Algoritmuselmélet 13. előadás

Katona Gyula Y.
Budapesti Műszaki és Gazdaságtudományi Egyetem
Számítástudományi Tsz.
I. B. 137/b
kiskat@cs.bme.hu

2002 Április 15.

Univerzális Turing gép

Turing-gép $\leftrightarrow$ program
Univerzális Turing-gép $\leftrightarrow$ fordító program (interperter)

M TG leírása és $s \in I^*$ bemenete $\Longrightarrow$ Univerzális TG $\Longrightarrow$ szimulálja M-et s bemenettel

Hogyan írjuk le az M TG-et?

Tegyük fel, hogy $k = 1$, $M = (Q, T, I, ü, \delta, q_0, F)$, $I = \{0, 1\}$ és $|F| = 1$. Pl.

- $I = \{0, 1\}, \quad T = \{0, 1, \ldots, t\}, \quad ü = t,$
- $Q = \{0, 1, \ldots, q\}, \quad q_0 = 0, \quad F = \{q\},$
- balra $= 0,$ jobbra $= 1,$ helyben $= 2$

Ekkor az M Turing-gép leírása, kódja $\Longrightarrow$

$$q\#t\#q_1\#x_1\#q'_1\#x'_1\#m'_1\#\ldots\#q_r\#x_r\#q'_r\#x'_r\#m'_r\#\#,$$

ahol a megfelelő számokat binárisan írjuk le, továbbá δ értékeit a következőképpen soroljuk fel (ahol értelmezett):

a $\delta(q_i, x_i) = (q'_i, x'_i, m'_i)$ tény kódja $q_i\#x_i\#q'_i\#x'_i\#m'_i$.

Minden szóba jövő M gépet egy $w \in I^*$ szóval írunk le.
Tetszőleges $w \in I^*$ szóhoz legfeljebb egy gép van, amelynek a kódja $w \Longrightarrow M_w$
Egymásból kiszámolható M és M_w.

Tétel. *Van olyan 3-szalagos U Turing-gép, amelyre teljesül a következő: ha $w, s \in I^*$, és M_w létezik, akkor az U gép a $w\#s$ bemenetet pontosan akkor fogadja el (utasítja el, kerül vele végtelen ciklusba), ha M_w az s bemenetet elfogadja (elutasítja, végtelen ciklusba kerül vele).*

Bizonyítás: (vázlat)
Első szalag $\Longrightarrow$ $w\#s$ input, w értelmezgetése
Második szalag $\Longrightarrow$ M_w egyetlen szalagjának felel meg.
Harmadik szalag $\Longrightarrow$ az M_w belső állapota

Előkészítés $\Longrightarrow$ ellenőrzi, hogy M_w létezik-e.
$\Longrightarrow$ NEM $\rightarrow$ megáll elutasító állapotban
$\Longrightarrow$ IGEN $\rightarrow$ átmásolja az s inputot a második szalagjára, és a harmadik szalagra a kezdőállapot kódját jegyzi fel.

$w\#s$
s
q_0

Az U az M_w gép egy lépését több lépésben szimulálja $\Longrightarrow$

$w\#s$
M_w szalagja az i-edik lépés után
M_w belső állapota az i-edik lépés után

U akkor áll meg, ha M_w megáll, pontosan akkor fogadja el a $w\#s$ bemenetét, ha a megállás után az M_w elfogadó állapotának kódja van az utolsó szalagon. ✓

Alapvető kiszámíthatatlansági tételek

Be fogjuk látni, hogy

$$\mathcal{R} \subsetneq \mathcal{RE} \subsetneq 2^{I^*}.$$

Definíció. *Azon gépek kódjainak L_d nyelve, amik nem fogadják el saját kódjukat a diagonális nyelv:*

$$L_d = \{w \in I^*;\ \text{az } M_w \text{ gép létezik, és } w \notin L_{M_w}\}.$$

