

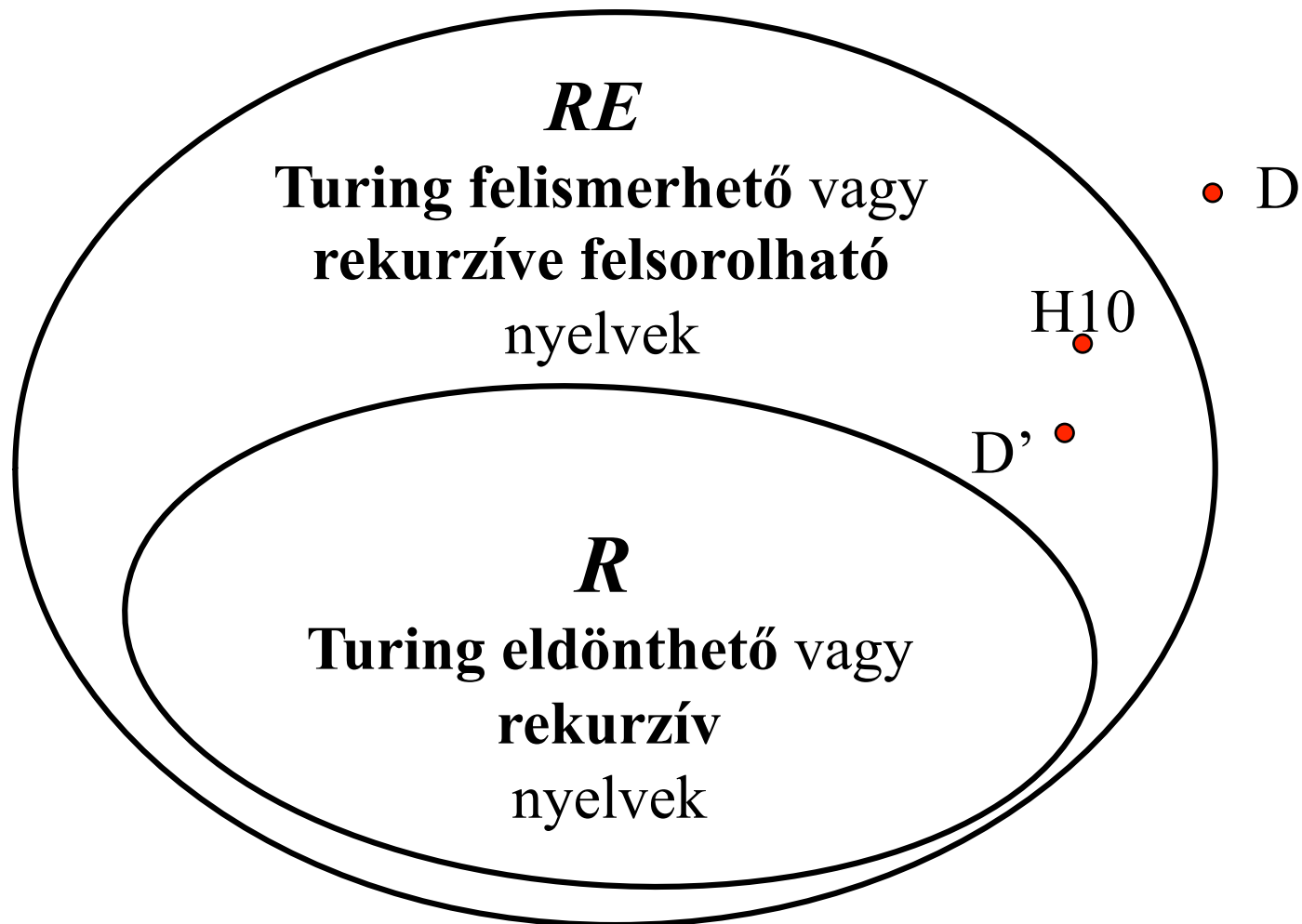
A digitális számítás elmélete

7. előadás március 21.

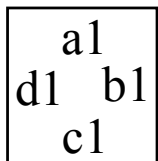
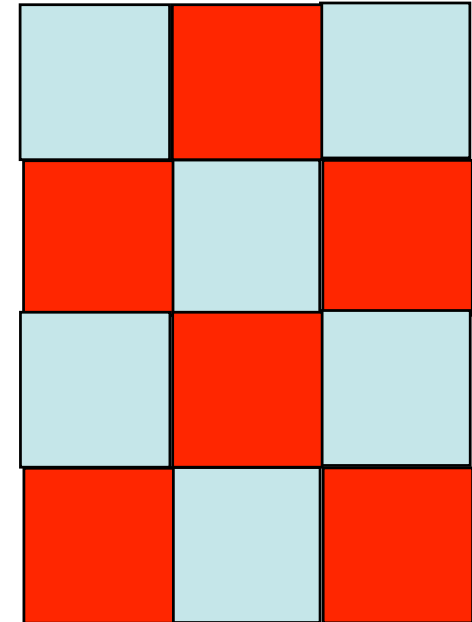
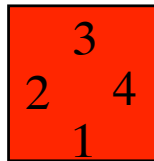
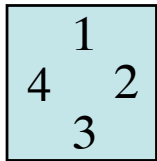
- További példák nem Turing-eldönthető problémákra
 - dominó
 - kongruens számok ... nem tudjuk
- Turing gép megadása kóddal
- Van nem Turing-felismerhető nyelv
 - számossági meggondolás
 - konkrét nyelv megkonstruálása
- Az univerzális Turing gép
- A megállási probléma

