Logika és számításelmélet

9. előadás

Számosság

(ismétlés), definíció

A véges halmazok fontos tulajdonsága a méretük ($\Rightarrow$ *természetes számok* fogalma). Cél: ennek kiterjesztése végtelen halmazokra. Egy ilyen általánosítás a **számosság** *(G. Cantor, 1845-1918)*.

Halmazok számossága

- A és B halmazoknak megegyezik a számossága, ha létezik bijekció köztük. Jelölése: $|A| = |B|$.
- A számossága legalább annyi, mint B számossága, ha van B-ből injekció A-ba. Jelölése: $|A| \geq |B|$.
- A számossága nagyobb, mint B számossága, ha van B-ből injekció A-ba, de bijeckió nincs. Jelölése: $|A| > |B|$.

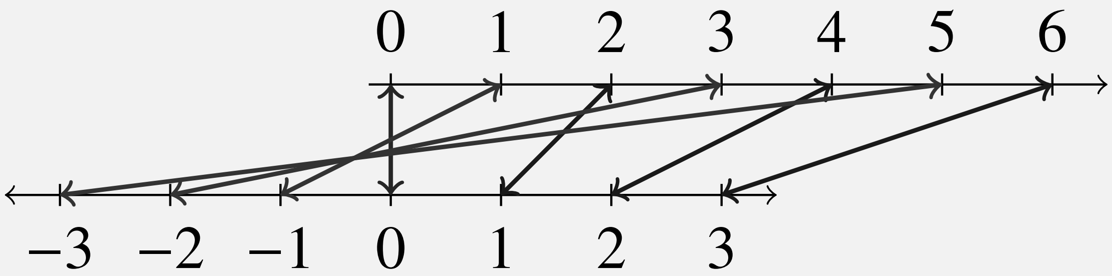
Cantor-Bernstein tétel

Ha A-ból B-be van injekció és B-ből A-ba is van, akkor A és B között bijekció is van, azaz ha $|A| \leq |B|$ és $|A| \geq |B|$, akkor $|A| = |B|$.

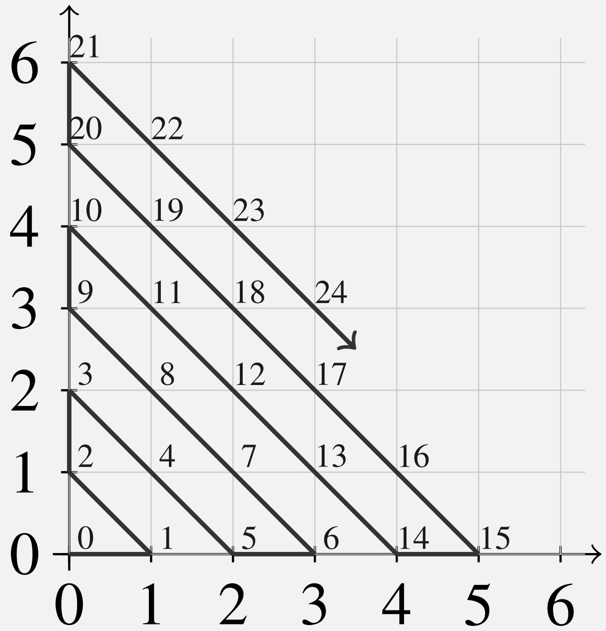
Számosság

Példák

1. Példa: $|\mathbb{N}| = |\mathbb{Z}|$.



2. példa: $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.



Számosság

További példa; a megszámlálhatóan végtelen számosság

3. példa: $|\mathbb{N}| = |\mathbb{Q}|$.
Bizonyítás:
$\mathbb{N} \subset \mathbb{Q}$, ezért $|\mathbb{N}| \leq \mathbb{Q}|$.
$\mathbb{Q}^+ := \{\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+,$ a tört nem egyszerűsíthető$\}$.
$\mathbb{Q}^- := \{-\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+,$ a tört nem egyszerűsíthető$\}$.
$\frac{p}{q} \in \mathbb{Q}^+ \mapsto (p, q) \in \mathbb{N} \times \mathbb{N}$ injektív, tehát $|\mathbb{Q}^+| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.
Legyen $\mathbb{Q}^+ = \{a_1, a_2 \ldots, \}$, $\mathbb{Q}^- = \{b_1, b_2 \ldots, \}$, ekkor
$\mathbb{Q} = \{0, a_1, b_1, a_2, b_2, \ldots\}$

Megszámlálhatóan végtelen számosság

$\mathbb{N}$ számosságát **megszámlálhatóan végtelennek** nevezzük. Egy halmaz **megszámlálható**, ha véges vagy megszámlálhatóan végtelen.