Tétel. *L_d nem rekurzíve felsorolható.*

Bizonyítás: Indirekt, tegyük fel hogy rekurzíve felsorolható $\Longrightarrow \exists\ M$ TG amire $L_d = L_M$, ennek kódja legyen w

- $w \in L_d \Longrightarrow L_d$ definíciója szerint $w \notin L_{M_w} = L_d$ ↯
- $w \notin L_d \Longrightarrow L_d$ definíciója szerint $w \in L_d = L_{M_w}$ ↯

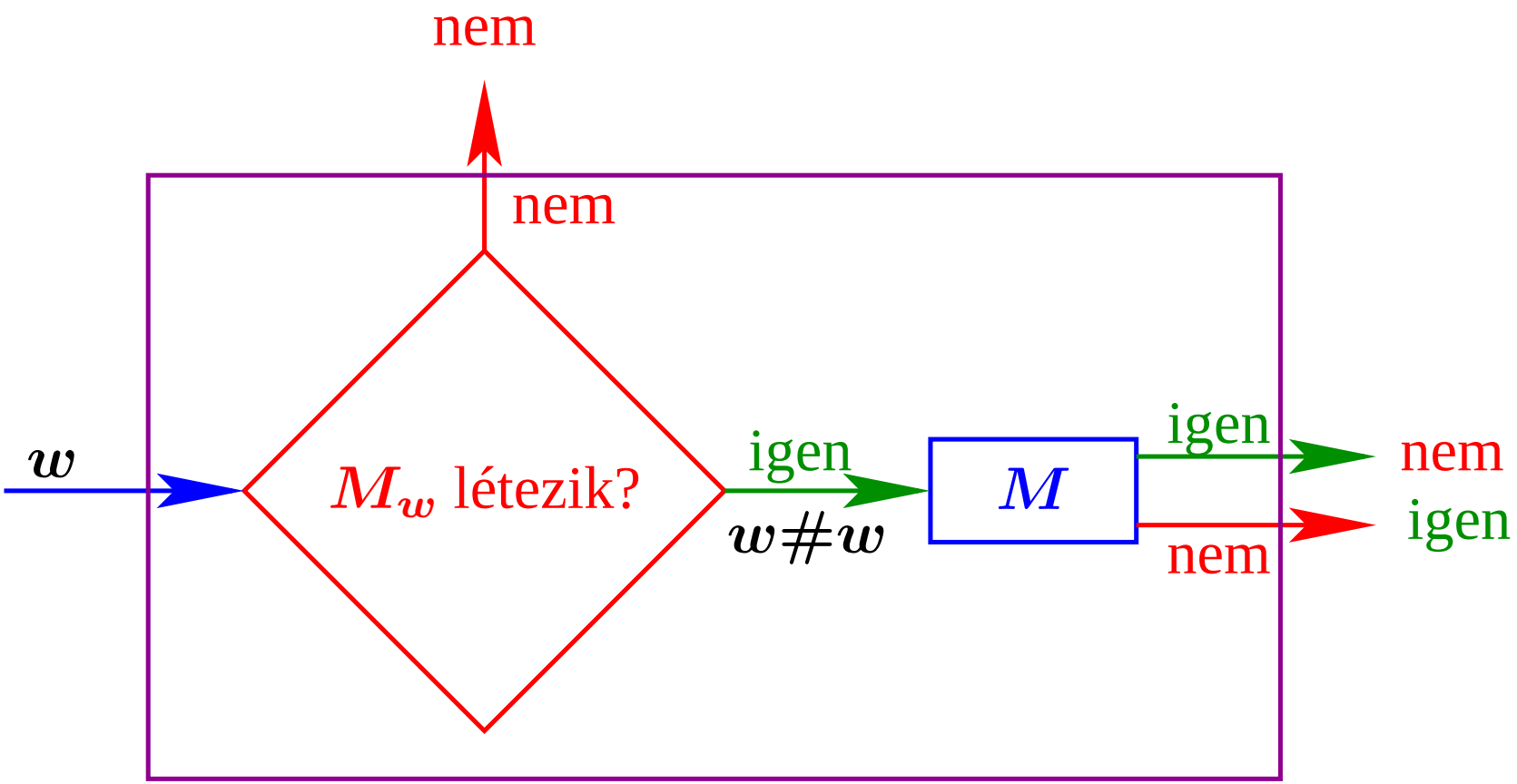
Az univerzális nyelv

Definíció. *Az olyan* (TG kód, input szó) *párok* L_u *nyelve, amelyekre a gép elfogadja az inputot az univerzális nyelv:*

