Számításelmélet kidolgozás

Turing gépek

http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/07/EA07SZ2.pdf
http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/08/EA08SZ2.pdf

Tétel (Church, 1936)

Két λ-kalkulusbeli kifejezés ekvivalenciája algoritmikusan eldönthetetlen.

Tétel (Turing, 1936)

A Turing-gépek megállási problémája algoritmikusan eldönthetetlen.

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 $\sqcup \in \Gamma \setminus \Sigma$.
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \to Q \times \Gamma \times \{L, S, R\}$ az átmenet függvény. δ az egész $(Q \setminus \{q_i, q_n\}) \times \Gamma$-n értelmezett függvény.

Konfiguráció

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

Az uqv konfiguráció egy tömör leírás a TG aktuális helyzetéről, mely a gép további működése szempontjából minden releváns információt tartalmaz: a szalag tartalma uv (uv előtt és után a szalagon már csak $\sqcup$ van), a gép a q állapotban van és az író-olvasó fej a v szó első betűjén áll. Két konfigurációt azonosnak tekintünk, ha csak balra/jobbra hozzáírt $\sqcup$-ekben térnek el egymástól.

A gép egy $u \in \Sigma^*$-beli szóhoz tartozó **kezdőkonfigurációja** a $q_0u\sqcup$ szó. (Vagyis q_0u, ha $u \neq \varepsilon$ és $q_0\sqcup$, ha $u = \varepsilon$).
Elfogadó konfigurációi azon konfigurációk, melyre $q = q_i$.
Elutasító konfigurációi azon konfigurációk, melyre $q = q_n$.
Az elfogadó és elutasító konfigurációk közös elnevezése **megállási konfiguráció**.

Jelölje C_M egy M TG-hez tartozó lehetséges konfigurációk halmazát. M $\vdash \subseteq C_M \times C_M$ **konfigurációátmenet-relációját** az alábbiak szerint definiáljuk.

$\vdash \subseteq C_M \times C_M$ 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: $\vdash$ reflexív, tranzitív lezártja, azaz:

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

$C \vdash^* C' \Leftrightarrow$

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

Az M TG által felismert nyelv

$L(M) = \{u \in \Sigma^* \mid q_0u\sqcup \vdash^* xq_iy$ valamely $x, y \in \Gamma^*, y \neq \varepsilon\}$.

Figyeljük meg, hogy $L(M)$ csak Σ feletti szavakat tartalmaz.

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

A Turing-felismerhető nyelveket szokás **rekurzívan felsorolható**nak (vagy *parciálisan rekurzívnak*, vagy *félig eldönthetőnek*) az eldönthető nyelveket pedig **rekurzív**nak is nevezni.

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

Nyilván $R \subseteq RE$. Igaz-e hogy $R \subset RE$?

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

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

Gyakran megelégszünk azzal, hogy a pontos időkorlát helyett jó aszimptotikus felső korlátot adunk az időigényre.

Legyenek $f, g : \mathbb{N} \to \mathbb{R}_0^+$ 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: $f(n)$ = 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.

O, Ω, Θ 2-aritású relációnak is felfogható az $\mathbb{N} \to \mathbb{R}_0^+$ 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 $\mathbb{N} \to \mathbb{R}_0^+$ függvények egy osztályozását adja. Az egyes függvényosztályokat általában "legegyszerűbb" tagjukkal reprezentáljuk. Pl. 1 (korlátos függvények), n (lineáris függvények), n^2 (négyzetes függvények), stb.

- $f, g = O(h) \ \Rightarrow\ f + g = O(h)$, 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 $f(n)/g(n) \to +\infty \Rightarrow f(n) = \Omega(g(n))$ és $f(n) \neq O(g(n))$

  ha $f(n)/g(n) \to c \quad (c > 0) \Rightarrow f(n) = \Theta(g(n))$

  ha $f(n)/g(n) \to 0 \quad \Rightarrow f(n) = O(g(n))$ és $f(n) \neq \Omega(g(n))$

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 $\sqcup \in \Gamma \setminus \Sigma$,
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma^k \to Q \times \Gamma^k \times \{L, S, R\}^k$ az átmenet függvény.

Konfiguráció

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

Ez azt reprezentálja, hogy az aktuális állapot q, az i. szalag tartalma $u_i v_i$ és az i. fej v_i első betűjén áll $(1 \leq i \leq k)$.

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

A $(q, u_1, v_1, \ldots, u_k, v_k)$ 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 $q = q_n$.

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 $v_1' = \sqcup$.

Vegyük észre, hogy a fejek nem kell hogy szikronban lépjenek, egymástól függetlenül mozoghatnak.

Ezek után a **többlépéses konfigurációátmenet** definíciója megegyezik az egyszalagos esetnél tárgyalttal. Jelölés: $\vdash^*$.

k-szalagos Turing-gép által felismert nyelv

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

A k-szalagos TG-ek által **felismerhető** illetve **eldönthető** nyelv fogalma szintén analóg az egyszalagos esettel.

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.

