Bevezetés a számításelméletbe

8. előadás

Nemdeterminisztikus Turing gép

Jelölés: $\mathcal{P}(X) = \{Y \mid Y \subseteq X\}$ az X halmaz hatványhalmaza.

Nemdeterminisztikus Turing gép (NTG)

Az egyszalagos **nemdeterminisztikus Turing gép** (továbbiakban röviden NTG) 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 $\sqcup \in \Gamma \setminus \Sigma$,
- $\delta : (Q \setminus \{q_i, q_n\}) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, S, R\})$.

Azaz míg a **determinisztikus** esetben a δ átmenetfüggvény minden egyes $(Q \setminus \{q_i, q_n\}) \times \Gamma$-beli párhoz **pontosan egy**, addig egy **nemdeterminisztikus** TG **akárhány** (pl. 0,1,5,100) darab $Q \times \Gamma \times \{L, S, R\}$-beli rendezett hármast rendelhet hozzá.

NTG egylépéses konfigurációátmenete

A **konfiguráció** fogalma azonos, jelölje most is C_M az M NTG lehetséges konfigurációinak halmazát.

Definíció

Egy $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ egyszalagos nemdeterminisztikus Turing gép $\vdash \subseteq C_M \times C_M$ **egylépéses konfigurációátmenet** relációját az alábbiak szerint definiáljuk.

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 $c = \sqcup$.

Példa: Tegyük fel, hogy $\delta(q_2, a) = \{(q_5, b, L), (q_1, d, R)\}$ Legyen továbbá $C_1 = bcq_2a\sqcup b$, $C_2 = bq_5cb\sqcup b$, $C_3 = bcdq_1\sqcup b$. Ekkor $C_1 \vdash C_2$ és $C_1 \vdash C_3$.

Nemdeterminisztikus Turing gép

Vegyük észre, hogy míg a **determinisztikus** esetben minden nem-megállási C konfigurációhoz **pontosan egy** C' konfiguráció létezett, melyre $C \vdash C'$, addig a **nemdeterminisztikus** esetben **több** ilyen is létezhet. Pl. 0,1,5,100 darab. Persze csak véges sok, hiszen $|Q \times \Gamma \times \{L, S, R\}|$ véges!

Többlépéses konfigurációátmenet: $\vdash$ reflexív, tranzitív lezártja, azaz:

Definíció

A $\vdash^* \subseteq C_M \times C_M$ **többlépéses konfigurációátmenet** relációját a következőképpen definiáljuk: $C \vdash^* C' \Leftrightarrow$

- 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 $C_n = C'$.

Példa: Tegyük fel, hogy $C_1 \vdash C_2$, $C_1 \vdash C_3$, $C_2 \vdash C_4$. Ekkor $C_1 \vdash^* C_1$, $C_1 \vdash^* C_2$, $C_1 \vdash^* C_3$ és $C_1 \vdash^* C_4$ is teljesül.

Nemdeterminisztikus Turing gép

Definíció

Az $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ nemdeterminisztikus Turing gép által **felismert nyelv**
$L(M) = \left\{ u \in \Sigma^* \mid q_0 u \sqcup \vdash^* x q_i y \text{ valamely } x, y \in \Gamma^*, y \neq \varepsilon \text{ -ra} \right\}$.

Bár a definíció formálisan megegyezik a determinisztikus TG által felismert nyelv definíciójával az egylépéses átmenet fogalmának módosulása miatt újra érdemes átgondolni mit jelent ez.

Determinisztikus esetben csupán egyetlen számítása létezik a gépnek adott kezdőkonfigurációból, így ha elfogadó konfigurációba jut, akkor nincs elutasító konfigurációba jutó számítása és viszont.