Nyelvek felismerhetősége – problémák eldönthetősége

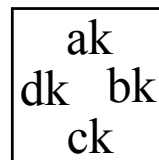
Az összes nyelv



A Dominóprobléma



...



k féle dominóval lefedhető-e a sík

$$F = a_1 * b_1 * c_1 * d_1 \# a_2 * b_2 * c_2 * d_2 \# \dots a_k * b_k * c_k * d_k \#$$

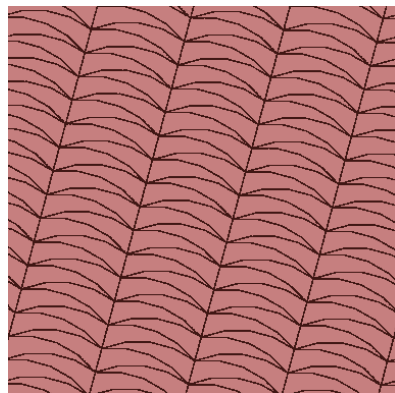
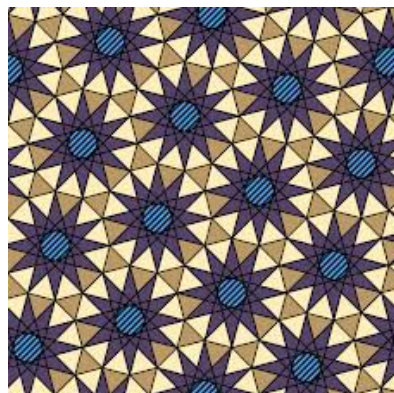
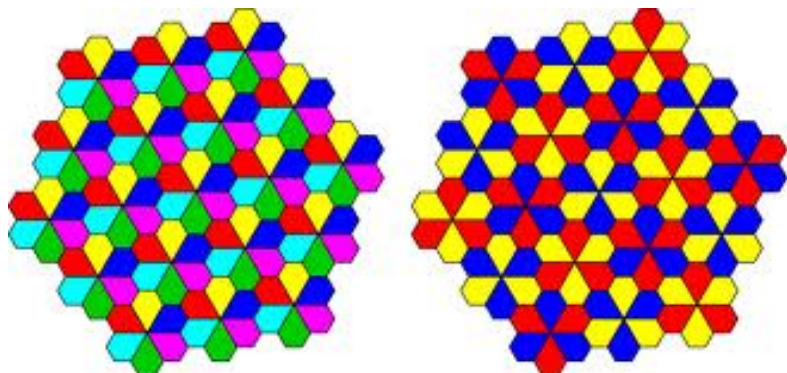
$$D = \{F \in \{0, 1, \dots, 9, *, \#\}^* \mid \text{a sík lefedhető az } F \text{ féle dominókkal}\}$$

D nem eldönthető, és nem is felismerhető, azaz

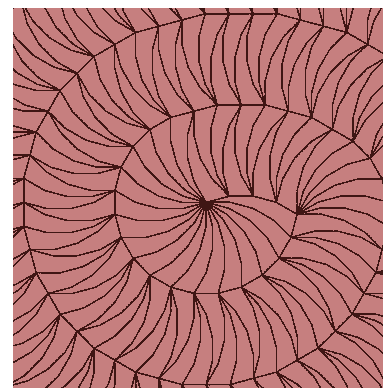
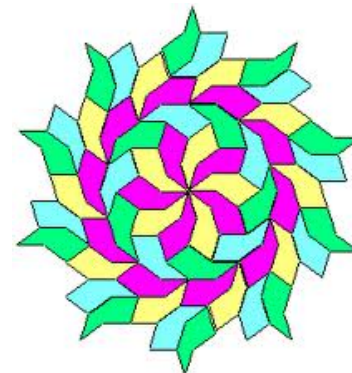
D nem rekurzív, és nem is rekurzíve felsorolható.

Periodikusság

- Periodikus:

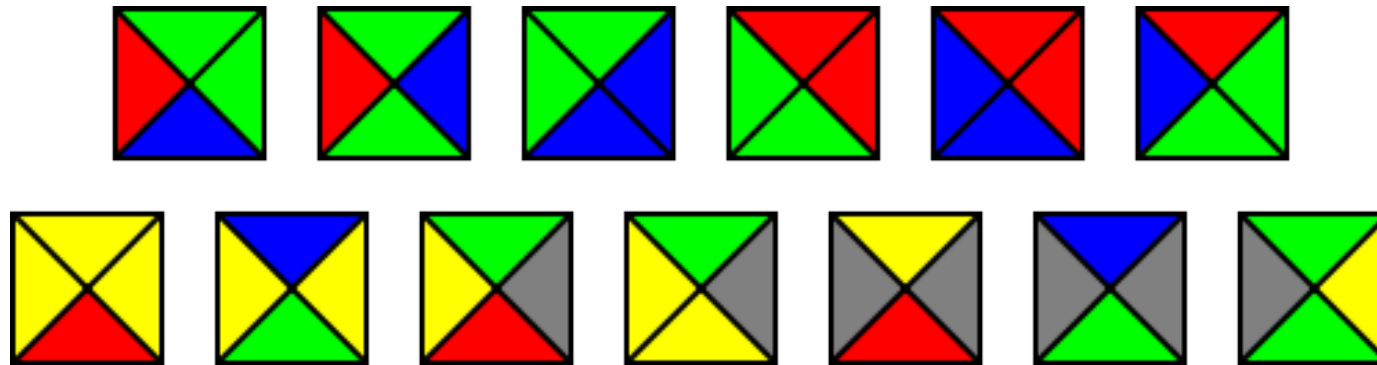


Nem periodikus:



Dominó probléma

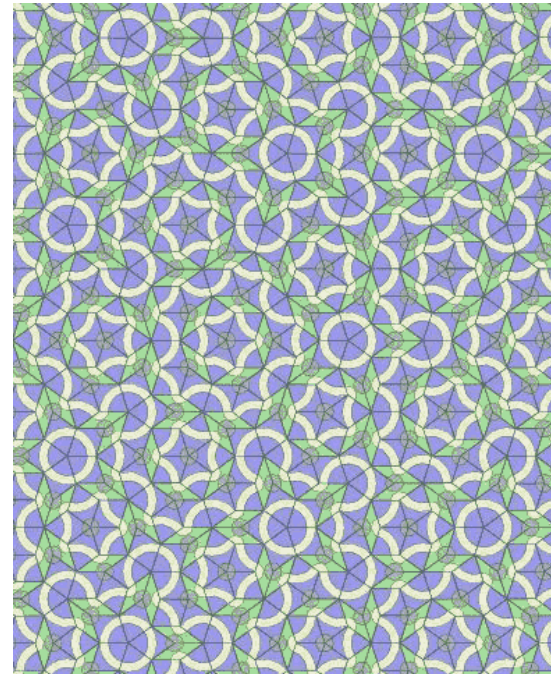
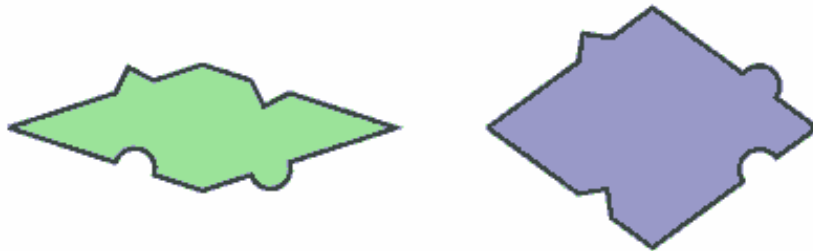
- Adott néhány csempefajta, oldalak színei illeszkedjenek.



- Bármekkora fürdőszobára elég?
 - Ha nem elég, akkor az kiderül (végigpróbálva)
 - Ha van periodikus, kiderül (végigpróbálva)

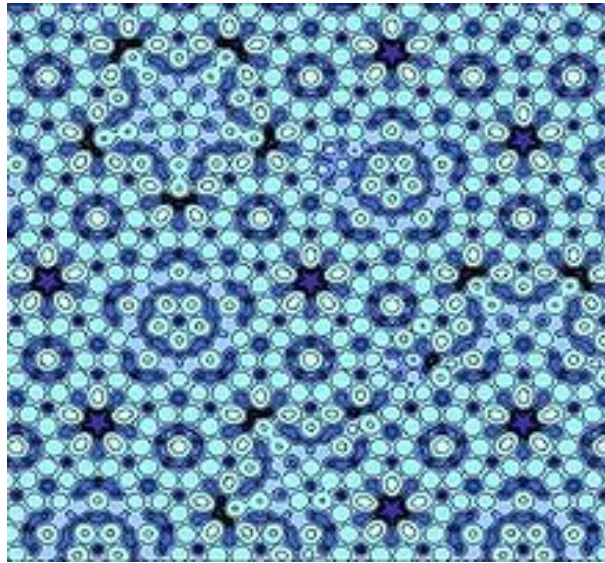
Kvázikristályok

- Léteznie kell olyan csempéknek, amikkel csak NEM periodikusan csempézhetünk.
- Penrose



Kvázikristályok

- Három dimenzióban: Al-Pd-Mn kristály, nem periodikus



- Schechtman: Nobel-díj 2011.