$$L_u = \{w\#s \in I^*;\ \text{az } M_w \text{ gép létezik, és } s \in L_{M_w}\}.$$

Tétel. [A. Turing, 1936] L_u *egy rekurzíve felsorolható, de nem rekurzív nyelv.*

Bizonyítás: L_u-t éppen az univerzális Turing-gépek ismerik fel $\Longrightarrow L_u$ rekurzíve felsorolható.
Tegyük fel indirekt, hogy L_u rekurzív; legyen M egy mindig megálló TG, ami felismeri L_u-t.
Konstruáljuk meg az M' TG-et:



Az M' gép mindig megáll, mert M mindig megáll.
M' pontosan akkor fogadja el w-t, ha M_w létezik és $w \notin L_{M_w}$.
$\Longrightarrow$ M' éppen az L_d nyelvet fogadja el ↯
hiszen L_d nem rekurzíve felsorolható ✓

Összefüggések a kiszámíthatósági fogalmak között

Ha van egy mindig megálló M algoritmusunk L felismerésére, akkor van algoritmus az $I^* \setminus L$ nyelv felismerésére is.
Ha csak olyan „fél” algoritmusunk van, ami nem mindig áll meg, ezt nem lehet megtenni.
Ha van fél algoritmus L-re és $I^* \setminus L$-re is, akkor ebből összejön egy egész algoritmus
Definíció. *A nyelvekből álló halmazokat (2^{I^*} részhalmazait)* nyelvosztályoknak *nevezzük. (Pl. $\mathcal{R}$, $\mathcal{RE}$, 2^{I^*}.)*
Legyen $X \subseteq 2^{I^*}$ egy nyelvosztály. Ekkor a komplementer nyelvosztály, co$X$ *az X-beli nyelvek komplementereiből áll:*

$$\mathrm{co}X = \{L \subseteq I^* : \quad I^* \setminus L \in X\}.$$

$\Longrightarrow$

$$X \subseteq Y \subseteq 2^{I^*} \implies \mathrm{co}X \subseteq \mathrm{co}Y.$$