Tétel

Megszámlálható sok megszámlálható halmaz uniója megszámlálható.

Van-e más végtelen számosság a megszámlálhatóan végtelenen kívül?

Igen, $|\mathbb{R}| > |\mathbb{N}|$.

Continuum számosság

$\mathbb{R}$ számosságát **continuumnak** nevezzük.

4. példa: $|\mathbb{R}| = |(0,1)|$.

$\operatorname{tg}(\pi(x - \frac{1}{2}))\big|_{(0,1)} : (0,1) \to \mathbb{R}$ bijekció $(0,1)$ és $\mathbb{R}$ között.

Megjegyzés: $|\mathbb{R}| = |(a,b)| = |[c,d]|$ és $|\mathbb{R}| = |\mathbb{R}^n|$.

5. Példa: $|\{0,1\}^*| = |\mathbb{N}|$.

A hossz-lexikografikus (shortlex) rendezés egy bijekció:
ε,0,1,00,01,10,11,000,001,010,011,100,101,110,111,0000,. . .

6. Példa
$$\Big|\{L \mid L \subseteq \{0,1\}^*\}\Big| = \Big|\{(b_1,\ldots,b_i,\ldots) \mid b_i \in \{0,1\},\ i \in \mathbb{N}\}\Big|$$

Természetes bijekció van köztük:
Soroljuk fel a bináris szavakat a hossz-lexikografikus rendezés szerint.
Egy nyelvhez rendeljük azt a megszámlálhatóan végtelen hosszúságú bitsorozatot, melynek 1 az i. bitje, ha benne van az i. szó, 0 ha nem (a nyelv *karakterisztikus vektorát*).

Jelöljük a jobboldali halmazt $\{0,1\}^{\mathbb{N}}$-nel.

7. Példa $|\{0,1\}^{\mathbb{N}}| = |[0,1)|$.

Bizonyítás (vázlat):

$x \in [0,1)$-hez rendeljük hozzá x kettedestört alakjának "0." utáni részét (ha kettő van akkor az egyiket). Injektív, így $|[0,1)| \leq |\{0,1\}^{\mathbb{N}}|$.

$\mathbf{z} \in \{0,1\}^{\mathbb{N}}$ minden 1-esét helyettesítsük 2-essel, írjuk elé "0."-t és tekintsük harmadostörtnek. Meggondolható, hogy ez injektív megfeleltetés, így $|\{0,1\}^{\mathbb{N}}| \leq |[0,1)|$.

A Cantor-Bernstein tétel alapján $|\{0,1\}^{\mathbb{N}}| = |[0,1)|$.

Számosság

Cantor-féle átlós módszer

Állítás: $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$

Bizonyítás:

$|\{0,1\}^{\mathbb{N}}| \geq |\mathbb{N}|$:

$H_0 := \{(1,0,0,0,\ldots),(0,1,0,0,\ldots),(0,0,1,0,\ldots),\ldots\}$

$H_0 \subset \{0,1\}^{\mathbb{N}}$, és $|H_0| = |\mathbb{N}|$.

Kell: $|\{0,1\}^{\mathbb{N}}| \neq |\mathbb{N}|$.

Számosság

Cantor-féle átlós módszer

Állítás: $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$

Indirekt tegyük fel, hogy $|\{0,1\}^{\mathbb{N}}| = |\mathbb{N}|$. Ez azt jelenti, hogy bijekcióba lehet állítani $\{0,1\}^{\mathbb{N}}$ elemeit $\mathbb{N}$ elemeivel, azaz $\{0,1\}^{\mathbb{N}} = \{u_i \,|\, i \in \mathbb{N}\} = \{u_1, u_2, \dots\}$ a $\{0,1\}^{\mathbb{N}}$ elemeinek egy felsorolása (a természetes számokkal való megindexelése).
Legyen $u_i = (u_{i,1}, u_{i,2}, \dots, u_{i,j}, \dots)$, ahol minden $i, j \in \mathbb{N}$-re $u_{i,j} \in \{0,1\}$.
Tekintsük az $u = \{\overline{u_{1,1}}, \overline{u_{2,2}}, \dots, \overline{u_{i,i}}, \dots)$ megszámlálhatóan végtelen hosszúságú bináris (azaz $\{0,1\}^{\mathbb{N}}$-beli) szót, ahol $\overline{b} = 0$, ha $b = 1$ és $\overline{b} = 1$, ha $b = 0$.

