

Tétel - Gödel első nemteljességi tétele

Tétel (Gödel első nemteljességi tétele, 1931) Az elemi aritmetikát tartalmazó effektíven kiszámítható elmélet nem lehet egyszerre helyes és teljes. \Rightarrow a Hilbert program megvalósíthatatlan.

Tétel - Chruch, 1936

Tétel (Church, 1936)

Két λ -kalkulusbeli kifejezés ekvivalenciája algoritmikusan eldönthetetlen.

Tétel - Turing, 1936

Tétel (Turing, 1936)

A Turing-gépek megállási problémája algoritmikusan eldönthetetlen.

Turing gép

Turing gép

A **Turing gép** (továbbiakban röviden TG) egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendezett hetes, ahol

- ▶ Q az állapotok véges, nemüres halmaza,
- ▶ $q_0, q_i, q_n \in Q$, q_0 a kezdő- q_i az elfogadó- és q_n az elutasító állapot,
- ▶ Σ és Γ ábécék, a bemenő jelek illetve a szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \setminus \Sigma$.
- ▶ $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, S, R\}$ az átmenet függvény.
 δ az egész $(Q \setminus \{q_i, q_n\}) \times \Gamma$ -n értelmezett függvény.

Turing gép konfiguráció

Konfiguráció

A TG **konfigurációja** egy uqv szó, ahol $q \in Q$ és $u, v \in \Gamma^*, v \neq \varepsilon$.

Egylépéses konfigurációátmenet

$\vdash \subseteq C_M \times C_M$ egylépéses konfigurációátmenet

Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$, $u, v \in \Gamma^*$.

- ▶ Ha $\delta(q, a) = (r, b, R)$, akkor $uqav \vdash ubrv'$, ahol $v' = v$, ha $v \neq \varepsilon$, különben $v' = \sqcup$,
- ▶ ha $\delta(q, a) = (r, b, S)$, akkor $uqav \vdash urbv$,
- ▶ ha $\delta(q, a) = (r, b, L)$, akkor $uqav \vdash u'rcbv$, ahol $c \in \Gamma$ és $u'c = u$, ha $u \neq \varepsilon$, különben $u' = u$ és $c = \sqcup$.

Többlépéses konfigurációátmenet

$\vdash^* \subseteq C_M \times C_M$ többlépéses konfigurációátmenet

$C \vdash^* C' \Leftrightarrow$

- ▶ ha $C = C'$ vagy
- ▶ ha $\exists n > 0 \wedge C_1, C_2, \dots \in C_n \in C_M$, hogy $\forall 1 \leq i \leq n - 1$ -re $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

Az M TG által felismert nyelv

Az M TG által felismert nyelv

$L(M) = \{u \in \Sigma^* \mid q_0 u \sqcup \vdash^* xq_i y \text{ valamely } x, y \in \Gamma^*, y \neq \varepsilon\}$.

Turing-felismerhető

Egy $L \subseteq \Sigma^*$ nyelv **Turing-felismerhető**, ha $L = L(M)$ valamely M TG-re.

eldönthető

Egy $L \subseteq \Sigma^*$ nyelv **eldönthető**, ha létezik olyan M TG, mely minden bemeneten megállási konfigurációba jut és $L(M) = L$.

rekurzívan felsorolható

A Turing-felismerhető nyelveket szokás **rekurzívan felsorolhatónak** (vagy *parciálisan rekurzívnak*, vagy *félíg eldönthetőnek*) az eldönthető nyelveket pedig **rekurzívnak** is nevezni.

A rekurzívan felsorolható nyelvek osztályát *RE* -vel, a rekurzív nyelvek osztályát pedig *R*-rel jelöljük.

futási ideje (időigénye)

Egy *M* TG **futási ideje (időigénye)** az *u* szón *n* ($n \geq 0$), ha *M* az *u*-hoz tartozó kezdőkonfigurációból *n* lépésekben (konfigurációátmenettel) jut el megállási konfigurációba. Ha nincs ilyen szám, akkor *M* futási ideje az *u*-n végtelen.

Legyen $f : \mathbb{N} \rightarrow \mathbb{N}$ egy függvény. Azt mondjuk, hogy *M* **időigénye** $f(n)$ (vagy, hogy *M* egy $f(n)$ időkorlátos gép), ha minden $u \in \Sigma^*$ input szóra, *M* időigénye az *u* szón legfeljebb $f(|u|)$.

Függvények aszimptotikus felső korlát, alsó korlát és éles korlátja

Legyenek $f, g : \mathbb{N} \rightarrow \mathbb{R}_0^+$ függvények, ahol \mathbb{N} a természetes számok, \mathbb{R}_0^+ pedig a nemnegatív valós számok halmaza.

- ▶ f -nek g aszimptotikus felső korlátja (jelölése: $f(n) = O(g(n))$);
ejtsd: $f(n) = \text{nagyordó } g(n)$) ha létezik olyan $c > 0$ konstans és $N \in \mathbb{N}$ küszöbindex, hogy $f(n) \leq c \cdot g(n)$ minden $n \geq N$ -re.
- ▶ f -nek g aszimptotikus alsó korlátja (jelölése: $f(n) = \Omega(g(n))$) ha létezik olyan $c > 0$ konstans és $N \in \mathbb{N}$ küszöbindex, hogy $f(n) \geq c \cdot g(n)$ minden $n \geq N$ -re.
- ▶ f -nek g aszimptotikus éles korlátja (jelölése: $f(n) = \Theta(g(n))$) ha léteznek olyan $c_1, c_2 > 0$ konstansok és $N \in \mathbb{N}$ küszöbindex, hogy $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$ minden $n \geq N$ -re.

Függvények aszimptotikus nagyságrend szerinti osztályozása
2-arithású reláció

O, Ω, Θ 2-arithású relációnak is felfogható az $\mathbb{N} \rightarrow \mathbb{R}_0^+$ függvények univerzumán, ekkor

- ▶ O, Ω, Θ tranzitív (pl. $f = O(g), g = O(h) \Rightarrow f = O(h)$)
- ▶ O, Ω, Θ reflexív
- ▶ Θ szimmetrikus
- ▶ O, Ω fordítottan szimmetrikus ($f = O(g) \Leftrightarrow g = \Omega(f)$)
- ▶ (köv.) Θ ekvivalenciareláció, az $\mathbb{N} \rightarrow \mathbb{R}_0^+$ függvények egy osztályozását adja. Az egyes függvényosztályokat általában "legegyszerűbb" tagjukkal reprezentáljuk. Pl. 1 (korlátos függvények), n (lineáris függvények), n^2 (négyzetes függvények), stb.