Egy felismerhető verzió (PCP)

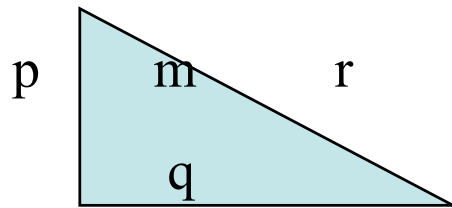
- $\begin{array}{|c|} \hline a_1 \\ \hline b_1 \\ \hline \end{array}, \quad \dots, \quad \begin{array}{|c|} \hline a_k \\ \hline b_k \\ \hline \end{array}, \quad a_i, b_i \in \{0,1\}\text{-feletti nem üres szavak.}$

$$F = a_1 * b_1 \# a_2 * b_2 \# \dots a_k * b_k \#$$

$$D' = \{F \in \{0,1,*,\#\}^* \mid \text{van olyan } i_1, \dots, i_n \text{ indexsorozat, hogy} \\ a_{i_1} \dots a_{i_n} = b_{i_1} \dots b_{i_n}\}.$$

Nyitott kérdés: a kongruens számok felismerése

Definíció: Egy m pozitív szám **kongruens**, ha van olyan derékszögű háromszög, melynek területe m , és oldalai racionális számok.



$$p^2 + q^2 = r^2$$

$$pq = 2m$$

Pl. 5 kongruens: $3/2$, $20/3$, $41/6$

6 kongruens 3,4,5

Nem ismert, hogy a K (a kongruens számok problémája) eldönthető-e.

Megj: K rekurzíve felsorolható: Mivel a rac. számok megszámlálhatók, az azokból alkotott párok is azok. Tehát ha van olyan p, q hogy $pq = 2m$ akkor az kiderül véges sok lépés után. Majd egy ilyen párra az is véges sok lépésben kiderül, ha az a Pythagorasz tételnek eleget tesz valamely r rac. számot választva.

Nyelvek felismerhetősége – problémák eldönthetősége

Tétel: Van olyan $L' \subseteq \Sigma^* = \{0,1\}^*$ nyelv, amely

nem Turing felismerhető, azaz nem rekurzíve felsorolható.

Biz: Egy TG leírható véges jelsorozattal, pl. a definíciós megadással.

Az összes TG felsorolható, mivel k hosszú jelsorozattal megadott TG véges sok van. Legyen $M_1, M_2, \dots, M_n, \dots$ egy felsorolásuk (lásd később részletesen).

Az M_i TG egyértelműen meghatározza az általa felismert L_i nyelvet,

így a Turing felismerhető nyelvek is felsorolhatók: $L_1, L_2, \dots, L_n, \dots$

Azaz a **Turing felismerhető nyelvek megszámlálhatóan sokan** vannak.

Másrészt: Az **összes Σ feletti nyelv számossága** éppen a $\{0,1\}^*$ lehetséges részhalmazainak a számossága, ami **több, mint megszámlálható**. (Biz. középiskola, ill. Cantor módszer.)

Egy nem Turing felismerhető nyelv

Feltesszük az $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{\text{elfogad}}, q_{\text{elutasít}})$ TG-ről, hogy:

- $Q = \{0, 1, \dots, q\}$, 0 a kezdő, q az elfogadó, q-1 az elutasító állapot
- $\Sigma = \{0, 1\}$ bemeneti abc,
- $\Gamma = \{0, 1, \dots, s\}$ szalag abc, s felel meg az üres jelnek, _-nek
- $J=1, B=0$

Ekkor M egyértelműen megadható egy $\{0, 1\}^*$ -beli w szóval, ez M **kódja**. Másrészt egy $\{0, 1\}^*$ -beli szóhoz legfeljebb egy M_w tartozik, aminek a jellegzetességei (állapotok, állapotátmenet fv, abc-k) megadhatók w alapján.

Tehát a TG-eket tekinthetjük speciális $\{0, 1\}^*$ -beli szavaknak.

Egy nem Turing felismerhető nyelv

Pl: Egy M TG megadható a köv. módon:

$$q\#s\# q_0\#x_0\#q_0' \# x_0' \# m_0'\#q_1\#x_1\#q_1' \# x_1' \# m_1'\#\dots$$
$$\dots q_r\#x_r \#q_r' \#x_r' \#m_r'$$

ahol $\delta(q_i, x_j) = (q_i', x_j', m_j')$

Írjuk fel az egész számokat binárisan a fenti sorozatban.

Az így kapott sorozatban alkalmazzuk a következő helyettesítést:

$$\# = 11, 1 = 01, 0 = 00.$$

Az egyértelműség érdekében az állapotátmenetek kódjait (azaz a

$$q_i\#x_i \#q_i' \#x_i' \#m_i' \text{ -nek megfelelő sorozatokat})$$

lexikografikusan soroljuk fel.

Ezzel M-et egy $\{0, 1\}^*$ -beli w szóval írtuk fel.

Egy nem Turing felismerhető nyelv

Jelölje M_w a w által kódolt Turing-gépet.

Megjegyzés: a $\{0, 1\}^*$ -beli szavak felsorolhatók.

Pl. a **kanonikusan**: Az üres szót, majd az 1, 2, ..., k , ...

hosszúságúakat soroljuk fel. Az azonos hosszú sorozatokat

lexikografikusan soroljuk fel, így: ε , 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, ...

Egy nem Turing felismerhető nyelv: L_d

Def: Diagonális nyelv: azon TG kódja, mely TG-ek nem fogadják el a saját kódjukat

$$L_d = \{ w \in \{0, 1\}^*, \text{ az } M_w \text{ gép létezik, és } w \notin L_{M_w} \}$$

Tétel: L_d nem rekurzíve felsorolható nyelv.

