 = \frac{\text{balcsillag}(u_1)}{\text{mindkétcsillag}(v_1)}, \quad d'_i = \frac{\text{balcsillag}(u_i)}{\text{jobbcsillag}(v_1)} \ (1 \leq i \leq n), \quad d'_{n+1} = \frac{*\#}{\#}.$$

Állítás: $\langle D, d_1 \rangle \in L_{\text{MPMP}} \iff \langle D' \rangle \in L_{\text{PMP}}$.

Az állítás bizonyítása:

- ha $d_{i_1} \cdots d_{i_m}$ MPMP egy (D, d_1) bemenetének egy megoldása, akkor $d'_0 d'_{i_2} \cdots d'_{i_m} d'_{n+1}$ megoldása D'-nek, mint PMP inputnak.
- ha $d'_{i_1} \cdots d'_{i_m}$ D'-nek, mint PMP inputnak egy megoldása, akkor az első illetve az utolsó betű egyezése miatt ez csak úgy lehetséges, hogy $d'_{i_1} = d'_0$ és $d'_{i_m} = d'_{n+1}$. Ekkor viszont $d_{i_1} \cdots d_{i_{m-1}}$ megoldása a (D, d_1) MPMP bemenetnek.

Ezzel az állítást bizonyítottuk. Mivel a megfeleltetés TG-pel kiszámítható, ezért $L_{\text{MPMP}} \leq L_{\text{PMP}}$.

Post Megfelelkezési Probléma

Most megmutatjuk, hogy $L_u \leq L_{\text{MPMP}}$.

Minden $\langle M, w\rangle$ (TG, szó) párhoz megadunk egy $\langle D, d\rangle$ (dominókészlet, kezdődominó) párt, úgy hogy

$w \in L(M) \iff D$-nek van d-vel kezdődő megoldása.

Legyen $M = (Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n)$ és $w = a_1 \cdots a_n \in \Sigma^*$.
(D, d) konstrukciója:

- $d := \frac{\#}{\#q_0 a_1 \cdots a_n \#}$ (ahol $\# \notin \Sigma$) $\quad d :\in D$
- – ha $\delta(p, a) = (q, b, R)$, akkor $\frac{pa}{bq} :\in D$
  – ha $\delta(p, a) = (q, b, L)$, akkor $(\forall c \in \Gamma :) \frac{cpa}{qcb} :\in D$
  – ha $\delta(p, a) = (q, b, S)$, akkor $\frac{pa}{qb} :\in D$
- $(\forall a \in \Gamma :) \frac{a}{a} :\in D$
- $\frac{\#}{\#}, \frac{\#}{\sqcup\#}, \frac{\#}{\#\sqcup} :\in D$
- $(\forall a \in \Gamma :) \frac{aq_i}{q_i}, \frac{q_i a}{q_i} :\in D$
- $\frac{q_i \#\#}{\#} :\in D$.

Post Megfelelkezési Probléma

Példa:

Ha M-nek $\delta(q_0, b) = (q_2, a, R)$ és $\delta(q_2, a) = (q_i, b, S)$ átmenetei, akkor $q_0bab \vdash aq_2ab \vdash aq_ibb$ egy bab-ot elfogadó konfigurációátmenet.

Az $\langle M, bab\rangle$-hoz tartozó dominókészlet tartalmazza többek között a

$\frac{\#}{\#q_0bab\#}$ kezdő-, $\frac{q_0b}{aq_2}$ és $\frac{q_2a}{q_ib}$ átmenet- , $\frac{a}{a}$, $\frac{b}{b}$, $\frac{\sqcup}{\sqcup}$ és $\frac{\#}{\#}$ identikus dominókat valamint a befejezéshez szükséges $\frac{aq_i}{q_i}$, $\frac{q_ib}{q_i}$ és $\frac{q_i\#\#}{\#}$ dominókat.

Ekkor egy kirakás (|-al blokkokra osztva):

$$\frac{\#}{\#q_0bab\#} \mid \frac{q_0b}{aq_2}\frac{a}{a}\frac{b}{b}\frac{\#}{\#} \mid \frac{a}{a}\frac{q_2a}{q_ib}\frac{b}{b}\frac{\#}{\#} \mid \frac{aq_i}{q_i}\frac{b}{b}\frac{b}{b}\frac{\#}{\#} \mid \frac{q_ib}{q_i}\frac{b}{b}\frac{\#}{\#} \mid \frac{q_ib}{q_i}\frac{\#}{\#} \mid \frac{q_i\#\#}{\#}$$

Post Megfelelkezési Probléma

$$\frac{\#}{\#q_0bab\#} \mid \frac{q_0b}{aq_2}\frac{a}{a}\frac{b}{b}\frac{\#}{\#} \mid \frac{a}{a}\frac{q_2a}{q_ib}\frac{b}{b}\frac{\#}{\#} \mid \frac{aq_i}{q_i}\frac{b}{b}\frac{b}{b}\frac{\#}{\#} \mid \frac{q_ib}{q_i}\frac{b}{b}\frac{\#}{\#} \mid \frac{q_ib}{q_i}\frac{\#}{\#} \mid \frac{q_i\#\#}{\#}$$

A fenti példán szemléltetjük, hogy $w \in L(M) \iff D$-nek van d-vel kezdődő megoldása.