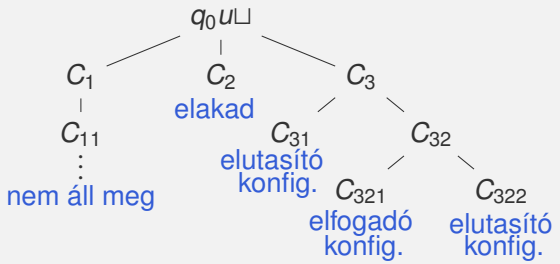
Egy NTG-nek azonban **több számítása is lehet ugyanarra a szóra**. Ezek között lehetnek elfogadó és elutasító (sőt nem terminálló!) számítások is. Egy NTG akkor fogad el egy szót, ha az adott szóra **legalább egy számítása q_i-ben ér véget** (hiszen ekkor a kezdőkonfiguráció és ez az elfogadó konfiguráció $\vdash^*$ relációban áll).

Nemdeterminisztikus számítási fa

Definíció

Egy M TG egy $u \in \Sigma^*$ inputjához tartozó **nemdeterminisztikus számítási fa** egy gyökeres fa, melynek csúcsai M konfigurációival 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.

Példa:



Tehát M elfogadja u-t, hiszen a $q_0 u \sqcup \vdash C_3 \vdash C_{32} \vdash C_{321}$ számítása elfogadó konfigurációba visz. **Egyetlen** elfogadó számítás is elég!

Nemdeterminisztikus számítási fa

Tehát adott inputra több számítás is lehetséges, ezek lehetnek elfogadóak, elutasítóak, **elakadóak** (ha olyan C-be jut, melyre $\{C' \mid C \vdash C'\} = \emptyset$), illetve végtelenek.

Észrevétel: $u \in L(M) \Leftrightarrow$ az u-hoz tartozó nemdeterminisztikus számítási fának van olyan levele, ami elfogadó konfiguráció.

Megjegyzés: a nemdeterminisztikus Turing gép definíciója értelemszerűen kiterjeszthető k-szalagos gépekre is, így beszélhetünk k-szalagos nemdeterminisztikus Turing gépekről is.

NTG-vel való eldönthetőség, időigény

Definíció

Az M NTG **felismeri** az $L \subseteq \Sigma^*$ nyelvet, ha $L(M) = L$.

Az M NTG **eldönti** az $L \subseteq \Sigma^*$ nyelvet, ha felismeri továbbá minden $u \in \Sigma^*$ input szóhoz tartozó nemdeterminisztikus számítási fa véges és a fa minden levele elfogadó vagy elutasító konfiguráció.

Definíció

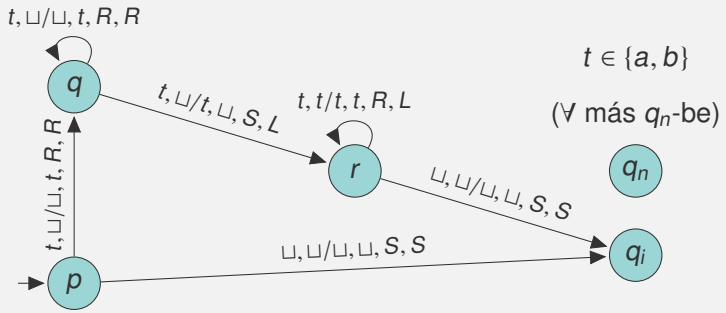
Az M NTG **$f(n)$ időkorlátos** (időigényű), ha minden $u \in \Sigma^*$ n hosszú szóra u számítási fája legfeljebb $f(n)$ magas.

Tehát, ha M $f(n)$ időkorlátos, akkor nincs végtelen számítása és minden n-re a legfeljebb n méretű bemeneteken a számításai (nemcsak az elfogadó, hanem az elutasító és elakadó számításai is) legfeljebb $f(n)$ lépésben véget érnek.