Mivel, minden megszámlálhatóan végtelen hosszúságú bináris szó fel van sorolva, ezért létezik olyan $k \in \mathbb{N}$, melyre $u = u_k$.

Ekkor u k.bitje $u_{k,k}$ (így jelöltük u_k k. bitjét), másrészt $\overline{u_{k,k}}$ (így definiáltuk u-t).
De ez nem lehetséges, tehát az indirekt feltevésünk, azaz hogy $|\{0,1\}^{\mathbb{N}}| = |\mathbb{N}|$ hamis.

Számosság

Cantor-féle átlós módszer

1. Következmény

A continuum számosság nagyobb, mint a megszámlálhatóan végtelen számosság.

2. Következmény

Több $\{0, 1\}$ feletti nyelv van mint $\{0, 1\}$ feletti szó. (Számosság értelemben.)

Számosság

Cantor-féle átlós módszer

Megjegyzés $\{L \mid L \subseteq \{0,1\}^*\} = \mathcal{P}(\{0,1\}^*)$. Igaz-e általában, hogy $|\mathcal{P}(H)| > |H|$?

Tétel

Minden H halmazra $|\mathcal{P}(H)| > |H|$.

Bizonyítás: $|\mathcal{P}(H)| \geq |H|$, hiszen $\{\{h\} \mid h \in H\} \subseteq \mathcal{P}(H)$.

$|\mathcal{P}(H)| \neq |H|$: Cantor-féle átlós módszerrel:
Indirekt $f : \mathcal{P}(H) \leftrightarrow H$ bijekció. Definiálunk egy $A \subseteq H$ halmazt:
$\forall x \in H: \quad x :\in A \iff x \notin f^{-1}(x)$

$f(A) \in A$ igaz-e? Ha igen, $f(A) \notin A$, ha nem $f(A) \in A$, tehát $f(A)$ se az A halmazban, se azon kívül nincs, ellentmondás.

Számítási feladatok megoldása TG-pel

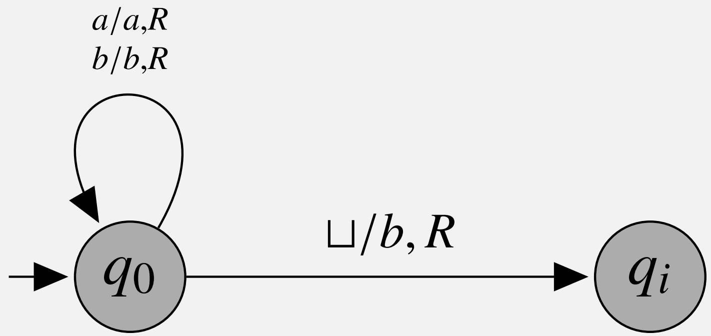
Használhatjuk a TG-eket szófüggvények kiszámítására is. A számítási feladatok megadhatók szófüggvényként.

Szófüggvényt kiszámító TG

Azt mondjuk, hogy az $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, (q_n) \rangle$ TG kiszámítja az $f : \Sigma^* \to \Delta^*$ szófüggvényt, ha minden $u \in \Sigma^*$-beli szóra megáll, és ekkor $f(u) \in \Delta^*$ olvasható az utolsó szalagján.

Megjegyzés: Nincs szükség q_i és q_n megkülönböztetésére, elég lenne egyetlen megállási állapot. [Ezért van q_n ()-ben.]

Példa: $f(u) = ub \quad (u \in \{a, b\}^*)$.



Problémák, mint formális nyelvek

Ha egy problémának megszámlálható sok lehetséges bemenete van (a hétköznapi problémák gyakorlatilag ilyenek), akkor a bemeneteket elkódolhatjuk egy véges ábécé felett.
Fontos-e, hogy mekkora ezen ábécé mérete? Egy d méretű ábécé esetén az első n bemenet elkódolásához nagyjából $log_d n$ hosszú szavak kellenek. Mivel $log_d n = \Theta(log_{d'} n)$, ha $d, d' \geq 2$, ezért a válasz az, hogy nem igazán számít.
De! Ne kódoljunk unárisan! Pl. 2 szám összeadása.