Biz: Indirekten, t. fel, hogy L_d rekurzíve felsorolható. Azaz van N TG, mely éppen L_d szavait ismeri fel, $L_d = L_N$. Azaz N felismeri w-t, ha w egy olyan M_w TG-t kódol, mely nem fogadja el a saját kódját.

Mi a helyzet N-nel? Legyen N kódja s. Felismeri-e N s-et, azaz $s \in L_d$ teljesül-e?

Ha feltesszük hogy igen, akkor a def. szerint $s \notin L_d$, ELLENTMONDÁS!!

Ha feltesszük hogy nem, akkor a def. szerint $s \in L_d$, ELLENTMONDÁS!!

Tehát mindkét esetben képtelenségre jutottunk, így az indirekt feltevésünk hamis.

Az univerzális Turing gép

Képes szimulálni tetszőleges, a w kódjával adott M_w TG-et.

Tétel: Van olyan U 3 szalagos TG, melyre teljesül, hogy ha

$w, s \in \{0, 1\}^*$, és M_w létezik, akkor az U gép pontosan akkor fogadja el (utasítja el, kerül végtelen ciklusba) az $w\#s$ bemenetet, amikor M_w az s bemenetet elfogadja (elutasítja, ciklusba kerül).

Bizonyítás: A 3 szalag szerepe

$w\#s$	nem változik, M_w működését adja meg
s	M_w szalagjának a szimulálása
0	M_w pillanatnyi állapota

Az univerzális Turing gép

U működése:

0. Ellenőrzi, hogy w TG-t ír-e le, ha nem, elutasít. Ha igen, beírja s -t a 2., és 0 -t (a kezdőállapot kódját) a 3. szalagra.

1. Az első szalag alapján meghatározza, hogy M_w mit lépne, ha a 3. szalagon megadott állapotban lenne, és az olvasófej alatt a 2. szalagon szereplő jelet látná.

U megteszi M_w lépését, és megfelelően módosítja a 2. és 3. szalag tartalmát.

U megáll elfogadó ill. elutasító állapotban, ha az M_w szerinti új állapot éppen elfogadó ill. elutasító. Ha nem, akkor az 1. lépést ismétli.

Az univerzális nyelv, L_u

Kérdés: Eldönthető-e, hogy egy adott M gép elfogad-e egy adott $s \in \{0, 1\}^*$ szót? ('Szuper' algoritmust keresnénk.)

Def: Univerzális nyelv

$$L_u = \{ w\#s \in \{0, 1\}^*, \quad M_w \text{ létezik,} \quad \text{és } s \in L_{M_w} \}$$

Megj: L_u éppen az univerzális TG nyelve,

azaz $L_u = L_U$, ahol U egy univ. TG.

Tehát L_u rekurzíve felsorolható.

Az univerzális nyelv, L_u

Tétel: (Turing, 1936) L_u nem rekurzív nyelv.

Biz: Indirekten, feltesszük hogy L_u rekurzív nyelv. Ekkor van N TG, mely eldönti L_u -t, azaz minden inputra megáll, és $L_u = L_N$.

Legyen N' a következők szerint működő TG:

1. Ha a $w \in \{0, 1\}^*$ bemenet nem TG kódja, elutasítja.
2. Ha a w bemenet egy TG kódja, akkor elindítja N -t az $w\#w$ bemenettel. Ha ez a szimuláció elfogadó állapotban megáll, akkor N' elutasító állapotban végez, és fordítva, elutasító N állapot esetén a N' végállapota elfogadó.