$$\mathrm{co}(\mathrm{co}X) = X$$

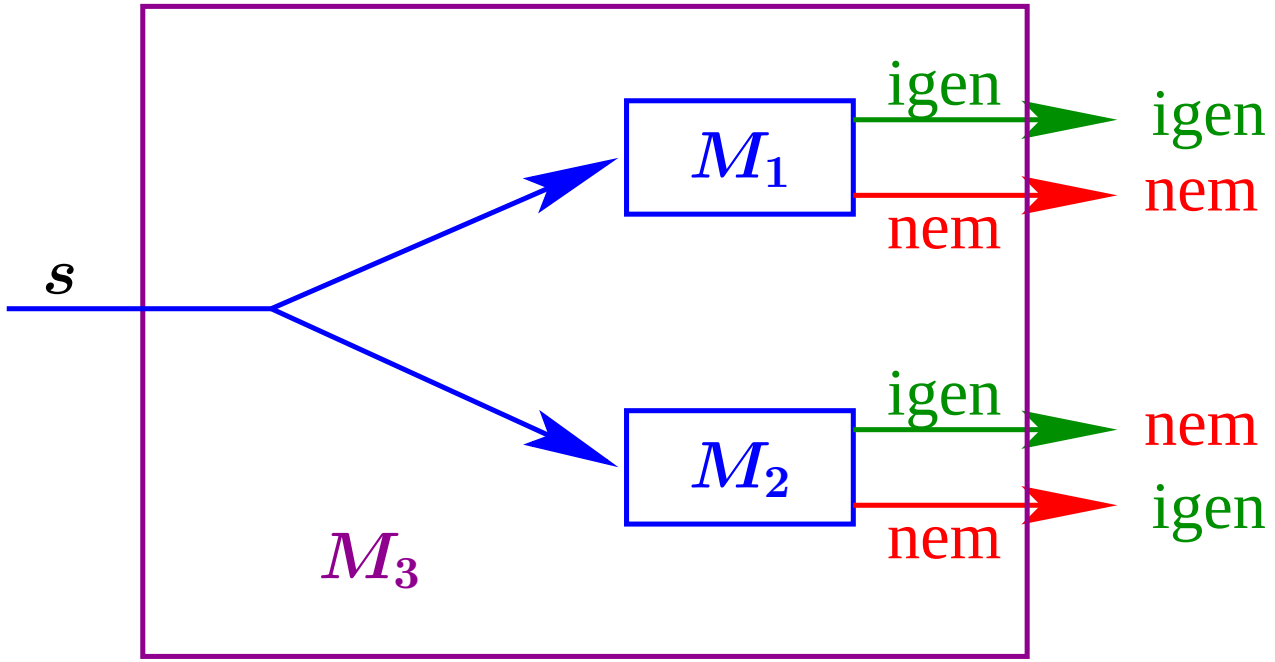
Tétel. $\mathcal{R} = co\mathcal{R}$

Bizonyítás: Ha $L \in \mathcal{R} \implies \exists\, M$ TG, mely minden inputon megáll és az L nyelvet fogadja el.
Cseréljük fel M elfogadó és elutasítva megálló állapotait $\implies$ co$\mathcal{R} \subseteq \mathcal{R}$. $\surd$
Másik irány:

$$\mathcal{R} = \text{co}(\text{co}\mathcal{R}) \subseteq \text{co}\mathcal{R}. \surd$$

Tétel. $\mathcal{R} = \mathcal{RE} \cap co\mathcal{RE}$

Bizonyítás: $\mathcal{R} \subseteq \mathcal{RE} \implies \mathcal{R} = \text{co}\mathcal{R} \subseteq \text{co}\mathcal{RE} \implies \mathcal{R} \subseteq \mathcal{RE} \cap \text{co}\mathcal{RE}$
Másik irány:
Tegyük fel, hogy $L \in \mathcal{RE} \cap \text{co}\mathcal{RE} \implies$ legyen M_1, illetve M_2 két TG, melyek az L, illetve az $I^* \setminus L$ nyelvet ismerik fel.
Egy mindig megálló M_3 TG-et szerkesztünk, melyre $L = L_{M_3}$:



Az M_3 pontosan akkor álljon meg, ha M_1 és M_2 valamelyike megáll.
M_3 akkor fogad el, ha a megállás M_1 elfogadó, vagy pedig M_2 elutasító állapotában történt.
$\Longrightarrow$ M_3 az L nyelvet ismeri fel és mindig megáll

M_3 megvalósítható párhuzamosság nélkül is $\Longrightarrow$ M_3 felváltva lépteti M_1-et és M_2-t. $\surd$

Függvények és halmazok

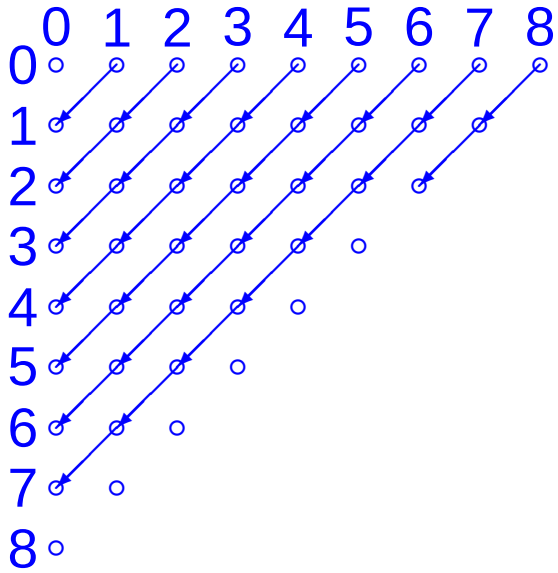
Tétel. *Az $L \subseteq I^*$ nyelv akkor és csak akkor rekurzíve felsorolható, ha van olyan $f : I^* \to I^*$ parciálisan rekurzív függvény, melynek értékkészlete éppen az L nyelv (szokásos jelöléssel $Im(f) = L$).*