Nemdeterminisztikus Turing gép

Példa

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



$(p, \varepsilon, abba, \varepsilon, \sqcup) \vdash (q, \varepsilon, bba, a, \sqcup) \vdash (r, \varepsilon, bba, \varepsilon, a) \vdash (q_n, \varepsilon, bba, \varepsilon, a)$

$(p, \varepsilon, abba, \varepsilon, \sqcup) \vdash (q, \varepsilon, bba, a, \sqcup) \vdash (q, \varepsilon, ba, ab, \sqcup) \vdash (r, \varepsilon, ba, a, b) \vdash (r, b, a, \varepsilon, ab) \vdash (r, ba, \sqcup, \varepsilon, \sqcup ab) \vdash (q_i, ba, \sqcup, \varepsilon, \sqcup ab)$

Hosszlexikografikus rendezés

Definíció

Legyen $X = \{x_1 \prec x_2 \prec \cdots \prec x_s\}$ egy rendezett ábécé. Ekkor X^* szavainak **hossz-lexikografikus** (shortlex) rendezése alatt azt a $\prec_{\text{shortlex}}$ rendezést értjük, melyre a következők teljesülnek. Minden $u_1 \cdots u_n, v_1 \cdots v_m \in X^*$-ra $u_1 \cdots u_n \prec_{\text{shortlex}} v_1 \cdots v_m \Leftrightarrow (n < m) \vee ((n = m) \wedge (u_k < v_k)$, ahol k a legkisebb olyan i, melyre $u_i \neq v_i$).

1. Példa: Ha $X = \{a, b\}$ és $a \prec b$, akkor X^* szavainak hossz-lexikografikus sorrendje:

$\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, \ldots$

2. Példa: Tekintsük a természetes számokat (azaz 0 számjeggyel nem kezdődhetnek, a 0 kivételével), mint számjegysorozatokat.

Ekkor $n < m$ pontosan akkor igaz, ha az $X = \{0,1,2,3,4,5,6,7,8,9\}$ rendezett ábécé feletti szavaknak tekintve őket $n \prec_{\text{shortlex}} m$ teljesül.

Nemdeterminisztikus Turing gép

Szimulálás determinisztikus TG-pel

Tétel

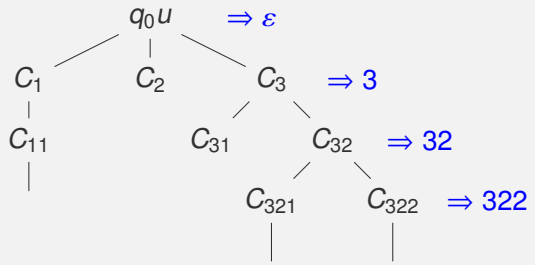
Minden $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n \rangle$ $f(n)$ időkorlátos NTG-hez megadható egy ekvivalens, $2^{O(f(n))}$ időkorlátos M' determinisztikus TG.

Bizonyítás (vázlat): Ötlet: Vegyük észre, hogy minden $u \in \Sigma^*$-ra u számítási fájának csúcsai éppen u parciális (nem feltétlen befejezett) számításainak felelnek meg. M' egy adott $u \in \Sigma^*$ bemeneten tehát szimulálni tudja u M-beli összes parciális számítását a számítási fájának szélességi bejárása által.

- Legyen d az M átmenetfüggvényének jobb oldalán szereplő halmazok számosságának a maximuma, azaz $d = \max_{(q,a) \in Q \times T} |\delta(q,a)|$.
- Legyen $T = \{1, 2, \ldots, d\}$ egy (rendezett) ábécé.
- minden $(q,a) \in Q \times \Gamma$ esetén rögzítsük le $\delta(q,a)$ elemeinek egy sorrendjét