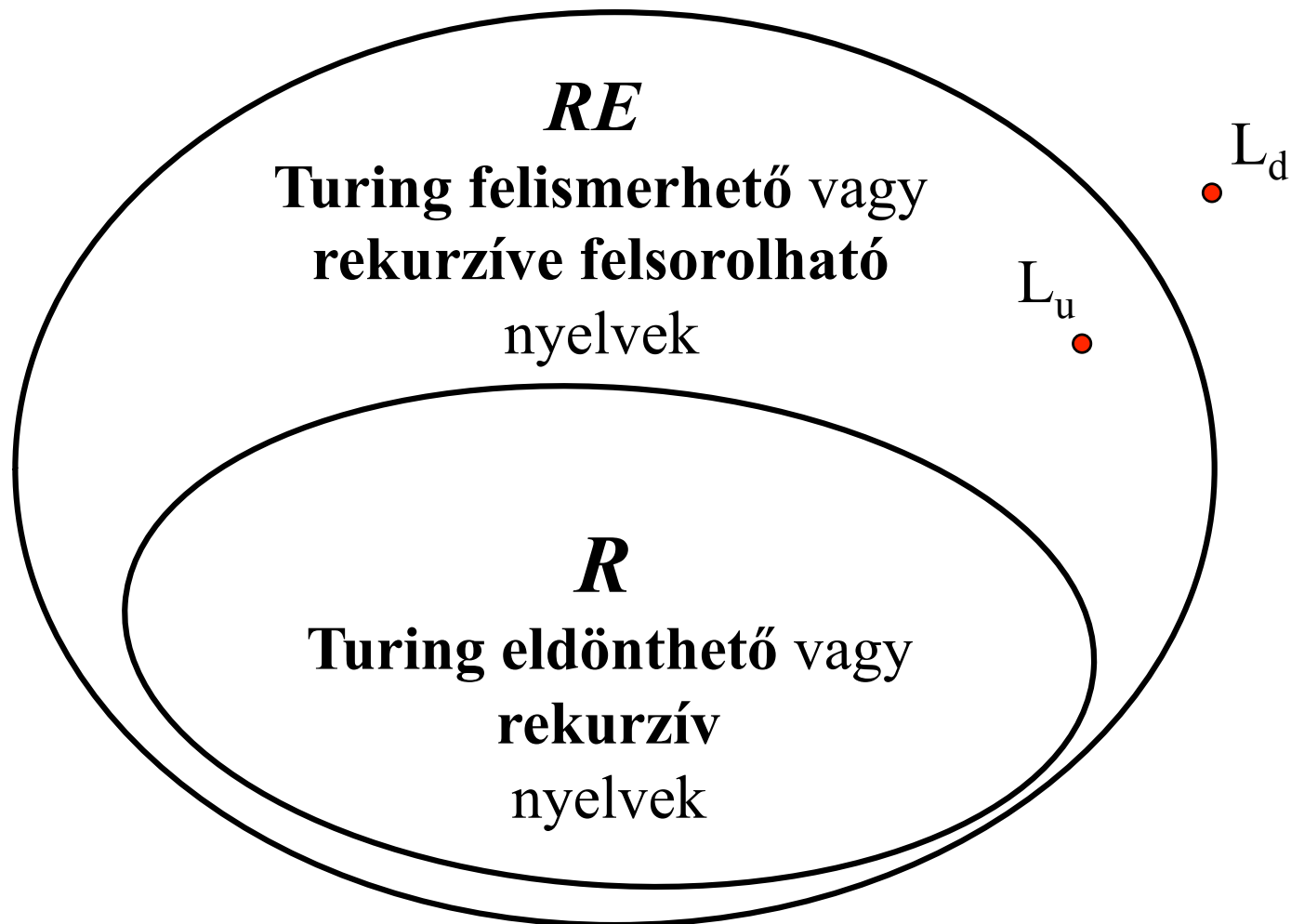
Az univerzális nyelv, L_u

N' minden w bemenetre megáll, az ind. feltevés miatt.

N' pontosan akkor fogadja el w -t, ha M_w létezik, és $w \notin L_M$.

Tehát az $L_{N'}$ a nyelv éppen az L_d nyelv, amelyről láttuk, hogy nem rekurzíve felsorolható. Tehát ellentmondásra jutottunk, az ind. feltevésünk hamis kell hogy legyen, amiből következik, hogy az eredeti állítás igaz.

Nyelvek felismerhetősége – problémák eldönthetősége



A megállási probléma

Kérdés: Eldönthető-e, hogy egy adott M TG gép megáll-e minden bemenetre? ('Nincs-e végtelen ciklus a programunkban'?)

Def: A megállási problémához (halting problem) tartozó L_h nyelv

$$L_h = \{w\#s \in \{0, 1\}^*, M_w \text{ létezik, és } s \text{ bemenettel elindítva megáll}\}$$

Tétel: L_h rekurzíve felsorolható, de nem rekurzív nyelv.

Biz: Legyen U egy univ. TG. Ez L_h szavaira meg fog állni. Legyen U' az a TG, mely azonos U-val, kivéve hogy U elutasít állapotát elfogadra változtattuk. Ekkor $L_h = L_{U'}$, azaz L_h rek. felsorolható.

A megállási probléma

Biz: Azt indirekte mutatjuk meg, hogy L_h nem rekurzív.

Ind. felt: L_h rekurzív, azaz van olyan M TG, mely mindig megáll, és

$$L_h = L_M$$

Legyen M' az a TG, mely először M -et futattja, majd ha M elfogadó állapotban végzett, U -t.