Bizonyítás: $\Rightarrow$: Tegyük fel, hogy L rekurzíve felsorolható $\Longrightarrow \exists M$ TG, melyre $L = L_M$.
$\Longrightarrow$ Legyen M' olyan TG, mely kezdetben az $s \in I^*$ bemenő szót felmásolja az output szalagjára, azután szimulálja az M gépet.
Kivétel: $\Longrightarrow$ ha M elutasító állapotban áll meg, akkor M' végtelen ciklusba esik.
$\Longrightarrow$ M' gép csak az $s \in L$ szavakra áll meg; megálláskor s lesz az output szalagon. $\Longrightarrow$
Az M' által kiszámított $f_{M'}$ függvény értékkészlete L. $\surd$

$\Leftarrow$: Tegyük fel, hogy f egy parciálisan rekurzív függvény, $f = f_M$, ahol M egy TG.
Tekintsük az I^* szavainak $w_0, \ldots, w_n \ldots$ kanonikus felsorolását.
Ki kellene próbálni minden w_i inputtal, hogy hátha pont s-et a keresett szót számolja ki M.

Baj van, ha valamelyik szóra végtelen ciklusba kerül.

A természetes számokból álló párok is felsorolhatók:



Az M' TG az (i, j) párok sorozata szerint megy sorba. Tegyük fel, hogy $s \in I^*$ az M' bemenete.

$\Longrightarrow$ M' szimulálja az M első $\leq i$ lépését a w_j szón.

Ha M megáll és o outputot produkál, akkor ellenőrzi, hogy $s = o$ teljesül-e.

IGEN $\rightarrow$ M' megáll és elfogadja s-et.

NEM (nem áll meg i lépésen belül, vagy az eredmény nem s) $\Longrightarrow$ következő pár

Mi lesz az M' gép $L_{M'}$ nyelve?

$L_{M'} \subseteq \mathrm{Im}(f)$ ✓

Ha $s \in \mathrm{Im}(f) \implies \exists j$, hogy $s = f_M(w_j)$

$\implies$ ha M a w_j bemeneten i lépésben kapja meg az s eredményt $\implies M'$ az (i, j) pár feldolgozásakor elfogadja s-et

$\implies L_{M'} \supseteq \mathrm{Im}(f)$ ✓

Definíció. *Egy $L \subseteq I^*$ nyelv* karakterisztikus függvénye, χ_L *a következő:*

$$\chi_L(s) = \begin{cases} 1 \in I^*, & \text{ha } s \in L \\ 0 \in I^*, & \text{ha } s \notin L \end{cases}$$

Tétel. *Az $L \subseteq I^*$ nyelv pontosan akkor rekurzív, ha χ_L egy rekurzív függvény.*

Bizonyítás: $\Rightarrow$: M' írojon ki a végén 0-t vagy 1-et ✓

$\Leftarrow$: Ha 1-et ír ki $\longrightarrow$ menjen elfogadóba, ha 0-t $\longrightarrow$ elutasítóba ✓

Eldönthetetlen problémák

Definíció. *Az $L \subseteq I^*$ nyelvet* eldönthetetlen nyelvnek *nevezzük, ha L nem rekurzív.*