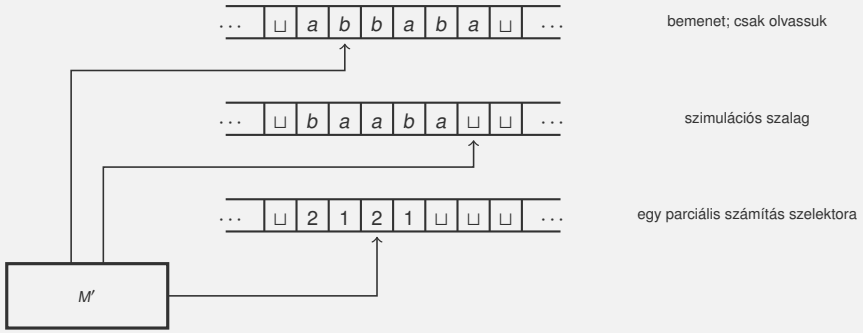
NTG szimulálása determinisztikus TG-pel

A számítási fa minden csúcsához egyértelműen hozzárendelhető egy T^*-beli szó, az adott konfigurációhoz tartozó parciális számítás (konfigurációátmenet-sorozat) ún. *szelektora*.



A gyökér szelektora ε. Tekintsük a gyökértől egy x csúcsig vezető egyértelmű utat, ha a szülő konfigurációnak x az i-edik gyereke és a szülő szelektora $w \in T^*$, akkor x szelektora $wi \in T^*$.

NTG szimulálása determinisztikus TG-pel



M' működése:

NTG szimulálása determinisztikus TG-pel

- M' kezdőkonfigurációja: az 1-es szalag tartalmazza a bemenetet, a 2-es és 3-as szalagok üresek.
- Amíg nincs elfogadás
  - M' rámásolja az 1-es szalag tartalmát a 2-esre
  - Amíg a 3-ik szalagon a fej nem $\sqcup$-re mutat
    - Legyen k a 3-ik szalagon a fej pozíciójában lévő betű
    - Legyen a 2-ik szalagon a fej pozíciójában lévő betű a és a szimulált M aktuális állapota q
    - Ha $\delta(q, a)$-nak van k-ik eleme, akkor
      - M' szimulálja M egy lépését ezen elem szerint
      - Ha ez q_i -be vezet, akkor M' is elfogad
      - Ha ez q_n-be vezet, akkor M' kilép ebből a ciklusból
    - M' a 3-ik szalagon eggyel jobbra lép
  - M' törli a 2. szalagot és előállítja a 3. szalagon a hossz-lexikografikus (shortlex) rendezés szerinti következő szót T felett (a fejet a szó elejére állítva)

NTG szimulálása determinisztikus TG-pel

- M' akkor és csak akkor lép elfogadó állapotba, ha a szimulált M elfogadó állapotba lép, azaz a két gép ekvivalens
- M'-nek $f(n)$-ben exponenciálisan sok számítást kell megvizsgálnia ($\leq$ egy $f(n)$ magasságú teljes d-áris fa belső csúcsainak száma darabot, ami $O(d^{f(n)})$). Mivel minden számítás legfeljebb $f(n)$ lépésből áll, így M' $f(n)O(d^{f(n)}) = 2^{O(f(n))}$ időkorlátos.

Megjegyzés:

- Abból, hogy a bizonyításban alkalmazott szimuláció exponenciális időigényű még nem következik, hogy nincs hatékonyabb szimuláció.
- Az a *sejtés*, hogy nem lehet a nemdeterminisztikus Turing gépet az időigény drasztikus romlása nélkül determinisztikus Turing géppel szimulálni.

Számosság

A véges halmazok fontos tulajdonsága a méretük ($\rightarrow$ **természetes számok** fogalma). Cél: ennek kiterjesztése végtelen halmazokra. Ez vezetett a **számosság** fogalmához*(G. Cantor, 1845-1918)*.

Definíció

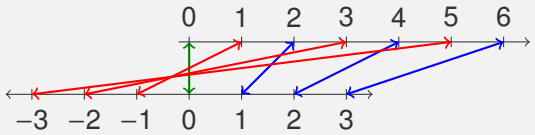
- A és B halmazoknak **megegyezik a számosságuk**, ha $\exists$ bijekció köztük. Jelölése: $|A| = |B|$.
- A-nak **legalább annyi a számossága**, mint B-nek, ha $\exists$ B-ből injekció A-ba. Jelölése: $|A| \geq |B|$.
- A-nak **nagyobb a számossága, mint B-nek**, ha $\exists$ B-ből A-ba injekció, de $\nexists$ bijeckió. Jelölése: $|A| > |B|$.