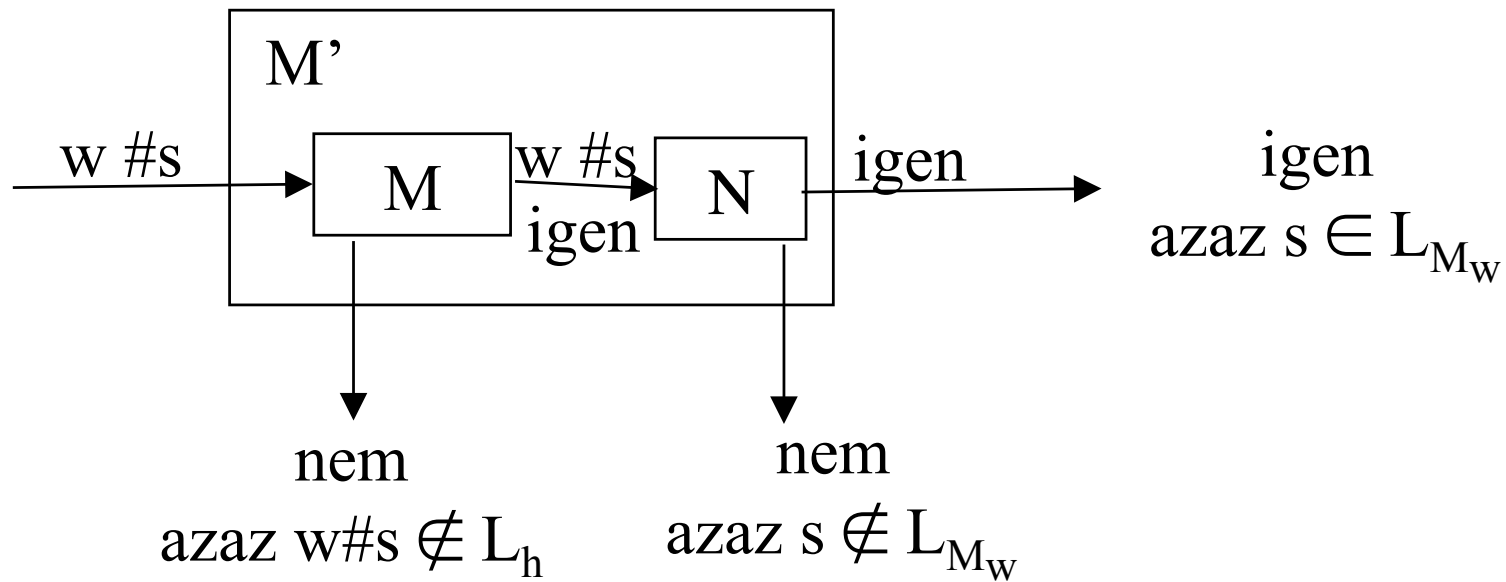
M' mindig megáll az ind. felt. miatt, és M' éppen L_u -t ismeri fel.

De L_u -ról láttuk, hogy nem rekurzív. Az ellentmondás oka az ind.

feltevés, az hamis tehát, azaz a tétel második részének állítása is igaz.

A megállási probléma

Ábra:



A megállási probléma üres inputra

Kérdés: Eldönthető-e, hogy egy adott M TG gép megáll-e az üres bemenetre?

Def: $L_\varepsilon = \{w \in \{0, 1\}^*, M_w \text{ létezik, és az } \varepsilon \text{ (üres) bemenettel elindítva megáll}\}$

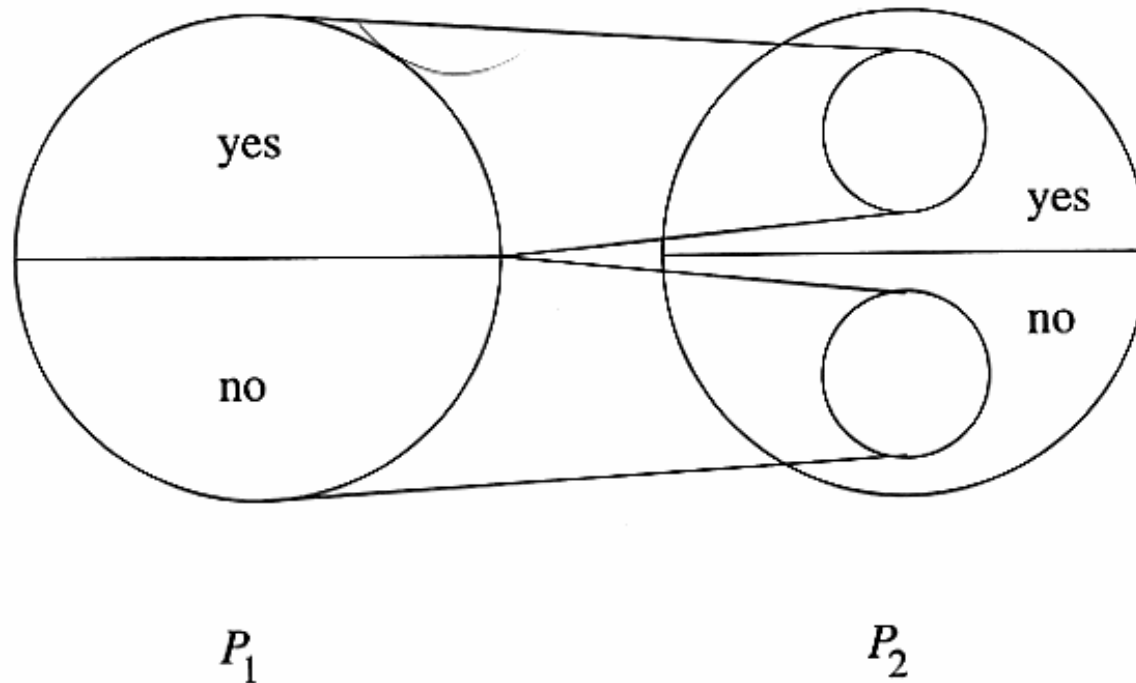
Tétel: L_ε rekurzíve felsorolható.

Biz: A rek. felsorolhatóságot bizonyítja, hogy egy $w \in L_\varepsilon$ esetén az L_h megállási nyelvet felismerő automatát a $w\#\varepsilon = w\#$ inputtal futtatva, ez a gép éppen L_ε -t ismeri fel.