Függvények aszimptotikus nagyságrend szerinti osztályozása
Tételek: Összeadásra való zártság, pozitív konstanssal szorzásra való zártság, szekvencia tétele, határérték

- ▶ $f, g = O(h) \Rightarrow f + g = O(h)$, hasonlóan Ω -ra, Θ -ra.
(Összeadásra való zártság)
- ▶ Legyen $c > 0$ konstans $f = O(g) \Rightarrow c \cdot f = O(g)$, hasonlóan Ω -ra, Θ -ra. (Pozitív konstanssal szorzásra való zártság)
- ▶ $f + g = \Theta(\max\{f, g\})$ (szekvencia tétele). A domináns tag határozza meg egy összeg aszimptotikus nagyságrendjét.
- ▶ Ha létezik az f/g határérték
 - ha $f(n)/g(n) \rightarrow +\infty \Rightarrow f(n) = \Omega(g(n))$ és $f(n) \neq O(g(n))$
 - ha $f(n)/g(n) \rightarrow c$ ($c > 0$) $\Rightarrow f(n) = \Theta(g(n))$
 - ha $f(n)/g(n) \rightarrow 0 \Rightarrow f(n) = O(g(n))$ és $f(n) \neq \Omega(g(n))$

k-szalagos Turing-gép

k-szalagos Turing-gép

A **k-szalagos Turing-gép** egy olyan $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendszer, ahol

- Q az állapotok véges, nemüres halmaza,
- $q_0, q_i, q_n \in Q$, q_0 a kezdő- q_i az elfogadó- és q_n az elutasító állapot,
- Σ és Γ ábécék, a bemenő jelek illetve a szalagszimbólumok ábécéje úgy, hogy $\Sigma \subseteq \Gamma$ és $\sqcup \in \Gamma \setminus \Sigma$,
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, S, R\}^k$ az átmenet függvény.

Konfiguráció k-szalagos Turing-gép

Konfiguráció

k-szalagos TG konfigurációja egy $(q, u_1, v_1, \dots, u_k, v_k)$ szó, ahol $q \in Q$ és $u_i, v_i \in \Gamma^*$, $v_i \neq \varepsilon$ ($1 \leq i \leq k$).

Kezdőkonfiguráció

Kezdőkonfiguráció

Az u szóhoz tartozó **kezdőkonfiguráció**: $u_i = \varepsilon$ ($1 \leq i \leq k$), $v_1 = u \sqcup$, és $v_i = \sqcup$ ($2 \leq i \leq k$).

Elfogadó/elutasító/megállási konfiguráció

Elfogadó/elutasító/megállási konfiguráció

A $(q, u_1, v_1, \dots, u_k, v_k)$ konfiguráció, ahol $q \in Q$ és $u_i, v_i \in \Gamma^*$, $v_i \neq \varepsilon$ ($1 \leq i \leq k$), **elfogadó konfiguráció**, ha $q = q_i$, **elutasító konfiguráció**, ha $q = q_n$, **megállási konfiguráció**, ha $q = q_i$ vagy $q = q_n$.

Egylépéses konfigurációátmenet k-szalagos Turing-gép

Legyen $k=2$ és $\delta(q, a_1, a_2) = (r, b_1, b_2, R, S)$ a TG egy átmenete.

Ekkor $(q, u_1, a_1 v_1, u_2, a_2 v_2) \vdash (r, u_1 b_1, v'_1, u_2, b_2 v_2)$, ahol $v'_1 = v_1$, ha $v_1 \neq \varepsilon$, különben $v'_1 = \sqcup$.

Többlépéses konfigurációátmenet k-szalagos Turing-gép

$\vdash^* \subseteq C_M \times C_M$ többlépéses konfigurációátmenet

$C \vdash^* C' \Leftrightarrow$

- ▶ ha $C = C'$ vagy
- ▶ ha $\exists n > 0 \wedge C_1, C_2, \dots \in C_n \in C_M$, hogy $\forall 1 \leq i \leq n - 1$ -re
 $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

k-szalagos Turing-gép által felismert nyelv

***k*-szalagos Turing-gép által felismert nyelv**

$L(M) = \{u \in \Sigma^* \mid (q_0, \varepsilon, u\sqcup, \varepsilon, \sqcup, \dots, \varepsilon, \sqcup) \vdash^*$
 $(q_i, x_1, y_1, \dots, x_k, y_k), x_1, y_1 \dots, x_k, y_k \in \Gamma^*, y_1, \dots, y_k \neq \varepsilon\}.$

k-szalagos Turing-gép futási ideje adott szóra

***k*-szalagos Turing-gép futási ideje adott szóra**

Egy *k*-szalagos Turing-gép **futási ideje** egy u szóra a hozzá tartozó kezdőkonfigurációból egy megállási konfigurációba megtett lépések száma.

Ekvivalens Turing-gépek

Ekvivalens TG-ek

Két TG **ekvivalens**, ha ugyanazt a nyelvet ismerik fel.

Tétel Szimulálás egy szalaggal k-szalagos Turing-Gép

Tétel

Minden M k -szalagos Turing-géphez megadható egy vele ekvivalens M' egyszalagos Turing-gép. Továbbá, ha M legalább lineáris időigényű $f(n)$ időkorlátos gép (azaz $f(n) \geq n$), akkor M' $O(f(n)^2)$ időkorlátos.

Bizonyítás Szimulálás egy szalaggal

A szimuláció menete egy $a_1 \dots a_n$ bemeneten:

1. M' kezdőkonfigurációja legyen $q'_0 \# \hat{a}_1 a_2 \dots a_n \# \hat{\sqcup} \# \dots \hat{\sqcup} \#$
2. M' először végigmegy a szalagon (számolja a #-okat) és eltárolja a $\hat{\sqcup}$ -pal megjelölt szimbólumokat az állapotában
3. M' méggyeszer végigmegy a szalagján és M átmenetfüggvénye alapján aktualizálja azt
4. ha M valamelyik szalagján nő a szó hozza, akkor M' -nek az adott ponttól mozgatnia kell a szalagja tartalmát jobbra
5. Ha M elfogadó vagy elutasító állapotba lép, akkor M' is belép a saját elfogadó vagy elutasító állapotába
6. Egyébként M' folytatja a szimulációt a 2-ik ponttal

Bizonyítás Szimulálás egy szalaggal -időigény

Meggondolható, hogy M egyetlen lépéseinak szimulálásakor

- ▶ a lépések számára aszimptotikus felső korlát az M' által addig felhasznált cellaterület (tár). (Kétszer végigmegy M' szalagján, legfeljebb k -szor kell egy \sqcup -nek helyet csinálni, ami szintén $O(\text{felhasznált cellaterület})$)
- ▶ a felhasznált cellaterület $O(1)$ -el nőtt. ($\leq k$ -val, hiszen $\leq k$ -szor kell egy \sqcup -t beszúrni)

Az M' által felhasznált cellaterület mérete kezdetben $\Theta(n)$, lépésenként $O(1)$ -gyel nőhet, így $O(n + f(n)O(1)) = O(n + f(n))$ közös, minden lépés után igaz aszimptotikus felső korlát az M' által felhasznált cellaterület méretére.