Az első blokk csak a $d = \frac{\#}{\#q_0bab\#}$ kezdődominóból áll.

A következő két blokkban alul és felül is konfigurációk következnek, felül mindig eggyel "lemaradva".

A 4.-6. blokkokban a $\frac{aq_i}{q_i}$ (és $\frac{q_ia}{q_i}$) típusú dominókkal egyesével behozható a felső szó lemaradása, egészen addig, amíg az alsó rész már csak $q_i\#$-al hosszabb.

Végül a 7. blokkban csak egy (záró)dominó szerepel, melynek az a szerepe, hogy behozza a még megmaradt lemaradást.

Post Megfelelkezési Probléma

A fenti példa alapján meg lehet általános esetben is konstruálni egy megoldást, így $w \in L(M) \Rightarrow$ van $\langle D, d \rangle$-nak megoldása.

Másrészt ha van d-vel kezdődő megoldás, akkor ez a dominósorozat két szavának hosszára vonatkozó megfontolások alapján csak q_i-t tartalmazó dominók használatával lehetséges. Meggondolható, hogy minden kirakás gyakorlatilag konfigurációátmenetek sorozata kell legyen az első q_i megjelenéséig, és így a w szóhoz tartozó kezdőkonfigurációból el lehet jutni elfogadó konfigurációba, azaz $w \in L(M)$.

Nyilván $\langle D, d \rangle$ $\langle M, w \rangle$-ből TG-pel kiszámítható, így beláttuk, hogy $L_u \leq L_{\text{MPMP}}$.

Innen a tétel bizonyítása: $L_u \leq L_{\text{MPMP}}$, $L_{\text{MPMP}} \leq L_{\text{PMP}}$ és tudjuk már, hogy $L_u \notin R$. Ebből a visszavezetés tranzitivitása és korábbi tételünk alapján $L_{\text{PMP}} \notin R$.

CF nyelvtanokkal kapcsolatos eldönthetetlen problémák

Egyértelmű nyelvtan

Egy G környezetfüggetlen (CF, 2-es típusú) nyelvtan **egyértelmű**, ha minden $L(G)$-beli szónak pontosan egy baloldali levezetése van G-ben. (Baloldali levezetés: mindig a legbaloldalibb nemterminálist írjuk át a mondatformában.)
$L_{\text{ECF}} = \{\langle G \rangle \mid G \text{ egy egyértelmű CF nyelvtan}\}$.

Tétel

$L_{\text{ECF}} \notin R$

Bizonyítás: Megmutatjuk, hogy $L_{\text{PMP}} \leq \overline{L_{\text{ECF}}}$.
Legyen $D = \left\{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\right\}$ egy tetszőleges dominókészlet.
$\Delta := \{a_1, \ldots, a_n\}$ úgy, hogy $\Gamma \cap \Delta = \emptyset$.
$P_A := \{A \to u_1 A a_1, \ldots, A \to u_n A a_n,\ A \to \varepsilon\}$.
$P_B := \{B \to v_1 B a_1, \ldots, B \to v_n B a_n,\ B \to \varepsilon\}$.

CF nyelvtanokkal kapcsolatos eldönthetetlen problémák

Egyértelmű nyelvtan

Bizonyítás: (folyt.)
$G_A = \langle A, \{A\}, \Gamma \cup \Delta, P_A \rangle$. $G_B = \langle B, \{B\}, \Gamma \cup \Delta, P_B \rangle$.
$G_D = \langle S, \{S, A, B\}, \Gamma \cup \Delta, \{S \to A, S \to B\} \cup P_A \cup P_B \rangle$.

$f : \langle D \rangle \to \langle G_D \rangle$ visszavezetés, mert:
* ha $\frac{u_{i_1}}{v_{i_1}} \cdots \frac{u_{i_m}}{v_{i_m}}$ megoldása D-nek, akkor $u_{i_1} \cdots u_{i_m} = v_{i_1} \cdots v_{i_m}$.
De ekkor $u_{i_1} \cdots u_{i_m} a_{i_m} \cdots a_{i_1} = v_{i_1} \cdots v_{i_m} a_{i_m} \cdots a_{i_1}$ kétféleképpen is levezethető, így G_D nem egyértelmű.