Ha I egy bemenet, jelölje $\langle I \rangle$ az I kódját.

Eldöntési probléma:
$L = \{\langle I \rangle \,|\, I$ a probléma igen példánya$\}$ eldönthető-e Turing géppel.

Kiszámítási probléma:
Van-e olyan TG, ami f-t illetve $\langle I \rangle \mapsto \langle f(I) \rangle$-t számítja ki.

A Turing gépek egy elkódolása

Tegyük fel, hogy $\Sigma = \{0, 1\}$. A fentiek szerint minden input hatékonyan kódolható Σ felett.
Egy M Turing-gép **kódja** (jelölése $\langle M \rangle$) a következő:
Legyen $M = (Q, \{0, 1\}, \Gamma, \delta, q_0, q_i, q_n)$, ahol

- $Q = \{p_1, \ldots, p_k\}$, $\Gamma = \{X_1, \ldots, X_m\}$, $D_1 = R$, $D_2 = S$, $D_3 = L$
- $k \geq 3$, $p_1 = q_0$, $p_{k-1} = q_i$, $p_k = q_n$,
- $m \geq 3$, $X_1 = 0$, $X_2 = 1$, $X_3 = \sqcup$.
- Egy $\delta(p_i, X_j) = (p_r, X_s, D_t)$ átmenet kódja $0^i10^j10^r10^s10^t$.
- $\langle M \rangle$ az átmenetek kódjainak felsorolása 11-el elválasztva.

Észrevétel: $\langle M \rangle$ 0-val kezdődik és végződik, nem tartalmaz 3 darab 1-t egymás után.

$\langle M, w \rangle := \langle M \rangle 111w$

Létezik nem Turing-felismerhető nyelv

Jelölés: Minden $i \geq 1$-re,

- jelölje w_i a $\{0, 1\}^*$ halmaz i-ik elemét a hossz-lexikografikus rendezés szerint.
- jelölje M_i a w_i által kódolt TG-t (ha w_i nem kódol TG-t, akkor M_i egy tetszőleges olyan TG, ami nem fogad el semmit)

Tétel

Létezik nem Turing-felismerhető nyelv.

Bizonyítás: Két különböző nyelvet nem ismerhet fel ugyanaz a TG. A TG-ek számossága megszámlálható (a fenti kódolás injekció $\{0, 1\}^*$-ba, ami volt, hogy megszámlálható). Másrészt viszont a $\{0, 1\}$ feletti nyelvek számossága continuum (volt).

Azaz valójában a nyelvek "többsége" ilyen. Tudnánk-e konkrét nyelvet mutatni? Igen, $L_{\text{átló}} = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$ például ilyen.

$L_{\text{átló}}$ Turing-felismerhetetlen

Tétel

$L_{\text{átló}} \notin RE$.

A Cantor-féle átlós módszerrel adódik:
Bizonyítás: Tekintsük azt a mindkét dimenziójában megszámlálhatóan végtelen méretű T bittáblázatot, melyre $T(i, j) = 1 \;\Leftrightarrow\; w_j \in L(M_i)$ $(i, j \geq 1)$.
Legyen $\mathbf{z}$ a T átlójában olvasható végtelen hosszú bitsztring, $\bar{\mathbf{z}}$ a $\mathbf{z}$ bitenkénti komplementere. Ekkor:

- minden $i \geq 1$-re, T i-ik sora az $L(M_i)$ nyelv karakterisztikus függvénye
- $\bar{\mathbf{z}}$ az $L_{\text{átló}}$ karakterisztikus függvénye
- Minden TG-pel felismerhető, azaz RE-beli nyelv karakterisztikus függvénye megegyezik T valamelyik sorával
- $\bar{\mathbf{z}}$ különbözik T minden sorától
- Ezek alapján $L_{\text{átló}}$ különbözik az összes RE-beli nyelvtől

Az univerzális TG

Felismerhetőség

Univerzális nyelv: $L_u = \{\langle M, w \rangle \mid w \in L(M)\}$.

Tétel

$L_u \in RE$

Bizonyítás: Konstruálunk egy 4 szalagos U "univerzális" TG-et, ami minden TG minden bementére szimulálja annak működését.

1. szalag: U ezt csak olvassa, itt olvasható végig $\langle M, w \rangle$.