Tehát M minden egyes lépéseinak szimulációja $O(n + f(n))$ M' -beli lépés.

Így M' összesen $f(n) \cdot O(n + f(n))$ időkorlátos, ami $O(f(n)^2)$, ha $f(n) = \Omega(n)$.

Tétel Turing-gép egy irányban végtelen szalaggal

Tétel

Minden egyszalagos M Turing-géphez van vele ekvivalens egyirányban végtelen szalagos M'' Turing-gép.

Nemdeterminisztikus Turing-gép (NTG)

Nemdeterminisztikus Turing-gép (NTG)

A **nemdeterminisztikus Turing-gép** (NTG) olyan $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ rendszer, ahol

- ▶ $Q, \Sigma, \Gamma, q_0, q_i, q_n$ ugyanaz, mint eddig
- ▶ $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, S, R\})$

Egylépéses konfigurációátmenet Nemdeterminisztikus TG

$\vdash \subseteq C_M \times C_M$ egylépéses konfigurációátmenet

Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$, $u, v \in \Gamma^*$.

- ▶ Ha $(r, b, R) \in \delta(q, a)$, akkor $uqav \vdash ubrv'$, ahol $v' = v$, ha $v \neq \epsilon$, különben $v' = \sqcup$,
- ▶ ha $(r, b, S) \in \delta(q, a)$, akkor $uqav \vdash urbv$,
- ▶ ha $(r, b, L) \in \delta(q, a)$, akkor $uqav \vdash u'rcbv$, ahol $c \in \Gamma$ és $u'c = u$, ha $u \neq \epsilon$ különben $u' = u$ és $c = \sqcup$

Többlépéses konfigurációátmenet Nemdeterminisztikus TG

$\vdash^* \subseteq C_M \times C_M$ többlépéses konfigurációátmenet

$C \vdash^* C' \Leftrightarrow$

- ▶ ha $C = C'$ vagy
- ▶ ha $\exists n > 0 \wedge C_1, C_2, \dots \in C_n \in C_M$, hogy $\forall 1 \leq i \leq n - 1$ -re $C_i \vdash C_{i+1}$ valamint $C_1 = C$ és $C_n = C'$.

Nemdeterminisztikus Turing-gép által felismert nyelv

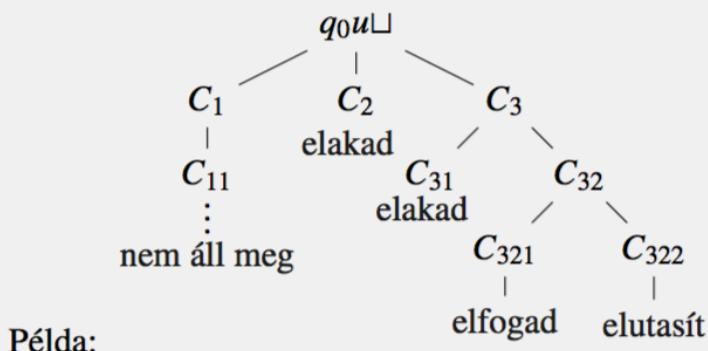
NTG által felismert nyelv

$$L(M) = \{u \in \Sigma^* \mid q_0 u \sqcup \vdash^* x q_i y \text{ valamely } x, y \in \Gamma^*, y \neq \epsilon\}.$$

Nemdeterminisztikus számítási fa

$u \in \Sigma^*$ nemdeterminisztikus számítási fája

Irányított fa, melynek csúcsai konfigurációkkal címkézettek. $q_0 u \sqcup$ a gyökér címkéje. Ha C egy csúcs címkéje, akkor $\{C' \mid C \vdash C'\}$ gyereke van és ezek címkéi éppen $\{C' \mid C \vdash C'\}$ elemei.



Elfogadja u -t, hiszen a $q_0 u \sqcup \vdash C_3 \vdash C_{32} \vdash C_{321}$ számítása elfogadó konfigurációba visz. Egy ilyen számítás is elég az elfogadáshoz.

eldönti, időkorlátos Nemdeterminisztikus TG

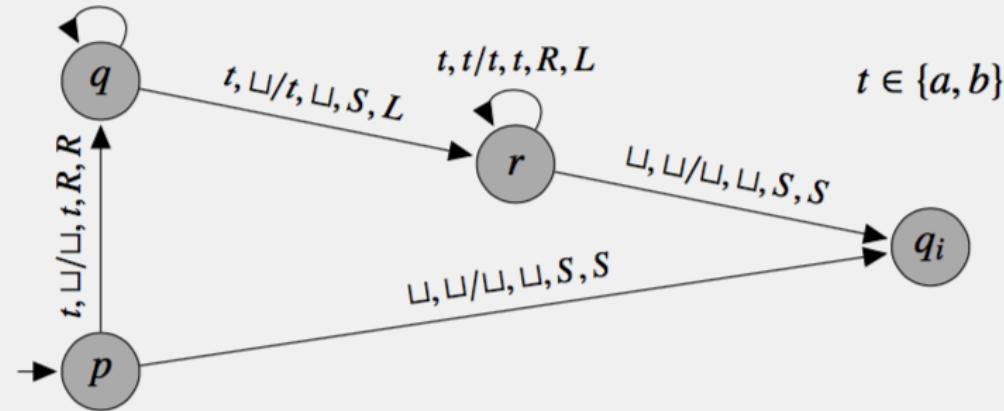
M **eldönti** az $L \subseteq \Sigma^*$ nyelvet, ha felismeri és minden $u \in \Sigma^*$ szóra az M számítási fája véges és minden levele elfogadó vagy elutasító konfiguráció.

M $f(n)$ **időkorlátos** (időigényű), ha minden $u \in \Sigma^*$ n hosszú szóra u számítási fája legfeljebb $f(n)$ magas.

Nemdeterminisztikus Turing-gép példa

Feladat: Készítsünk egy M nemdeterminisztikus Turing-gépet, melyre $L(M) = \{ww^{-1} \mid w \in \{a, b\}^*\}$!

$t, \sqcup/\sqcup, t, R, R$



Szimulálás determinisztikus TG-pel

Tétel

Minden $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ $f(n)$ idejű NTG-hez megadható egy ekvivalens, $2^{O(f(n))}$ idejű M' determinisztikus TG.

Halmazok számossága

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 tételek

Cantor-Bernstein tételek

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 $|A| = |B|$.