Cantor-Bernstein-Schröder tétel

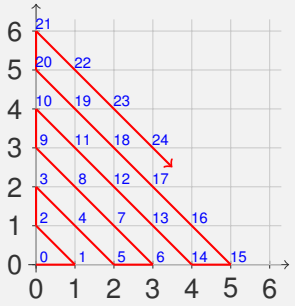
Ha $\exists$ injekció A-ból B-be és B-ből A-ba is, akkor $\exists$ bijekció A és B között, azaz ha $|A| \leq |B|$ és $|A| \geq |B|$, akkor $|A| = |B|$.

Számosság – példák

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



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



A megszámlálhatóan végtelen számosság

3. példa: $|\mathbb{N}| = |\mathbb{Q}|$.

Bizonyítás:
$\mathbb{N} \subset \mathbb{Q}$, ezért $|\mathbb{N}| \leq |\mathbb{Q}|$.

$\mathbb{Q}^+ := \{\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+, \text{a tört nem egyszerűsíthető}\}$.
$\mathbb{Q}^- := \{-\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+, \text{a tört nem egyszerűsíthető}\}$.
$\frac{p}{q} \in \mathbb{Q}^+ \mapsto (p, q) \in \mathbb{N} \times \mathbb{N}$ 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
$\mathbb{Q} = \{0, a_1, b_1, a_2, b_2, \ldots\}$.

Definíció

Egy A halmaz **megszámlálhatóan végtelen számosságú**, ha létezik A és $\mathbb{N}$ között bijekció.

Azaz egy A halmaz számossága megszámlálhatóan végtelen, ha elemei megindexelhetők a természetes számokkal.

A continuum számosság

Egy halmaz **megszámlálható**, ha számossága véges vagy megszámlálhatóan végtelen.

Tétel: Megszámlálható sok megszámlálható halmaz uniója megszámlálható.
Bizonyítás (vázlat) Konstrukció: mint $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ bizonyításánál.

Definíció

Egy A halmaz **continuum számosságú**, ha létezik A és $\mathbb{R}$ között bijekció.

Be fogjuk látni, hogy $|\mathbb{R}| > |\mathbb{N}|$.

4. példa: $|\mathbb{R}| = |(0, 1)|$.

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

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

Szavakkal kapcsolatos halmazok számossága

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

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

Jelöljük a megszámlálhatóan ∞ hosszúságú $\{0, 1\}$-sorozatok halmazát $\{0, 1\}^{\mathbb{N}}$-nel, azaz

$\{0, 1\}^{\mathbb{N}} := \{(b_1, \ldots, b_i, \ldots) \mid b_i \in \{0, 1\},\ i \in \mathbb{N}\}$.

6. Példa: $\left|\left\{L \mid L \subseteq \{0, 1\}^*\right\}\right| = \left|\{0, 1\}^{\mathbb{N}}\right|$

Bizonyítás: Jelölje w_i $\{0, 1\}^*$ hossz-lexikografikus rendezésének i. szavát $(i \in \mathbb{N})$.

Egy L nyelvhez rendeljük hozzá azt a megszámlálhatóan végtelen hosszúságú $\mathbf{b}_L = (b_1, \ldots, b_i, \ldots)$ bitsorozatot, amelyre $b_i = 1 \Leftrightarrow w_i \in L$.

Ez nyilván bijekció, $\mathbf{b}_L$-t nevezhetjük is az L nyelv **karakterisztikus sorozatának**.

Szavakkal kapcsolatos halmazok számossága

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

Bizonyítás (vázlat):

Minden $x \in [0,1)$-hez rendeljük hozzá x kettedestört alakjának "0." utáni részét. Ez nem feltétlen egyértelmű, hiszen a véges kettedestörteknek két végtelen kettedestört alakja is van. (Például 0,01=0,0100...=0,0011...)