2. szalag: M aktuális szalagtartalma (elkódolva a fentiek szerint)

3. szalag: M aktuális állapota (elkódolva a fentiek szerint)

4. szalag: segédszalag

Az univerzális TG

Felismerhetőség

Univerzális nyelv: $L_u = \{\langle M, w\rangle \mid w \in L(M)\}$.

Tétel

$L_u \in RE$

U működése vázlatosan:

- Megnézi, hogy a bemenetén szereplő szó első része kódol-e TG-t; ha nem elutasítja a bemenetet
- ha igen felmásolja w-t a 2., q_0 kódját a 3. szalagra
- Szimulálja M egy lépését:
  – Leolvassa a második szalagról M aktuálisan olvasott szalagszimbólumát
  – Leolvassa a harmadik szalagról M aktuális állapotát
  – Szimulálja M egy lépését (ha kell, használja a segédszalagot) M első szalagon található leírása alapján.
- Ha M aktuális állapota elfogadó vagy elutasító, akkor U is belép a saját elfogadó vagy elutasító állapotába

Az univerzális TG

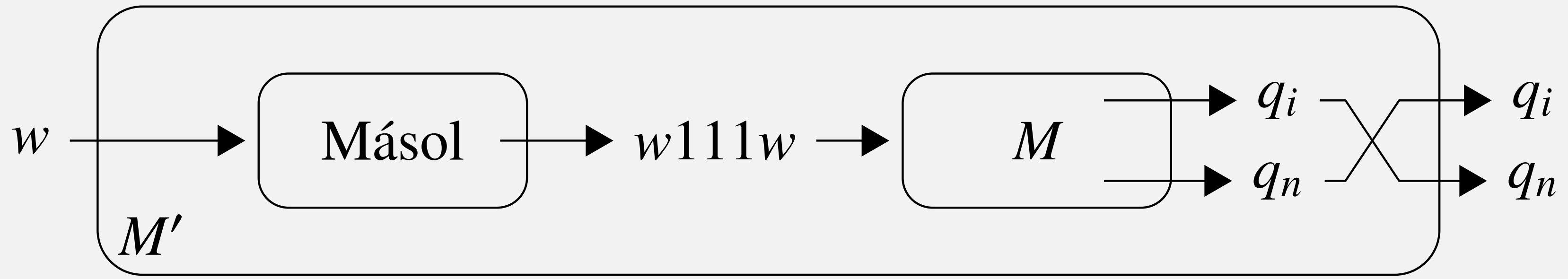
Eldönthetetlenség

Megjegyzés: Ha M nem áll meg w-n, akkor U se áll meg $\langle M, w\rangle$-n, így U nem dönti el L_u-t.

Tétel

$L_u \notin R$.

Bizonyítás: Indirekt, tegyük fel, hogy létezik L_u-t eldöntő M TG. M-et felhasználva készítünk egy $L_{\text{átló}}$-t felismerő M' TG-et.



$w \in L(M') \;\Leftrightarrow w111w \notin L(M) \Leftrightarrow$ a w által kódolt TG nem fogadja el w-t $\Leftrightarrow\; w \in L_{\text{átló}}$.

Tehát $L(M') = L_{\text{átló}}$, ami lehetetlen egy előző tétel miatt.