Megszámlálhatóan végtelen számosság

Megszámlálhatóan végtelen számosság

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

Tétel

Megszámlálható sok megszámlálható halmaz uniója megszámlálható.

Continuum számosság

Continuum számosság

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

Állítás Cantor-féle átlós módszer - bizonyítás

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

Bizonyítás:

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

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

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

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

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 $\{0, 1\}^{\mathbb{N}} = \{u_i \mid i \in \mathbb{N}\} = \{u_1, u_2, \dots\}$ 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 hosszságú bináris (azaz $\{0, 1\}^{\mathbb{N}}$ -beli) szót, ahol $\bar{b} = 0$, ha $b = 1$ és $\bar{b} = 1$, ha $b = 0$.

Mivel, minden megszámlálhatóan végtelen hosszságú 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.

Tétel Cantor-féle átlós módszer

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:

$$\forall x \in H : x \in A \Leftrightarrow x \notin f^{-1}(x)$$

$f(A) \in A$ 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.

Szófüggvényt kiszámító Turing-gép

Szófüggvényt kiszámító TG

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

Egy M Turing-gép kódja

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

- $Q = \{p_1, \dots, p_k\}$, $\Gamma = \{X_1, \dots, X_m\}$, $D_1 = R$, $D_2 = S$, $D_3 = L$
- $k \geq 3$, $p_1 = q_0$, $p_{k-1} = q_i$, $p_k = q_n$,
- $m \geq 3$, $X_1 = 0$, $X_2 = 1$, $X_3 = \sqcup$.
- Egy $\delta(p_i, X_j) = (p_r, X_s, D_t)$ átmenet kódja $0^i 10^j 10^r 10^s 10^t$.
- $\langle M \rangle$ az átmenetek kódjainak felsorolása 11-el elválasztva.

Tétel bizonyítás Létezik nem Turing-felimserhető nyelv

Tétel

Létezik nem Turing-felismerhető nyelv.

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

tétel bizonyítás Látló Turing-felismerhetetlen

Tétel

$L_{\text{átló}} \notin RE$.

A Cantor-féle átlós módszerrel adódik:

Bizonyítás: Tekintsük azt a minden 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

tétel bizonyítás felismerhetőség Univerzális Turing-gép

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.

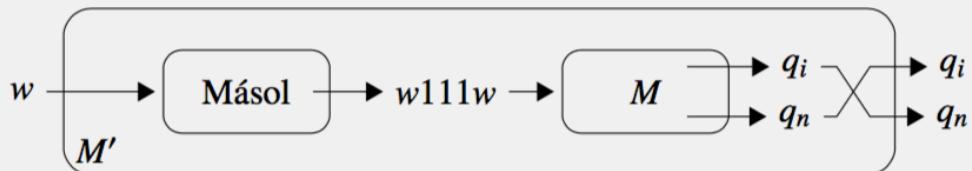
- 1. szalag:** U ezt csak olvassa, itt olvasható végig $\langle M, w \rangle$.
- 2. szalag:** M aktuális szalagtartalma (elkódolva a fentiek szerint)
- 3. szalag:** M aktuális állapota (elkódolva a fentiek szerint)
- 4. szalag:** segédszalag

tétel bizonyítás Eldönthetetlenség Univerzális TG

Tétel

$L_u \notin R$.

Bizonyítás: Indirekt, tegyük fel, hogy létezik L_u -t előző 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.

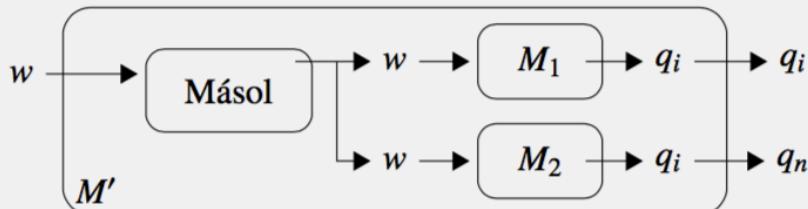
Tétel bizonyítás RE és R tulajdonságai

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 $L \in R$.

tétel bizonyítás RE (nem) zárt a komplementer-képzésre (következmény)

Következmény

RE nem zárt a komplementer-képzésre.

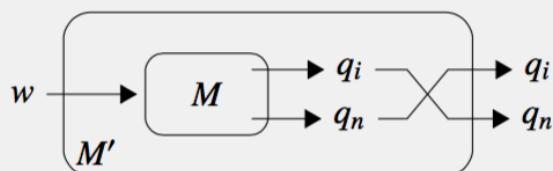
Bizonyítás:

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:



Kiszámítható szófüggvény

Kiszámítható szófüggvény

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

def, téTEL bIZONYÍTÁS Visszavezetés

Visszavezetés

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

[Emil Posttól származik, angolul many-one reducibility]

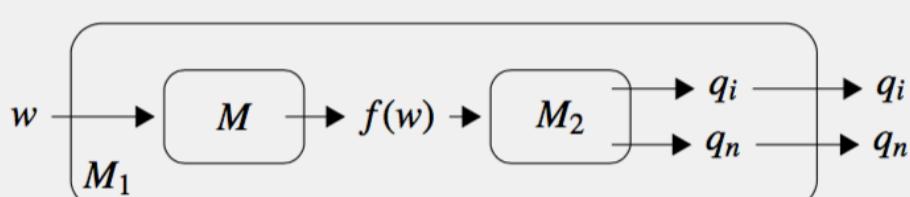
TéTEL

- 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 $L_2 \notin R$.

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 döntenı.

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 $L_1 \in R$.

Turing gépek megállási problémája Tétel bizonyítás

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

Belátható, hogy

- $f : \langle M, w \rangle \rightarrow \langle M', w \rangle$ 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:

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

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

Turing gépek megállási problémája Tétel bizonyítás

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

- $f : \langle M, w \rangle \rightarrow \langle M', w \rangle$ 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.

Rekurzíve felsorolható nyelvek tulajdonságai

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 $\mathcal{P} = RE$.

Rice tételezés bizonyítása

Rice tétele

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

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 pároshoz elkészítünk egy M' (valójában $M'_{\langle M, w \rangle}$) kétsalagos 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 $L(M') = L$).

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 $L_{\mathcal{P}} \notin R$.

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.
- $\overline{L_{\mathcal{P}}} \notin R \Rightarrow L_{\mathcal{P}} \notin R$ (tételezés volt).

Post megfelelkezési probléma def téTEL bizonítás

Legyenek $u_1, \dots, u_n, v_1, \dots, v_n \in \Sigma^+$ ($n \geq 1$).

A $D = \{d_1, \dots, d_n\}$ 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 $\frac{a}{ab} \frac{b}{ca} \frac{ca}{a} \frac{a}{ab} \frac{abc}{c}$.

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.

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.