Ezek után az **időigény** definíciója megegyezik az egyszalagos esetnél tárgyalttal.

Ekvivalens TG-ek

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

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.

Tétel

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

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
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, S, R\})$

Konfigurációk C_M halmazának fogalma azonos.

$\vdash \subseteq C_M \times C_M$ 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 $v \neq \varepsilon$, 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 $u \neq \varepsilon$, különben $u' = u$ és $c = \sqcup$.

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

$C \vdash^* C' \Leftrightarrow$

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

NTG által felismert nyelv

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

Egy NTG-re úgy gondolhatunk, hogy több számítása is lehet ugyanarra a szóra. Akkor fogad el egy szót, ha legalább egy számítása q_i-ben ér véget.

$u \in \Sigma^*$ 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.

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.

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.

Számosság / Nyelvek

http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/09/EA09SZ2.pdf
http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/10/EA10SZ2.pdf

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 $|A| = |B|$.

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

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

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.)

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

Tétel

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

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.]

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

Eldöntési probléma:
$L = \{\langle I \rangle \mid I$ 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.

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

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

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

Tétel

Létezik nem Turing-felismerhető nyelv.

$$L_{\text{átló}} = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$$

Tétel

$L_{\text{átló}} \notin RE$.

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

Tétel

$L_u \in RE$

Tétel

$L_u \notin R$.

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 $L \in R$.

Következmény

RE nem zárt a komplementer-képzésre.

Tétel

R zárt a komplementer-képzésre

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 $w \in L_1 \Leftrightarrow f(w) \in L_2$. 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 $L_2 \notin R$.

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 $L_1 \in R$.

Megállási probléma:
$L_h = \{\langle M, w\rangle \mid M \text{ megáll a } w \text{ bemeneten}\}$.

$$L_u \subseteq L_h$$

Tétel

$L_h \notin R$.

Tétel

$L_h \in RE$.

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

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 $d_i = \frac{u_i}{v_i}$ $(1 \leq i \leq n)$.
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 $u_{i_1} \cdots u_{i_m} = v_{i_1} \cdots v_{i_m}$.

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

Tétel

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

Tétel

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

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

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

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
- $L(G_1) = L(G_2)$
- $L(G_1) \subseteq L(G_2)$

Tétel

Eldönthetetlen, hogy A elsőrendű logikai formulára

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

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

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.

Bonyolultságelmélet

http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/10/EA10SZ2.pdf
http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/11/EA11SZ2.pdf
http://web.cs.elte.hu/~tichlerk/logikaesszamitaselmelet/12/EA12SZ2.pdf

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

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 $w \in L_1 \iff f(w) \in L_2$. 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.

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.

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 $L' \leq_p L$.

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

Tétel (Cook)

SAT NP-teljes.

Tétel

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

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

Tétel

3SAT NP-teljes.

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

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

Tétel

3Színezés NP-teljes.

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

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

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**.

LEFOGÓ PONTHALMAZ=$\{\langle G, k\rangle \mid G$-nek van k 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 ($k \leq |V(G)|$).

Tétel

KLIKK, FÜGGETLEN PONTHALMAZ, LEFOGÓ PONTHALMAZ NP-teljes.

$\mathcal{S}$ egy **hipergráf** (vagy halmazrendszer), ha $\mathcal{S} = \{A_1, \ldots, A_n\}$, 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=$\{\langle \mathcal{S}, k\rangle \mid \mathcal{S}$ egy hipergráf és $\mathcal{S}$-hez van k elemű lefogó ponthalmaz$\}$.

Tétel

HIPERGRÁF LEFOGÓ PONTHALMAZ NP-teljes.

Hamilton út/kör

Adott egy $G = (V, E)$ irányítatlan / irányított gráf ($|V| = n$). Egy $P = v_{i_1}, \ldots, v_{i_n}$ felsorolása a csúcsoknak **Hamilton út** G-ben, ha $\{v_{i_1}, \ldots, v_{i_n}\} = V$ és minden $1 \le k \le n-1$-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**.

Jelölés: H-út/ H-kör Hamilton út/ Hamilton kör helyett.

HÚ=$\{\langle G, s, t\rangle \mid$ van a G irányított gráfban s-ből t-be H-út$\}$.

IHÚ=$\{\langle G, s, t\rangle \mid$ van a G irányítatlan gráfban s-ből t-be H-út$\}$.

IHK=$\{\langle G\rangle \mid$ van a G irányítatlan gráfban H-kör$\}$.

Tétel

HÚ NP-teljes

Tétel

IHÚ NP-teljes

Tétel

IHK NP-teljes

TSP=$\{\langle G, K\rangle \mid G$-ben van $\le K$ súlyú H-kör$\}$.

Tétel

TSP NP-teljes

NP-köztes nyelv

L NP-köztes, ha $L \in$ NP, $L \notin$ P és L nem NP-teljes.

Ladner tétele

Ha P $\neq$ NP, akkor létezik NP-köztes nyelv.

co$\mathfrak{C}$ bonyolultsági osztály

Ha $\mathfrak{C}$ egy bonyolultsági osztály 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 $L_1 \in \mathfrak{C}$.