Tétel: L_ε nem eldönthető. Bizonyítás: **visszavezetéssel.**

Visszavezetések

P_1 visszavezetése P_2 -re ($P_1 \leq P_2$):



Def. $L_1 \subseteq \Sigma^*$ visszavezethető az $L_2 \subseteq \Delta^*$ nyelvre, ha van olyan Turing-géppel kiszámítható $f: \Sigma^* \rightarrow \Delta^*$ függvény, hogy minden $w \in \Sigma^*$ szóra teljesül, hogy $w \in L_1 \Leftrightarrow f(w) \in L_2$.

Visszavezetések

Tétel: Ha $L_1 \leq L_2$ és

- L_2 eldönthető (rekurzív), akkor L_1 is eldönthető.
- L_2 Turing-felismerhető (rekurzívan felsorolható), akkor L_1 is Turing-felismerhető.

Biz.: pl. a visszavezetést kiszámoló és az L_2 -t eldöntő Turing-gép „kompozíciója” az L_1 nyelvet dönti el.

Hogyan lehet ezt eldönthetetlenség bizonyítására használni?

Ha $L_1 \leq L_2$ és L_1 nem eldönthető, akkor L_2 sem lehet eldönthető.

A megállási probléma eldönthetlensége újra

Tétel: L_h eldönthetetlen.

Biz.: Megmutatjuk, hogy $L_u \leq L_h$. Tetszőleges M Turing-géphez és s bemenethez konstruáljuk meg az M' Turing-gépet a következő módon.

M' annyiban különbözik M -től, hogy amikor M elutasító állapotba lép, akkor M' végtelen ciklusba lép. Minden további esetben az M' másolja M működését. Legyen w és w' rendre az M és az M' kódja. Nyilvánvaló, hogy az $f(w)=w'$ fgv. kiszámítható egy Turing-géppel. Továbbá:

$$w\#s \in L_u \Leftrightarrow w'\#s \in L_h.$$

L_ε eldönthetlensége újra

Tétel: L_ε eldönthetetlen.

Biz.: Megmutatjuk, hogy $L_h \leq L_\varepsilon$.

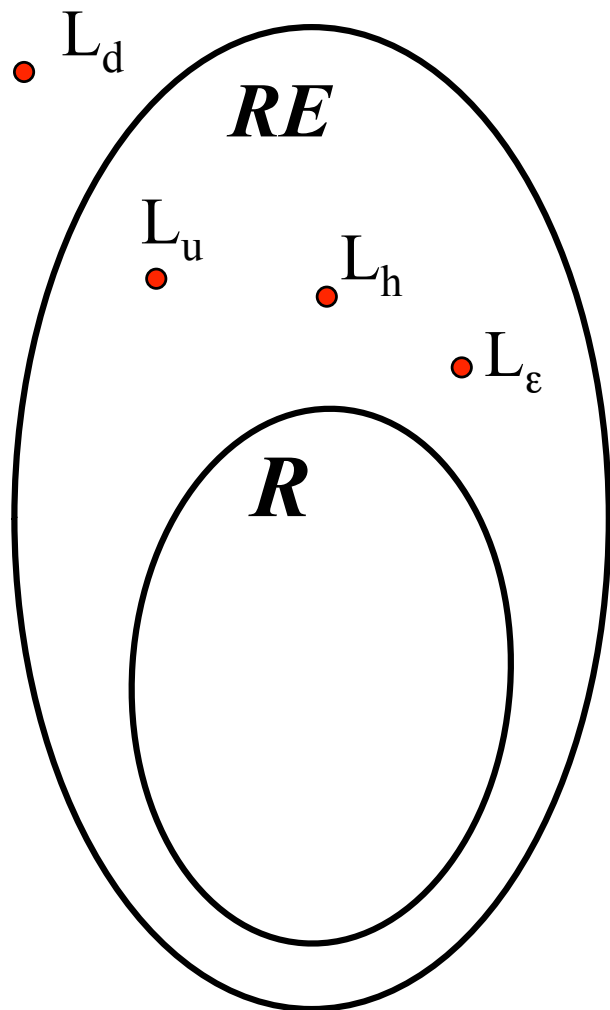
Adott M Turing-géphez és s bemenethez legyen M' a következő Turing-gép.

M' tetszőleges u bemeneten a következőt teszi. M' megvizsgálja u -t, és ha u nem az üres szó, akkor M' elfogadja a bemenetet. Ha u az üres szó, akkor M felmásolja a szalagjára az s szót és elkezdi szimulálni az M -et az s szón. Legyen rendre w és w' az M és az M' kódja. Az $f(w)=w'$ fgv. kiszámítható egy Turing-géppel. Továbbá:

$$w\#s \in L_u \Leftrightarrow w' \in L_h.$$

Áttekintés

Bizonyítások:



$L_d \notin RE$ Indirekte, közvetlenül Cantor diag.
elv.

$L_u \in R$ -ből következne, hogy $L_d \in RE$

$L_h \in R$ -ből következne, hogy $L_u \in R$

$L_\varepsilon \in R$ -ből következne, hogy $L_h \in R$