* ha G_D nem egyértelmű, akkor van olyan szó, aminek két baloldali levezetése van. De ezek $S \to A$-val illetve $S \to B$-vel kell kezdődjenek, hiszen G_A és G_B egyértelmű.A generált szavak xy, $x \in \Gamma^*, y \in \Delta^*$ alakúak, így ugyanaz a generált Γ feletti prefix is. Így a két levezetés D egy megoldását adja.

f nyilván TG-pel kiszámítható. Mivel $L_{\mathrm{PMP}} \notin R$, következik, hogy $\overline{L_{\mathrm{ECF}}} \notin R$, amiből kapjuk, hogy $L_{\mathrm{ECF}} \notin R$.

CF nyelvtanokkal kapcsolatos eldönthetetlen problémák

Közös metszet, ekvivalencia, tartalmazás

Tétel

Eldönthetetlenek az alábbi CF nyelvtanokkal kapcsolatos kérdések. Legyen G_1 és G_2 két CF nyelvtan.

- $L(G_1) \cap L(G_2) \neq \emptyset$
- $L(G_1) = \Gamma^*$ valamely Γ-ra
- $L(G_1) = L(G_2)$
- $L(G_1) \subseteq L(G_2)$

Csak az elsőt bizonyítjuk. L_{PMP}-t vezethetjük vissza rá. Legyen $D = \left\{\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\right\}$ a dominókészlet. Készítsük el a fenti G_A és G_B nyelvtanokat. Könnyen látható, hogy D-nek akkor és csak akkor van megoldása, ha $L(G_A)$-nak és $L(G_B)$-nek van nemüres metszete.
(A másik 3 állítás: biz. nélkül)

Eldönthetetlen problémák az elsőrendű logikában

Tétel

Eldönthetetlen, hogy A elsőrendű logikai formulára

(1) $\models A$ teljesül-e (logikailag igaz-e).

(biz. nélkül). L_{PMP}-t lehet visszavezetni rá. Azaz minden D dominókészlethez megadható egy A_D elsőrendű formula, melyre van D-nek megoldása $\Leftrightarrow \models A_D$. (részletek l. pl. Gazdag jegyzet)

Következmény

Legyen $\mathcal{F}$ egy elsőrendű formulahalmaz és A egy elsőrendű formula. Eldönthetetlen, hogy

(2) A kielégíthetetlen-e

(3) A kielégíthető-e

(4) $\mathcal{F} \models A$ teljesül-e

Bizonyítás: (2) $\models \neg A \Leftrightarrow A$ kielégíthetetlen. (3) Eldönthetetlen nyelv komplementere. (4) Kieléghetetlenségre visszavezethető (l. logika rész).

Eldönthetetlen problémák az elsőrendű logikában

Logikából tanultuk, hogy van olyan algoritmus, ami egy tetszőleges A elsőrendű formulára pontosan akkor áll meg igen válasszal, ha A kielégíthetetlen (például a elsőrendű logika rezolúciós algoritmusa). Ezért a kielégíthetetlenség eldöntése RE-beli probléma.

$\Rightarrow$ a kielégíthetőség eldöntése nem RE-beli probléma.

Mi a helyzet nulladrendű logika esetén?

A fenti kérdések mindegyike eldönthető. (ítélettábla). Véges sok interpretáció van, elsőrendben végtelen.

Nulladrendű logikában, az a kérdés van-e hatékony megoldás.

A továbbiakban az R nyelvosztályt vizsgáljuk. (Bonyolultságelmélet.)

BONYOLULTSÁGELMÉLET

Determinisztikus és nemdeterminisztikus időbonyolultsági osztályok

A továbbiakban eldönthető problémákkal foglalkozunk, ilyenkor a kérdés az, hogy milyen hatékonyan dönthető el az adott probléma.

- $\mathrm{TIME}(f(n)) =$
  $\{L \mid L$ eldönthető $O(f(n))$ időigényű determinisztikus TG-pel$\}$
- $\mathrm{NTIME}(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ időigényű NTG-pel$\}$
- $\mathrm{P} = \bigcup_{k \geq 1} \mathrm{TIME}(n^k)$.
- $\mathrm{NP} = \bigcup_{k \geq 1} \mathrm{NTIME}(n^k)$.
- Észrevétel: $\mathrm{P} \subseteq \mathrm{NP}$.
- Sejtés: $\mathrm{P} \neq \mathrm{NP}$ (sejtjük, hogy igaz, de bizonyítani nem tudjuk).