Válasszuk ilyenkor a ∞ 0-ra végződő alakot. Ez a leképezés így nem bijekció, de injektív, azaz $|[0,1)| \leq |\{0,1\}^{\mathbb{N}}|$.

Fordítva, $\mathbf{z} \in \{0,1\}^{\mathbb{N}}$ minden 1-esét helyettesítsük 2-essel, írjunk elé "0."-t és tekintsük végtelen harmadostörtnek. Meggondolható, hogy csak 0-ásokat és 2-eseket tartalmazó harmadostört alakja egy valós számnak legfeljebb 1 lehet (azaz a véges harmadostörtek két alakja közül legaláb az egyik tartalmaz 1-est). Tehát $|\{0,1\}^{\mathbb{N}}| \leq |[0,1)|$.

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

Megszámlálhatóan végtelen vs continuum számosság

Tétel

$|\mathbb{R}| > |\mathbb{N}|$

Bizonyítás:

Mivel $|\{0,1\}^{\mathbb{N}}| = |\mathbb{R}|$, ezért elég belátni, hogy $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$.

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

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

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

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

Indirekt tegyük fel, hogy bijekcióba lehet állítani $\{0,1\}^{\mathbb{N}}$ elemeit $\mathbb{N}$ elemeivel, azaz $\{0,1\}^{\mathbb{N}} = \{u_i \mid i \in \mathbb{N}\} = \{u_1, u_2, \ldots\}$ a $\{0,1\}^{\mathbb{N}}$ elemeinek egy felsorolása (a természetes számokkal való megindexelése).

A Cantor-féle átlós módszer

Jelölje $u_{i,j}$ u_i j. bitjét ($i,j \in \mathbb{N}, u_{i,j} \in \{0,1\}$), azaz

$$u_i = (u_{i,1}, u_{i,2}, \ldots, u_{i,j}, \ldots).$$

Tekintsük az $u = \{\overline{u_{1,1}}, \overline{u_{2,2}}, \ldots, \overline{u_{i,i}}, \ldots)$ 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 egy bit nem lehet 0 és 1 is egyszerre, tehát az indirekt feltevésünk, azaz hogy $\{0,1\}^{\mathbb{N}}$ és $\mathbb{N}$ között $\exists$ bijekció helytelen volt.

Megjegyzés: A bizonyítás módszerét **Cantor-féle átlós módszernek** nevezik.

Túl sok a nyelv

Következmény

A $\{0,1\}$ feletti nyelvek halmazának számossága nagyobb, mint a $\{0,1\}$ feletti szavak számossága.

Ezekhez csak foglaljuk össze amit tudunk:
$|\mathbb{R}| = |[0,1)| = |\{0,1\}^{\mathbb{N}}| = \left|\left\{L \mid L \subseteq \{0,1\}^*\right\}\right| > |\mathbb{N}| = |\{0,1\}^*|$.

Észrevétel: $\left\{L \mid L \subseteq \{0,1\}^*\right\} = \mathcal{P}(\{0,1\}^*)$.

Igaz-e általában, hogy $|\mathcal{P}(H)| > |H|$?

Hatványhalmaz számossága

Tétel

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

Bizonyítás: [Cantor-féle átlós módszerrel]

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

$|\mathcal{P}(H)| \neq |H|$: Indirekt $\exists\, f : \mathcal{P}(H) \leftrightarrow H$ bijekció. Definiálunk egy $A \subseteq H$ halmazt: $\forall x \in H : \quad x :\in A \;\Leftrightarrow\; x \notin f^{-1}(x)$

$f(A) \in A$ igaz-e? Ha igaz, $f(A) \notin A$, ha nem igaz $f(A) \in A$ következik A definíciójából. Tehát $f(A) \in A$ se igaz, se hamis nem lehet, ellentmondás.

Következmény

Minden számosságnál van nagyobb számosság, tehát végtelen sok számosság van.