$L_{\text{MPMP}} = \{\langle D, d \rangle \mid d \in D \wedge D\text{-nek van } d\text{-vel kezdődő megoldása}\}$.

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) := $a_1 * a_2 * \cdots * a_n *$.

mindkétszíllag(u) := $* a_1 * a_2 * \cdots * a_n *$.

Post Megfelelkezési Probléma dominőkészlet def állítás bizonyítás

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

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

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

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 $L_{\text{MPMP}} \leq L_{\text{PMP}}$.

CF nyelvtanokkal kapcsolatos eldönthetetlen problémák

Nyelvtan egyértelmű nyelvtan def térel bizonyítás

Egy G környezetfüggetlen (CF, 2-es típusú) nyelvtan **egyértelmű**, ha minden $L(G)$ -beli szónak pontosan egy baloldali levezetése van G -ben. (Baloldali levezetés: minden 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 $D = \left\{ \frac{u_1}{v_1}, \dots, \frac{u_n}{v_n} \right\}$ egy tetszőleges dominókészlet.

$\Delta := \{a_1, \dots, a_n\}$ úgy, hogy $\Gamma \cap \Delta = \emptyset$.

$$P_A := \{A \rightarrow u_1 A a_1, \dots, A \rightarrow u_n A a_n, A \rightarrow \varepsilon\}.$$

$$P_B := \{B \rightarrow v_1 B a_1, \dots, B \rightarrow v_n B a_n, B \rightarrow \varepsilon\}.$$

$$G_A = \langle A, \{A\}, \Gamma \cup \Delta, P_A \rangle. G_B = \langle B, \{B\}, \Gamma \cup \Delta, P_B \rangle.$$

$$G_D = \langle S, \{S, A, B\}, \Gamma \cup \Delta, \{S \rightarrow A, S \rightarrow B\} \cup P_A \cup P_B \rangle.$$

$f : \langle D \rangle \rightarrow \langle G_D \rangle$ 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 $S \rightarrow A$ -val illetve $S \rightarrow B$ -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 $L_{\text{PMP}} \notin R$, következik, hogy $\overline{L_{\text{ECF}}} \notin R$, amiből kapjuk, hogy $L_{\text{ECF}} \notin R$.

Eldönthetetlen CF nyelvtanokkap kapcsolatos kérdések tételek bizonyítás

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 $D = \left\{ \frac{u_1}{v_1}, \dots, \frac{u_n}{v_n} \right\}$ 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)

Elsőrendű logikai formulára A teljesül-e tétele következmény bizonyítás

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)

Polinom idő

Polinom időben kiszámítható szófüggvény

Az $f : \Sigma^* \rightarrow \Delta^*$ 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 $f : \Sigma^* \rightarrow \Delta^*$ 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 $L_2 \in P$, akkor $L_1 \in P$.
- ▶ Ha $L_1 \leq_p L_2$ és $L_2 \in NP$, akkor $L_1 \in NP$.

Az elsőt bizonyítjuk, a második analóg.

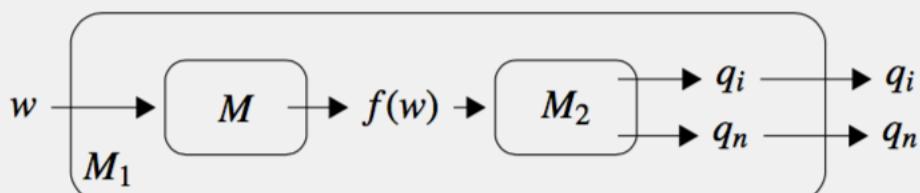
Bizonyítás:

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

Nehéz nyelv, teljes nyelv téTEL bIZONYÍTÁS

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 $NP \subseteq P$.

NP-teljes nyelv polinom idejű visszavezetésre nézve

NP-teljes nyelv

Egy L probléma **NP-teljes** (a polinom idejű visszavezetésre nézve), ha

- ▶ $L \in NP$
- ▶ L NP-nehéz, azaz minden $L' \in NP$ esetén $L' \leq_p L$.

Cook Tétel SAT

$SAT = \{\langle \varphi \rangle \mid \varphi \text{ kielégítható nulladrendű KNF}\}$

Tétel (Cook)

SAT NP-teljes.

kSAT Tétel Bizonyítás

Tétel

Ha L NP-teljes, $L \leq_p L'$ és $L' \in NP$, akkor L' NP-teljes.

Bizonyítás: Legyen $L'' \in NP$ tetszőleges. Mivel L NP-teljes, ezért $L'' \leq_p L$. Mivel a feltételek szerint $L \leq_p L'$, ezért a polinom idejű visszavezetések tranzitívitása miatt ($p_1(p_2(n))$ is polinom!) L' NP-nehéz. Ebből és a 3. feltételből kövezkezik az állítás.

Tehát polinom idejű visszavezetéssel további nyelvek NP-teljessége bizonyítható.

$kSAT = \{\langle \varphi \rangle \mid \varphi \text{ kielégíthető KNF és minden tagban pontosan } k \text{ különböző literál van}\}.$

Az ilyen formulákat k KNF-nek nevezzük a továbbiakban.

3SAT tétele bizonyítása

Tétel

3SAT NP-teljes.

- 3SAT NP-beli: lásd SAT
- $SAT \leq_p 3SAT$
Kell $f : \varphi \mapsto \varphi'$, φ KNF, φ' 3KNF, φ' kielégíthető $\Leftrightarrow \varphi$ kielégíthető, f polinom időben kiszámolható.

$\varphi \mapsto \varphi'$:

ℓ	$\ell \vee X \vee Y, \ell \vee X \vee \neg Y, \ell \vee \neg X \vee Y, \ell \vee \neg X \vee \neg Y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee X, \ell_1 \vee \ell_2 \vee \neg X$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee X, \neg X \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \dots \vee \ell_n (n \geq 5)$	$\ell_1 \vee \ell_2 \vee X_1, \neg X_1 \vee \ell_3 \vee X_2, \dots, \neg X_{n-2} \vee \ell_{n-1} \vee \ell_n$

$X, Y, X_1, \dots, X_{n-2}$ új ítéletváltozók. φ' ezek konjunkciója.

Megjegyzés: HORNSAT: mint SAT, de klózonként max. 1 pozitív literál lehet. HORNSAT és 2SAT $\in P$.

Gráf k -színezhető 3színezés

Egy gráf **k -színezhető**, ha csúcsai k színnel színezhetők úgy, hogy a szomszédos csúcsok színei különbözőek.

3Színezés = $\{\langle G \rangle \mid G \text{ 3-színezhető}\}$

Tétel

3Színezés NP-teljes.

Klikk, független ponthalmaz

Az alábbi nyelvek esetén G egyszerű, irányítatlan gráf k pedig egy nemnegatív egész. G egy teljes részgráfját **klikknek**, egy üres részgráfját **független ponthalmaznak** mondjuk.