Tétel

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

Következmény

coNP zárt a polinom idejű visszavezetésre nézve.

Tétel

L $\mathfrak{C}$-teljes $\Longleftrightarrow$ $\overline{L}$ co$\mathfrak{C}$-teljes.

UNSAT := $\{\langle\varphi\rangle \mid \varphi$ kielégíthetetlen nulladrendű formula$\}$.

TAUT := $\{\langle\varphi\rangle \mid$ a φ nulladrendű formula tautológia$\}$.

Tétel

UNSAT és TAUT coNP-teljesek.

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 tárigénye

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

Így az off-line TG-pel **szublineáris** (lineáris alatti) tárbonyolultságot is mérhetünk.

- $\text{SPACE}(f(n)) := \{L \mid L$ eldönthető $O(f(n))$ tárkorlátos determinisztikus off-line TG-pel$\}$
- $\text{NSPACE}(f(n)) := \{L \mid L$ eldönthető $O(f(n))$ tárkorlátos nemdeterminisztikus off-line TG-pel$\}$
- $\text{PSPACE}:=\bigcup_{k\geq 1}\text{SPACE}(n^k)$.
- $\text{NPSPACE}:=\bigcup_{k\geq 1}\text{NSPACE}(n^k)$.
- $\text{L}:=\text{SPACE}(\log n)$.
- $\text{NL}:=\text{NSPACE}(\log n)$.

ELÉR$=\{\langle G, s, t\rangle \mid$ 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 $\in \text{SPACE}(\log^2 n)$.

Az 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 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 ELÉR $\in$ P vagy ELÉR $\in \text{SPACE}(\log^2 n)$ tételeket alkalmazva a konfigurációs gráfra, vagy annak egy részgráfjára.

Savitch tétele

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

Következmény

PSPACE = NPSPACE

Tétel

NL$\subseteq$ P

Tétel

ELÉR $\in$ NL

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 $L' \in$NL nyelvre, $L' \leq_\ell L$; ha ráadásul $L \in$NL is teljesül, akkor L **NL-teljes** (a log. táras visszavezetésre nézve)

Tétel

L zárt a logaritmikus tárral való visszavezetésre nézve

Következmény

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

Tétel

ELÉR NL-teljes a logaritmikus tárral történő visszavezetésre nézve.

Immerman-Szelepcsényi tétel

NL = coNL

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

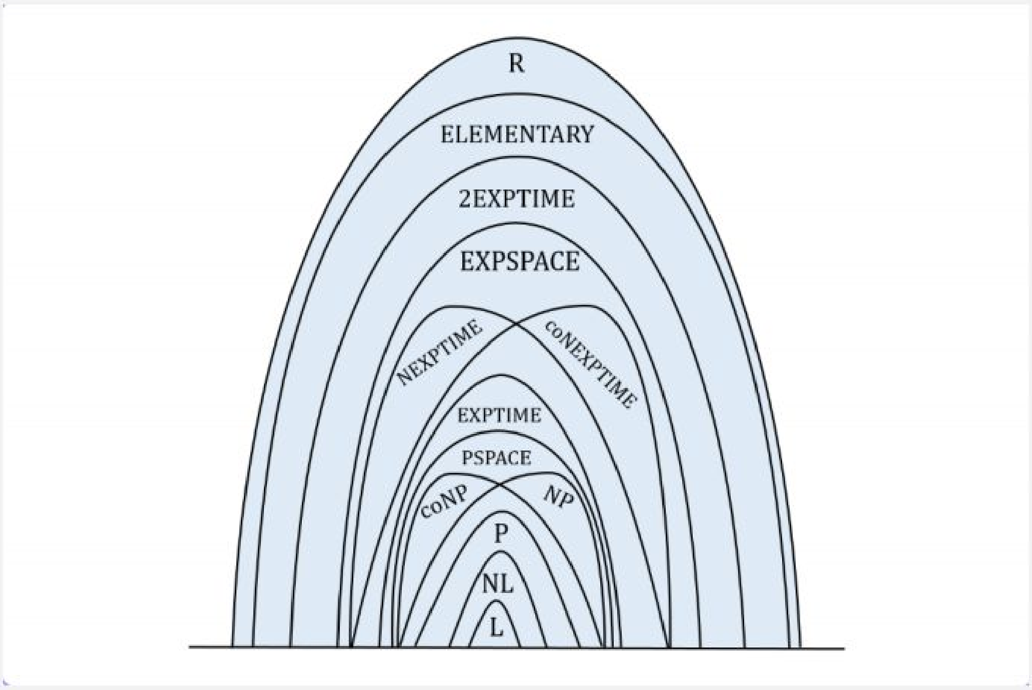
Tétel

NL$\subset$PSPACE és P$\subset$EXPTIME.

Tétel

L$\subseteq$NL=coNL$\subseteq$P$\subseteq$NP$\subseteq$PSPACE$\subseteq$EXPTIME

R szerkezete



R szerkezete P≠NP esetén [ábra: Gazdag Zs. jegyzet]