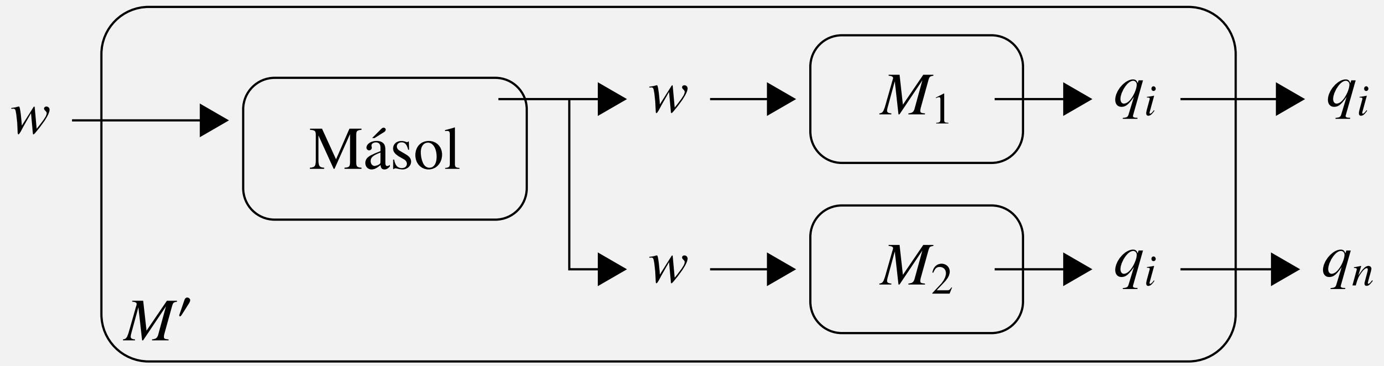
RE és R tulajdonságai

Jelölés: Ha $L \subseteq \Sigma^*$, akkor jelölje $\bar{L} = \{u \in \Sigma^* \mid u \notin L\}$.

Tétel

Ha L és $\bar{L} \in RE$, akkor $L \in R$.

Bizonyítás: Legyen M_1 és M_2 rendre az L-t és $\bar{L}$-t felismerő TG.
Konstruáljuk meg az M' kétszalagos TG-t:



M' lemásolja w-t a második szalagjára, majd felváltva szimulálja M_1 és M_2 egy-egy lépését addig, amíg valamelyik elfogadó állapotba lép. Így M' az L-et ismeri fel, és minden bemeneten meg is áll, azaz $L \in R$.

RE és R tulajdonságai

Következmény

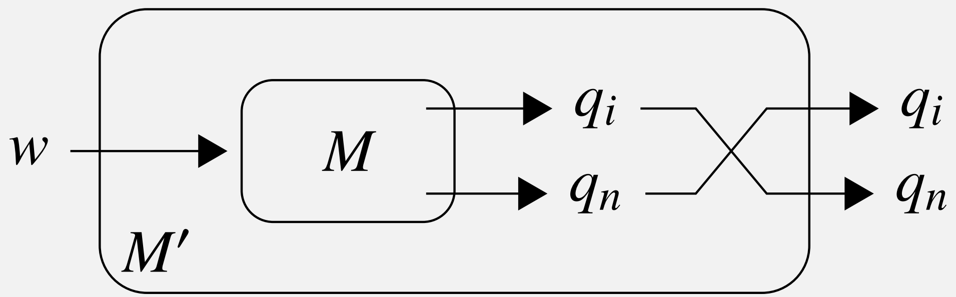
RE nem zárt a komplementer-képzésre.

Bizonyítás:
Legyen $L \in RE \setminus R$ (L_u pl. egy ilyen nyelv) Ekkor $\bar{L} \notin RE$, hiszen ha $\bar{L} \in RE$ lenne, akkor ebből az előző tétel miatt $L \in R$ következne, ami ellentmondás.

Tétel

R zárt a komplementer-képzésre

Bizonyítás: Legyen $L \in R$ és M egy TG, ami az L-t dönti el. Akkor az alábbi M' $\bar{L}$-t dönti el:



Visszavezetés

Kiszámítható szófüggvény

Az $f : \Sigma^* \to \Delta^*$ szófüggvény **kiszámítható**, ha van olyan Turing-gép, ami kiszámítja. [lásd szófüggvényt kiszámító TG]

Visszavezetés

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

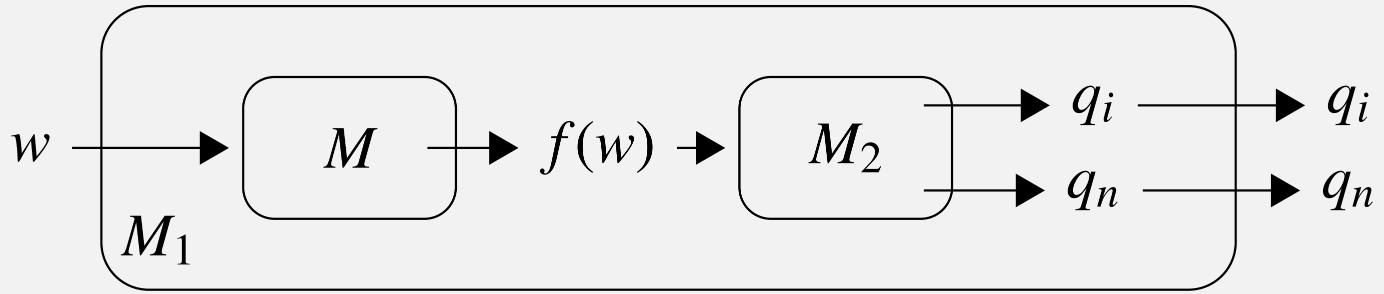
[Emil Posttól származik, angolul many-one reducibility]

Tétel

- Ha $L_1 \leq L_2$ és $L_1 \notin RE$, akkor $L_2 \notin RE$.
- Ha $L_1 \leq L_2$ és $L_1 \notin R$, akkor $L_2 \notin R$.