KLIKK = $\{\langle G, k \rangle \mid G\text{-nek van } k \text{ méretű klikkje}\}$

FÜGGETLEN PONTHALMAZ =

$\{\langle G, k \rangle \mid G\text{-nek van } k \text{ méretű független ponthalmaza}\}$

csúcshalmaz ponthalmaz lefogja, lefogó

Legyen $S \subseteq V(G)$ és $E \in E(G)$. Ha $S \cap E \neq \emptyset$, akkor a csúcshalmaz **lefogja** E -t. Ha S minden $E \in E(G)$ élt lefog, akkor S egy **lefogó ponthalmaz**.

[Megjegyzés: LEFOGÓ PONTHALMAZ a Gazdag jegyzetben csúcslefedés néven szerepel]

LEFOGÓ PONTHALMAZ= $\{\langle G, k \rangle \mid G\text{-nek van } k \text{ méretű lefogó ponthalmaza}\}$

Ha G -nek van k méretű klikkje/független ponthalmaza, akkor bármely kisebb k -ra is van. Ha van k méretű lefogó ponthalmaz, akkor bármely nagyobb k -ra is van ($k \leq |V(G)|$).

hipergráf halmazrendszer lefogó ponthalmaz tételek bizonyítás

\mathcal{S} egy **hipergráf** (vagy halmazrendszer), ha $\mathcal{S} = \{A_1, \dots, A_n\}$, ahol $A_i \subseteq U$, ($1 \leq i \leq n$) valamely U alaphalmazra. $H \subseteq U$ egy **lefogó ponthalmaz**, ha $\forall 1 \leq i \leq n : H \cap A_i \neq \emptyset$.

HIPERGRÁF LEFOGÓ PONTHALMAZ= $\{\langle \mathcal{S}, k \rangle \mid \mathcal{S} \text{ egy hipergráf és } \mathcal{S}\text{-hez van } k \text{ elemű lefogó ponthalmaz}\}.$

Tétel

HIPERGRÁF LEFOGÓ PONTHALMAZ NP-teljes.

Bizonyítás: **HIPERGRÁF LEFOGÓ PONTHALMAZ** NP-beli, hiszen polinom időben ellenőrizhető, hogy U egy részhalmaza minden \mathcal{S} -beli halmazt metsz-e.

LEFOGÓ PONTHALMAZ a **HIPERGRÁF LEFOGÓ PONTHALMAZ** speciális esete, hiszen a gráf a hipergráf speciális esete: egy gráf éleire úgy gondolunk, mint 2-elemű halmazokra, így a gráf éleinek halmaza egy hipergráf. (A visszavezetés az identikus leképezés.

$U := V(G)$, $\mathcal{S} := E(G)$, k ugyanaz).

Hamilton út hamilton kör

Hamilton út/kör

Adott egy $G = (V, E)$ irányítatlan / irányított gráf ($|V| = n$). Egy $P = v_{i_1}, \dots, v_{i_n}$ felsorolása a csúcsoknak **Hamilton út** G -ben, ha $\{v_{i_1}, \dots, v_{i_n}\} = V$ és minden $1 \leq k \leq n - 1$ -re $\{v_{i_k}, v_{i_{k+1}}\} \in E$ (illetve irányított esetben $(v_{i_k}, v_{i_{k+1}}) \in E$). Ha $\{v_{i_n}, v_{i_1}\} \in E$ (illetve irányított esetben $(v_{i_n}, v_{i_1}) \in E$) is teljesül, akkor P **Hamilton kör**.

Hamilton út teljes téTEL bIZONYÍTÁS

TéTEL

HÚ NP-teljes

BIZONYÍTÁS: NP-beli, hiszen polinom időben előállítható egy n darab csúcs egy P felsorolása. P -ről polinom időben ellenőrizhető, hogy a csúcsok egy permutációja-e és hogy tényleg H-út-e.

Irányítatlan hamilton út teljes téTEL bIZONYÍTÁS

TéTEL

IHÚ NP-teljes

BIZONYÍTÁS: $\text{IHÚ}_{\leq_p} \text{IHÚ}$. Adott G, s, t , ahol G irányított. Kell G', s', t' , ahol G' irányítatlan és akkor és csak akkor van G -ben s -ből t -be H-út, ha G' -ben van s' -ből t' -be.

G minden v csúcsának feleljen meg G' -ben 3 csúcs v_{be} , $v_{\text{közép}}$ és v_{ki} .
és G' élei közé vegyük be a $\{v_{\text{be}}, v_{\text{közép}}\}$ és $\{v_{\text{közép}}, v_{\text{ki}}\}$ éleket. Továbbá minden $E = (u, v)$ G -beli él estén adjuk hozzá $E(G')$ -höz $\{u_{\text{ki}}, v_{\text{be}}\}$ -t.
 $s' := s_{\text{be}}$, $t' := t_{\text{ki}}$.

Könnyű látni, hogy ha P H-út G -ben, akkor P' H-út G' -ben, ahol P' -t úgy kapjuk P -ból, hogy minden v csúcsot v_{be} , $v_{\text{közép}}$ és v_{ki} -vel helyettesítünk, ebben a sorrendben.

Fordítva, könnyen látható, hogy ha P egy H-út G' -ben akkor v_{be} , $v_{\text{közép}}$, v_{ki} sorrendű 3-asok követik egymást (különben a $v_{\text{közép}}$ -eket nem tudnánk felfűzni). Ezeket a 3-asokat v -vel helyettesítve egy G -beli utat kapunk.

Az utak kezdetére és végére vonatkozó feltételek is teljesülnek.

Irányítatlan hamilton kör teljes téTEL bIZONYÍTÁS

TÉTEL

IHK NP-teljes

BIZONYÍTÁS: $\text{IHÚ} \leq_p \text{IHK}$. Adott G, s, t . G' konstrukciójában adjunk hozzá egy új x csúcsot és két új élt $\{s, x\}$ -et és $\{t, x\}$ -t G -hez.

Könnyen meggondolható, hogy akkor és csak akkor van G -ben s -t H-út, ha G' -ben van H-kör.

co bonyolultsági osztály def téTEL biz

co \mathfrak{C} bonyolultsági osztály

Ha \mathfrak{C} egy bonyolultsági osztály $\text{co}\mathfrak{C} = \{L \mid \bar{L} \in \mathfrak{C}\}$.

Bonyolultsági osztály polinom idejű visszavezetésre való zártsága

\mathfrak{C} zárt a polinomidejű visszavezetésre nézve, ha minden esetben ha $L_2 \in \mathfrak{C}$ és $L_1 \leq_p L_2$ teljesül következik, hogy $L_1 \in \mathfrak{C}$.