$\aleph_0 := |\mathbb{N}|, \aleph_1 := |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. Ha $|H| = \aleph_i$ akkor $\aleph_{i+1} := |\mathcal{P}(H)|$.

A Turing gépek egy elkódolása

Tegyük fel, hogy $\Sigma = \{0, 1\}$. Ez feltehető, mivel minden input hatékonyan kódolható Σ felett.

Definíció

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 $0^i 1 0^j 1 0^r 1 0^s 1 0^t$.
- $\langle M \rangle$ az átmenetek kódjainak felsorolása 11-el elválasztva.

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

Definíció

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

Létezik nem Turing-felismerhető nyelv

Tétel

Létezik nem Turing-felismerhető nyelv.

Bizonyítás: A TG-ek számossága megszámlálható (a fenti kódolás injekció $\{0,1\}^*$-ba, amiről tudjuk, hogy megszámlálható). Másrészt azt is tudjuk, hogy a $\{0,1\}$ feletti nyelvek számossága continuum. Tehát nem jut minden nyelvre őt felismerő TG (minden TG egyetlen nyelvet ismer fel).

Megjegyzés: Tehát valójában a nyelvek „többsége” $\notin$ RE. Tudnánk-e konkrét nyelvet mondani?

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)

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

Tétel

$L_{\text{átló}} := \{w_i \mid w_i \notin L(M_i)\} \notin RE$.

Bizonyítás: [Cantor-féle átlós módszerrel]

Tekintsük azt a mindkét dimenziójában megszámlálhatóan végtelen T bittáblázatot, melyre $T(i,j) = 1 \;\Leftrightarrow\; w_j \in L(M_i)$ $(i, j \geq 1)$.

Legyen $\mathbf{z} = (T(1,1), \ldots, T(i,i), \ldots)$ a T átlójában olvasható megszámlálhatóan végtelen hosszú bitsztring és $\bar{\mathbf{z}}$ a $\mathbf{z}$ bitenkénti komplementere. Ekkor:

- minden $i \geq 1$-re, T i-ik sora az $L(M_i)$ nyelv karakterisztikus sorozata
- $\bar{\mathbf{z}}$ az $L_{\text{átló}}$ karakterisztikus sorozata.
- Minden TG-pel felismerhető, azaz RE-beli nyelv karakterisztikus sorozata megegyezik T valamelyik sorával.
- $\bar{\mathbf{z}}$ különbözik T minden sorától.
- Tehát $L_{\text{átló}}$ 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 M TG minden bementére szimulálja annak működését.

Feltehető, hogy M egyszalagos.

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

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

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

4. szalag: segédszalag

Az univerzális TG

Felismerhetőség

U működése vázlatosan:

1. Megnézi, hogy a bemenetén szereplő szó első része kódol-e TG-t; ha nem $\Rightarrow$ elutasítja a bemenetet
2. ha igen $\Rightarrow$ felmásolja w-t a 2., q_0 kódját a 3. szalagra
3. Szimulálja M egy lépését:
   – Leolvassa a második szalagról M aktuálisan olvasott szalagszimbólumát.
   – Leolvassa a harmadik szalagról M aktuális állapotát.
   – Szimulálja M egy lépését M első szalagon található leírása alapján. Ehhez U számára ehhez minden információ rendelkezésre áll. A 2. szalagon elő kell állítania az új szalagtartalmat a fej helyzetével és a 3. szalagon az új állapotot. Ehhez, ha szükséges használja a 4. szalagot. A megvalósítás átmenetszintű részletezésétől eltekintünk.
4. Ha M aktuális állapota elfogadó/elutasító, akkor U is belép a saját elfogadó/elutasító állapotába. Különben goto **3.**

Az univerzális TG

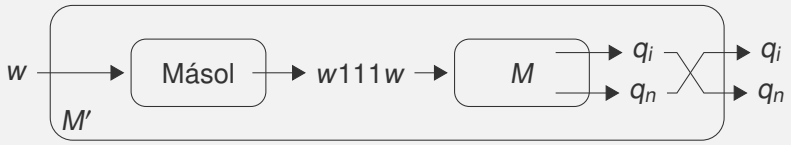
Eldönthetetlenség

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, csak felismeri.