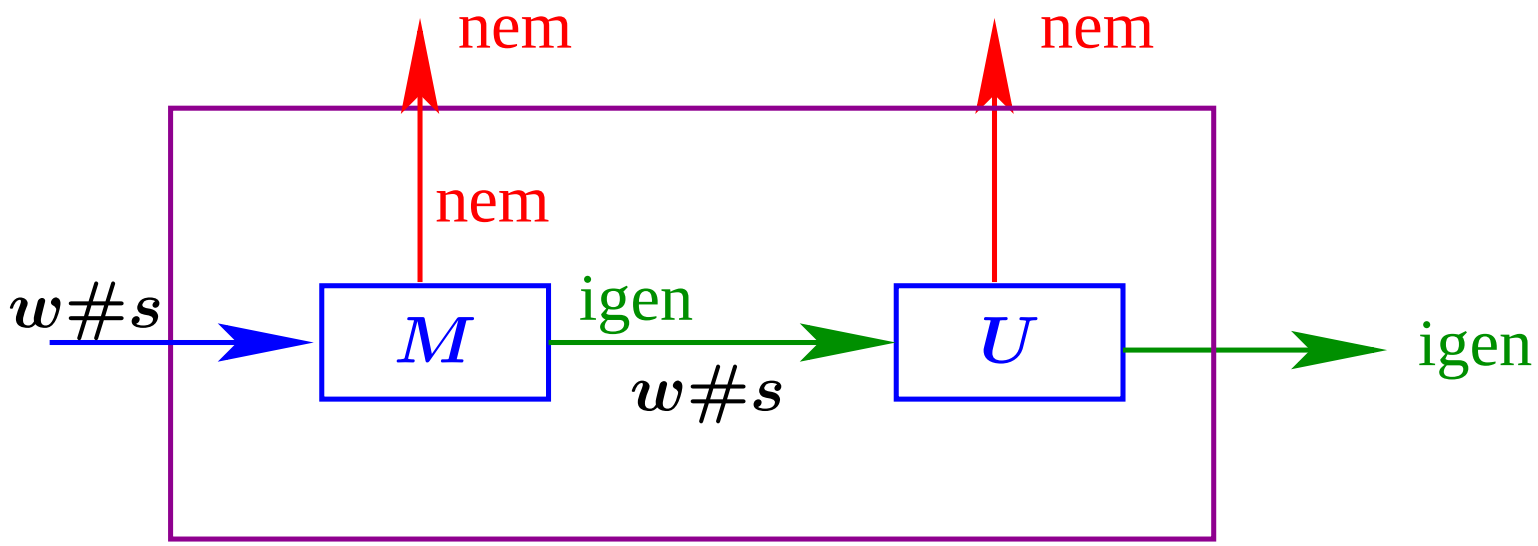
Definíció. Megállási probléma: *Megáll-e egy TG egy adott inputon?*

$$L_h = \left\{ w\#s \in I^* \;\middle|\; \begin{array}{l} \text{az } M_w \text{ gép létezik, és az } s \text{ bemenettel} \\ \text{elindítva véges sok lépésben megáll} \end{array} \right\}.$$

Tétel. $L_h \in \mathcal{RE} \setminus \mathcal{R}$.

Bizonyítás: $L_h \in \mathcal{RE}$: Vegyünk egy univerzális Turing-gépet, amit kicsit módosítunk: ha megáll menjen át elfogadóba

$L_h \notin \mathcal{R}$: Indikekt, tegyük fel, hogy rekurzív $\Longrightarrow \exists M$ TG, ami felismeri és mindig megáll.



Ez gép L_u-t felismeri és mindig megáll ↯

Tétel. [A. Church, 1936] *Legyen*

$$L_\epsilon = \{w \in I^* : \ M_w \textit{ létezik és az } \epsilon \textit{ (üres) inputon megáll}\}.$$

$$L_\epsilon \in \mathcal{RE} \setminus \mathcal{R}.$$

Bizonyítás: $L_\epsilon \in \mathcal{RE}$: Az üres inputtal futassuk az L_h-t felismerő gépet ✓

$L_\epsilon \notin \mathcal{R}$: Belátjuk, hogy ha L_ϵ rekurzív ($\exists M$, ami felismeri és mindig megáll), akkor L_h is.