Visszavezetés

Bizonyítás:
Legyen $L_2 \in RE$ ($\in R$) és tegyük fel, hogy $L_1 \leq L_2$. Legyen M_2 az L_2-t felismerő (eldöntő), M pedig a visszavezetést kiszámító TG. Konstruáljuk meg M_1 -et:



Ha M_2 felismeri L_2-t M_1 is fel fogja ismerni L_1-t, ha el is dönti, akkor M_1 is el fogja dönteni.

Következmény

- Ha $L_1 \leq L_2$ és $L_2 \in RE$, akkor $L_1 \in RE$.
- Ha $L_1 \leq L_2$ és $L_2 \in R$, akkor $L_1 \in R$.

Bizonyítás: Indirekten azonnal adódik a fenti tételből.

A Turing gépek megállási problémája

Megállási probléma:
$L_h = \{\langle M, w\rangle \mid M$ megáll a w bemeneten$\}$.
[Megjegyzés: más jegyzetekben L_{halt} néven is előfordulhat.]
Észrevétel: $L_u \subseteq L_h$

Igaz-e ha $A \subseteq B$, és A eldönthetetlen akkor B is az? Nem.

Tétel

$L_h \notin R$.

Bizonyítás: Az előző tétel alapján elég megmutatni, hogy $L_u \leq L_h$, hiszen tudjuk, hogy $L_u \notin R$.
Tetszőleges M TG-re, legyen M' az alábbi TG
M' tetszőleges u bemeneten a következőket teszi:

1. Futtatja M-et u-n
2. Ha M q_i-be lép, akkor M' is q_i -be lép
3. Ha M q_n-be lép, akkor M' végtelen ciklusba kerül

A Turing gépek megállási problémája

Bizonyítás: (folyt.)

Belátható, hogy

- $f : \langle M, w \rangle \to \langle M', w \rangle$ kiszámítható függvény
- Tetszőleges (M, w) (TG,input)-párra $\langle M, w \rangle \in L_u \Leftrightarrow M$ elfogadja w-t $\Leftrightarrow M'$ megáll w-n $\Leftrightarrow \langle M', w \rangle \in L_h$

Tehát f által L_u visszavezethető L_h-ra. Így $L_h \notin R$.

Megjegyzés: Visszavezetések megadásakor jellemzően csak azon szavakra térünk ki, amelyek ténylegesen kódolnak valamilyen nyelvbeli objektumot (TG-t, (TG,szó) párt, stb.)

Pl. a fenti esetben nem foglalkoztunk azzal, hogy f mit rendeljen olyan szavakhoz, melyek nem kódolnak (TG, szó) párt. Ez általában egy könnyen kezelhető eset, most:

$$f(x) = \begin{cases} \langle M', w \rangle & \text{ha } \exists M \text{ TG, hogy} x = \langle M, w \rangle \\ \varepsilon & \text{egyébként,} \end{cases} \qquad (x \in \{0, 1\}^*)$$

hiszen ε nem kódol (TG,szó) párt (L_h elemei (TG,szó) párok).

A Turing gépek megállási problémája

Tétel

$L_h \in RE$.

Bizonyítás: Az előző tétel következménye alapján elég megmutatni, hogy $L_h \leq L_u$, hiszen tudjuk, hogy $L_u \in RE$. Tetszőleges M Turing-gépre, legyen M' az alábbi TG: M' tetszőleges u bemeneten a következőket teszi:

1. Futtatja M-et u-n
2. Ha M q_i-be lép, akkor M' is q_i -be lép
3. Ha M q_n-be lép, akkor M' q_i -be lép

Belátható, hogy

- $f : \langle M, w\rangle \to \langle M', w\rangle$ kiszámítható függvény
- Tetszőleges (M, w) (TG,input)-párra $\langle M, w\rangle \in L_h \Leftrightarrow M$ megáll w-n $\Leftrightarrow M'$ elfogadja w-t $\Leftrightarrow \langle M', w\rangle \in L_u$

Tehát f által L_h visszavezethető L_u-ra.