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.

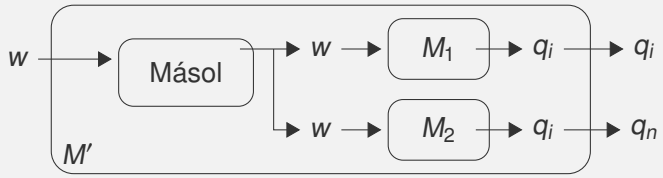
RE és R tulajdonságai

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

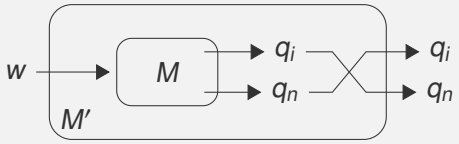
RE nem zárt a komplementer-képzésre.

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

Tétel

Ha $L \in R$, akkor $\overline{L} \in R$. (Azaz R zárt a komplementer-képzésre.)

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



Számítási feladatok megoldása TG-pel

Az eldöntési (igen/nem kimenetű) problémák általánosításai a (ki)számítási problémák. Ilyenkor a kimenet bármi lehet. A kiszámítási problémákra is algoritmikus megoldást keresünk.

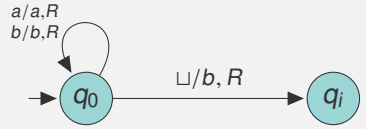
Feltehetjük (megfelelő kódolás alkalmazásával), hogy f értelmezési tartománya Σ^*, értékkészlete Δ^* valamely Σ, Δ ábécékre.

Definíció

Azt mondjuk, hogy az $M = \langle Q, \Sigma, \Delta, \delta, q_0, q_i, (q_n)\rangle$ 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: A definíció értelmében nincs szükség q_i és q_n megkülönböztetésére, elég lenne egyetlen megállási állapot. [Ezért van q_n ()-ben.]

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



Visszavezetés

Definíció

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

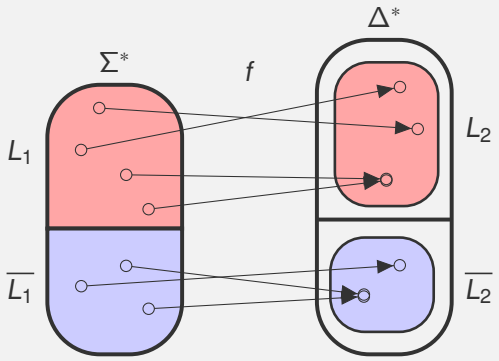
Definíció

$L_1 \subseteq \Sigma^*$ **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: $L_1 \leq L_2$

Megjegyzés: A fogalom Emil Posttól származik, angol nyelvű szakirodalomban: many-one reducibility

Visszavezetés

$L_1 \leq L_2$



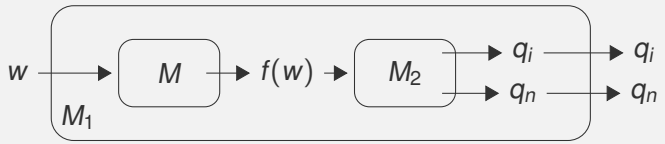
f kiszámítható, az egész Σ^*-on értelmezett, $f(L_1) \subseteq L_2$ valamint $f(\overline{L_1}) \subseteq \overline{L_2}$. f nem kell hogy injektív legyen és az se kell, hogy szürjektív.

Tétel

- 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 $L_1 \in R$.

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

Bizonyítás: Indirekt bizonyítással azonnal adódik a fenti tételből.

A Turing gépek megállási problémája

Megállási probléma: megáll-e M w-n?

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

Megjegyzés: más jegyzetekben L_{halt} néven is előfordulhat.

Észrevétel: $L_u \subseteq L_h$

Kérdés: 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

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.