Volt: P és NP zártak a polinomidejű visszavezetésre nézve.

TÉTEL

Ha \mathfrak{C} zárt a polinomidejű visszavezetésre nézve, akkor $\text{co}\mathfrak{C}$ is.

BIZONYÍTÁS: Legyen $L_2 \in \text{co}\mathfrak{C}$ és L_1 tetszőleges nyelvek, melyekre $L_1 \leq_p L_2$. Utóbbiból következik, hogy $\bar{L}_1 \leq_p \bar{L}_2$ (ugyanaz a visszavezetés jó!). Mivel $\bar{L}_2 \in \mathfrak{C}$, ezért a téTEL feltétele miatt $\bar{L}_1 \in \mathfrak{C}$. Azaz $L_1 \in \text{co}\mathfrak{C}$.

KÖVETKEZMÉNY

coNP zárt a polinom idejű visszavezetésre nézve.

TÉTEL

$L \in \mathfrak{C}$ -teljes $\iff \bar{L} \in \text{co}\mathfrak{C}$ -teljes.

BIZONYÍTÁS:

- ▶ Ha $L \in \mathfrak{C}$, akkor $\bar{L} \in \text{co}\mathfrak{C}$.
- ▶ Legyen $L' \in \mathfrak{C}$, melyre $L' \leq_p L$. Ekkor $\bar{L}' \leq_p \bar{L}$.
Ha L' befutja \mathfrak{C} -t akkor \bar{L}' befutja $\text{co}\mathfrak{C}$ -t. Azaz minden $\text{co}\mathfrak{C}$ -beli nyelv polinom időben visszavezethető \bar{L} -re.

Tehát \bar{L} $\text{co}\mathfrak{C}$ -beli és $\text{co}\mathfrak{C}$ -nehéz, így $\text{co}\mathfrak{C}$ -teljes.

Off-line Turing-gép

Off-line Turing-gép

Az **off-line Turing-gép** egy legalább 3 szalagos gép, amelynek az első szalagja csak olvasható, az utolsó szalagja csak írható. További szalagjait munkaszalagoknak nevezzük.

Off-line TG-ek tárígénye

Az off-line TG **tárígénye** egy adott inputra a munkaszalagjain felhasznált cellák száma. Egy TG $f(n)$ **tárkorlátos**, ha bármely u inputra legfeljebb $f(|u|)$ tárat használ.

ELÉR probléma

ELÉR = { $\langle G, s, t \rangle$ | A G irányított gráfban van s -ből t -be út}.

ELÉR $\in P$ (valójában $O(n^2)$, lásd Algoritmusok és adatszerk. II., szélességi/mélységi bejárás)

Tétel

ELÉR $\in \text{SPACE}(\log^2 n)$.

Bizonyítás:

- ▶ Rögzítsük a csúcsok egy tetszőleges sorrendjét.
- ▶ $\text{ÚT}(x, y, i) :=$ igaz, ha létezik x -ból y -ba legfeljebb 2^i hosszú út.
- ▶ s -ből van t -be út G -ben $\iff \text{ÚT}(x, y, \lceil \log n \rceil) =$ igaz.
- ▶ $\text{ÚT}(x, y, i) =$ igaz $\iff \exists z (\text{ÚT}(x, z, i - 1) =$ igaz $\wedge \text{ÚT}(z, y, i - 1) =$ igaz).
- ▶ Ez alapján egy rekurzív algoritmust készítünk, melynek persze munkaszalagján tárolnia kell, hogy a felsőbb szinteken milyen (x, y, i) -kre létezik folyamatban lévő hívás.
- ▶ ha $i = 0$, akkor $2^0 = 1$ hosszú út (megnézi az inputot).
- ▶ A munkaszalon (x, y, i) típusú hármasok egy legfeljebb $\lceil \log n \rceil$ hosszú sorozata áll. A hármasok 3. attribútuma 1-esével csökkenő sorozatot alkot $\lceil \log n \rceil$ -től
- ▶ $\text{ÚT}(x, y, i)$ meghívásakor az utolsó hármas (x, y, i) a munkaszalagon. Az algoritmus felírja az $(x, z, i - 1)$ hármasat a munkaszalagra (x, y, i) utáni helyre majd kiszámítja $\text{ÚT}(x, z, i - 1)$ értékét.
- ▶ Ha hamis, akkor kitörli $(x, z, i - 1)$ -et és z értékét növeli.
- ▶ Ha igaz, akkor is kitörli $(x, z, i - 1)$ -et és $(z, y, i - 1)$ -et ráírja, (y -t tudja az előző (x, y, i) hármasból).
 - Ha igaz, akkor $\text{ÚT}(x, y, i)$ igaz, visszalép $((x, y, i)$ és $(z, y, i - 1)$ 2. argumentumának egyezéséből látja)
 - Ha hamis akkor kitörli és z értékét eggyel növelve $\text{ÚT}(x, z, i - 1)$ -en dolgozik tovább.
- ▶ Ha egyik z se volt jó, akkor $\text{ÚT}(x, y, i)$ hamis.

Konfigurációs gráf

Az $\text{ÚT}(s, t, \lceil \log n \rceil)$ algoritmus a munkaszalagján $O(\log n)$ darab tagból álló egyenként $O(\log n)$ hosszú (x, y, i) hármast tárol, így $\text{ELÉR} \in \text{SPACE}(\log^2 n)$.

Konfigurációs gráf

Egy M TG G_M **konfigurációs gráfjának** csúcsai M konfigurációi és $(C, C') \in E(G_M) \Leftrightarrow C \vdash_M C'$.

Elérhetőségi módszer: bonyolultsági osztályok közötti összefüggéseket lehet bizonyítani az $\text{ELÉR} \in \text{P}$ vagy $\text{ELÉR} \in \text{SPACE}(\log^2 n)$ tételeket alkalmazva a konfigurációs gráfra, vagy annak egy részgráfjára.

Savitch tétele

Savitch tétele

Ha $f(n) \geq \log n$, akkor $\text{NSPACE}(f(n)) \subseteq \text{SPACE}(f^2(n))$.

Bizonyítás: Legyen M egy $f(n)$ tárigényű NTG és w az M egy n hosszú bemenete.

Ekkor M egy konfigurációját $O(f(n) + \log n)$ tárral eltárolhatjuk (aktuális állapot, a munkaszalagok tartalma, fejek pozíciója, az első szalag fejének pozíciója n féle lehet, ezért $\geq \log n$ tár kell ennek eltárolásához). Ha $f(n) \geq \log n$, akkor ez $O(f(n))$.

Feltehető, hogy M -nek csak egy elfogadó konfigurációja van.
(Törölje le a TG a munkaszalagjait, mielőtt q_i -be lép!)