NP

A P tartalmazza a gyakorlatban is hatékonyan megoldható problémákat.

Milyen problémákat tartalmaz NP?

Egy L NP-beli problémához definíció szerint létezik őt polinom időben eldöntő NTG ami gyakran a következőképpen működik: a probléma minden I bemenetére polinom időben „megsejti” (azaz nemdeterminisztikusan generálja) I egy lehetséges m megoldását és polinom időben leellenőrzi (determinisztikusan), hogy m alapján $I \in L$-e.

A következőkben a P és NP bonyolultsági osztályok közötti kapcsolatot vizsgáljuk.

Polinom idejű visszavezetés

Polinom időben kiszámítható szófüggvény

Az $f : \Sigma^* \to \Delta^*$ szófüggvény **polinom időben kiszámítható**, ha van olyan Turing-gép, ami polinom időben kiszámítja.

Visszavezetés polinom időben

$L_1 \subseteq \Sigma^*$ **polinom időben visszavezethető** $L_2 \subseteq \Delta^*$-ra, ha van olyan $f : \Sigma^* \to \Delta^*$ polinom időben kiszámítható szófüggvény, hogy $w \in L_1 \Leftrightarrow f(w) \in L_2$. Jelölés: $L_1 \leq_p L_2$.

A polinom idejű visszavezetést Richard Karpról elnevezve *Karp-redukciónak* is nevezik.

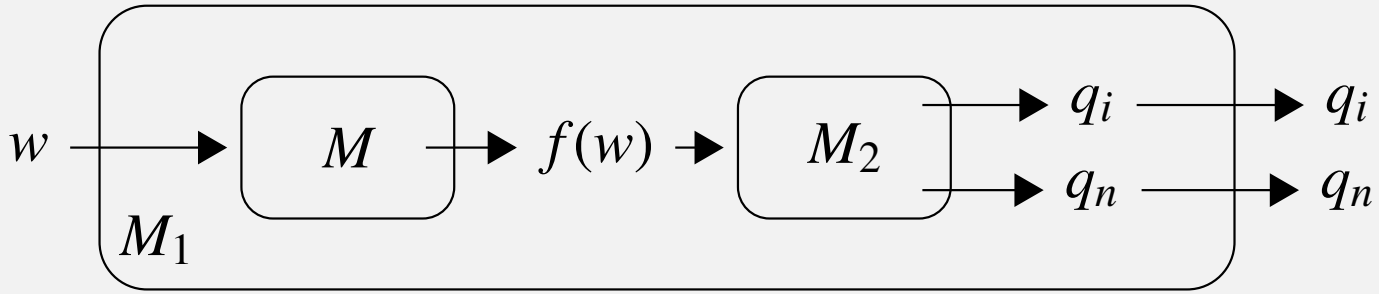
Tétel

- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{P}$, akkor $L_1 \in \mathrm{P}$.
- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{NP}$, akkor $L_1 \in \mathrm{NP}$.

Az elsőt bizonyítjuk, a második analóg.

Polinom idejű visszavezetés

Bizonyítás:
Legyen $L_2 \in$ P és tegyük fel, hogy $L_1 \leq_p L_2$.
Legyen M_2 az L_2-t eldöntő, míg M a visszavezetést kiszámító TG.
Feltehetjük, hogy M $p(n)$ és M_2 $p_2(n)$ polinom idejű TG-ek.
Konstruáljuk meg M_1-et:



- M_1 eldönti az L_1 nyelvet
- ha w n hosszú, akkor $f(w)$ legfeljebb $p(n)$ hosszú lehet
- M_1 időigénye $p_2(p(n))$, ami szintén polinom

Polinom idejű visszavezetés

Adott problémaosztályra nézve nehéz nyelv

Legyen $\mathfrak{C}$ egy problémaosztály. egy L probléma $\mathfrak{C}$**-nehéz** (a polinom idejű visszavezetésre nézve), ha minden $L' \in \mathfrak{C}$ esetén $L' \leq_p L$.

Adott problémaosztályban teljes nyelv

Egy $\mathfrak{C}$-nehéz L probléma $\mathfrak{C}$**-teljes**, ha $L \in \mathfrak{C}$.

Tétel

Legyen L egy NP-teljes probléma. Ha $L \in$ P, akkor P = NP.

Bizonyítás: Elég megmutatni, hogy NP $\subseteq$ P.
Legyen $L' \in$ NP egy tetszőleges probléma.
Ekkor $L' \leq_p L$, hiszen L NP-teljes.
Mivel $L \in$ P, ezért az előző tétel alapján $L' \in$ P.
Ez minden $L' \in$ NP-re elmondható, ezért NP $\subseteq$ P.