Ha L_h bemenete $w\#s$, akkor olyan M'-t konstruálunk, aminek belső állapotaiba kódoljuk az s inputot. ✓

Hilbert 10. problémája

Legyen $f(x_1, \ldots, x_m)$ egész együtthatós m változós polinom:

$$f(x_1, \ldots, x_m) = \sum_{i_1=0}^{n_1} \cdots \sum_{i_m=0}^{n_m} a_{i_1 \ldots i_m} {x_1}^{i_1} \cdots {x_m}^{i_m}$$

Az f polinom *foka* az előző felírásban előforduló legnagyobb kitevőösszeg:

$$\deg f = \max\{i_1 + \ldots + i_m \mid a_{i_1 \ldots i_m} \neq 0\}.$$

Az

$$(*) \qquad f(x_1, \ldots, x_m) = 0$$

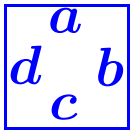
alakú egyenleteket *diofantikus egyenleteknek* nevezzük.
A $(*)$ diofantikus egyenlet *megoldásán* egy olyan $(u_1, \ldots, u_m) \in \mathbb{Z}^m$ egészekből álló m-est értünk, melyre $f(u_1, \ldots, u_m) = 0$.

Van-e megoldása egy adott diofantoszi egyenletnek?

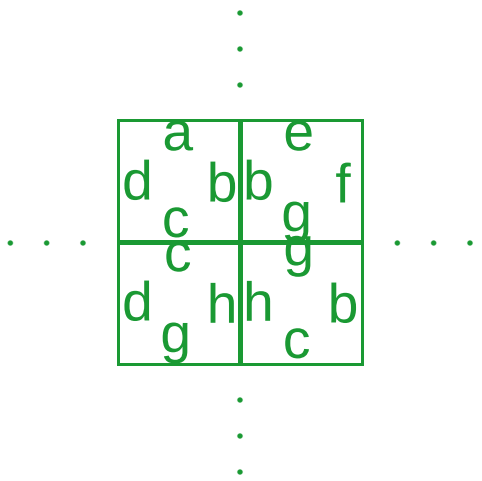
Tétel. [Matijaszevics, 1970] *Ez eldönthetetlen probléma.*

A Dominóprobléma

Dominó:



Egymásmellé rakás:



Forgatni nem szabad!

Dominóprobléma: *Adott dominó-típusok egy véges $\mathcal{F}$ halmaza; eldöntendő, hogy a sík lefedhető-e hézagtalanul szabályosan illeszkedő $\mathcal{F}$-beli típusú dominókkal.* $\Longrightarrow$ D nyelv

Tétel. $D \notin \mathcal{R}$ *és* $D \in co\mathcal{RE}$.

Post megfeleltetési problémája

Emil Post

Legyen Σ egy véges abc. *Post megfeleltetési problémájának* egy bemenete egy (s,t) $(s,t \in \Sigma^*)$ alakú rendezett párokból álló véges $\mathcal{P}$ halmaz.
A megfeleltetési feladat $\mathcal{P}$ bemenetét *megoldhatónak* nevezzük, ha vannak olyan (nem feltétlenül különböző) $\mathcal{P}$-beli $(s_1,t_1),(s_2,t_2),\ldots,(s_n,t_n)$ párok úgy, hogy

$$s_1 s_2 \cdots s_n = t_1 t_2 \cdots t_n.$$

Ilyenkor az $s_1 s_2 \cdots s_n$, vagy ami ugyanaz, a $t_1 t_2 \cdots t_n$ szót a $\mathcal{P}$ *megoldásának* nevezzük.
Például a $\mathcal{P} = \{(iz, riz), (kar, ka), (ma, ma)\}$ rendszer megoldható. Egy lehetséges megoldás a *karizma* szó.

Tétel. *Ez a probléma eldönthetetlen.*