A legfeljebb ekkora méretű konfigurációkat tartalmazó konfigurációs gráf mérete $2^{df(n)}$ valamely $d > 0$ konstansra. Így az előző tétel szerint $O(\log^2(2^{df(n)})) = O(f^2(n))$ tárral egy determinisztikus TG eldönti, hogy

$\text{ÚT}(c_{\text{kezdő}}, c_{\text{elfogadó}}, \lceil \log(2^{df(n)}) \rceil)$ igaz-e.

Savitch tétele következmény

Következmény

PSPACE = NPSPACE

Bizonyítás: polinom négyzete is polinom.

Tétel

$NL \subseteq P$

Bizonyítás

Legyen $L \in NL$ és M L -et $f(n) = O(\log n)$ tárral eldöntő NTG.

Meggondolható, hogy egy n méretű inputra M legfeljebb $f(n)$ méretű szalagtartalmakat tartalmazó konfigurációinak a száma legfeljebb $cnd^{\log n}$ alkalmas c, d konstansokkal, ami egy $p(n)$ polinommal felülről becsülhető. Így a G konfigurációs gráfnak legfeljebb $p(n)$ csúcsa van. G polinom időben megkonstruálható.

Feltehető, hogy G -ben egyetlen elfogadó konfiguráció van. G -ben a kezdőkonfigurációból az elfogadó konfiguráció elérhetősége $O(p^2(n))$ idejű determinisztikus TG-pel eldönthető, azaz $L \in P$.

L és NL

ELÉR fontos szerepet tölt be az $L \stackrel{?}{=} NL$ kérdés vizsgálatában is.

Tétel

ELÉR $\in NL$

Bizonyítás: Az M 3-szalagos NTG a (G, s, t) inputra ($n = |V(G)|$) a következőt teszi:

- ▶ ráírja s -t a második szalagra
- ▶ ráírja a 0-t a harmadik szalagra
- ▶ Amíg a harmadik szalagon n -nél kisebb szám áll
 - Legyen u a második szalagon lévő csúcs
 - Nemdeterminisztikusan felírja u helyére egy v ki-szomszédját a második szalagra
 - Ha $v = t$, akkor elfogadja a bemenetet, egyébként növeli a harmadik szalagon lévő számot binárisan eggyel
- ▶ Elutasítja a bemenetet
- ▶ Mindkét szalag tartalmát $O(\log n)$ hosszú kóddal tárolhatjuk.

LOG táras visszavezetés, NL-nehéz, NL-teljes nyelv

Log. táras visszavezetés

Egy $L_1 \subseteq \Sigma^*$ nyelv **logaritmikus tárral visszavezethető** egy $L_2 \subseteq \Delta^*$ nyelvre $L_1 \leq_{\ell} L_2$, ha $L_1 \leq L_2$ és a visszavezetéshez használt függvény kiszámítható logaritmikus táras determinisztikus (off-line) Turing-géppel

NL-nehéz, NL-teljes nyelv

Egy L nyelv **NL-nehéz** (a log. táras visszavezetésre nézve), ha minden $L' \in \text{NL}$ nyelvre, $L' \leq_{\ell} L$; ha ráadásul $L \in \text{NL}$ is teljesül, akkor L **NL-teljes** (a log. táras visszavezetésre nézve)

Tétel

L zárt a logaritmikus tárral való visszavezetésre nézve

Bizonyítás: Tegyük fel, hogy $L_1 \leq_{\ell} L_2$ és $L_2 \in \text{NL}$.

Legyen M_2 az L_2 -t eldöntő, M pedig a visszavezetésben használt f függvényt kiszámoló logaritmikus táras determinisztikus TG.

Az M_1 TG egy tetszőleges u szóra a következőképpen működik

- ▶ A második szalagján egy bináris számlálóval nyomon követi, hogy M_2 feje hányadik betűjét olvassa az $f(u)$ szónak; legyen ez a szám i (kezdetben 1)
- ▶ Amikor M_2 lépne egyet, akkor M_1 az M -et szimulálva előállítja a harmadik szalagon $f(u)$ i -ik betűjét (de csak ezt a betűt!!!)
- ▶ Ezután M_1 szimulálja M_2 aktuális lépését a harmadik szalagon lévő betű felhasználásával és aktualizálja a második szalagon M_2 fejének újabb pozícióját
- ▶ Ha eközben M_1 azt látja, hogy M_2 elfogadó vagy elutasító állapotba lép, akkor M_1 is belép a saját elfogadó vagy elutasító állapotába, egyébként folytatja a szimulációt a következő lépéssel

Belátható, hogy M_1 L_1 -et dönti el és a működése során csak logaritmikus méretű tárat használ, azaz $L_1 \in L$.

ELÉR NL teljessége

Következmény

Ha L NL-teljes és $L \in L$, akkor $L = NL$.

Bizonyítás: Legyen $L' \in NL$ tetszőleges, ekkor $L \leq_{\ell} L'$ és $L \in L'$, így L logaritmikus tárral való visszavezetésre nézve zártsága miatt $L' \in NL$. Tehát $L = NL$.

Tétel

ELÉR NL-teljes a logaritmikus tárral történő visszavezetésre nézve.

Bizonyítás:

- ▶ Korábban láttuk, hogy $ELÉR \in NL$
- ▶ Legyen $L \in NL$, megmutatjuk, hogy $L \leq_{\ell} ELÉR$
- ▶ Legyen M egy L -et eldöntő $O(\log n)$ táras NTG és $|u| = n$
- ▶ Az $O(\log n)$ tárat használó konfigurációk $\leq c \cdot \log n$ hosszúak (alkalmas c -re)

Immerman-Szelepcsényi téTEL

Immerman-Szelepcsényi téTEL

$NL = coNL$

Hierarchia tétele

$\text{EXPTIME} := \bigcup_{k \in \mathbb{N}} \text{TIME}(2^{n^k})$.

Tétel

$\text{NL} \subset \text{PSPACE}$ és $\text{P} \subset \text{EXPTIME}$.

(biz. nélkül)

Tétel

$\text{L} \subseteq \text{NL} = \text{coNL} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} \subseteq \text{EXPTIME}$

Bizonyítás: 1 és 4 definíció szerint, 2-es Immerman-Szelepcsényi, 3-ast előbb bizonyítottuk. 5-ös: egy TG-nek "nincs ideje" több tárat használni, mint időt. 6-os: elérhetőségi módszerrel. A használt tárban exponenciális méretű lesz a konfigurációs gráf, a gráf méretében négyzetes (azaz összességében a tár méretében exponenciális) időben tudjuk az elérhetőséget tesztelni a kezdőkonfigurációból az elfogadóba konfigurációba.

Sejtés: Utóbbiban minden tartalmazás valódi.