# Teoria de la calculabilitat

Antoni Lozano

Universitat Politècnica de Catalunya

# Contingut

# Contingut

La teoria de la computació està formada per les teories:

1. d'autòmats i llenguatges
2. de la calculabilitat
3. de la complexitat

Pregunta comuna:

Quines són les capacitats i limitacions dels ordinadors

# Introducció

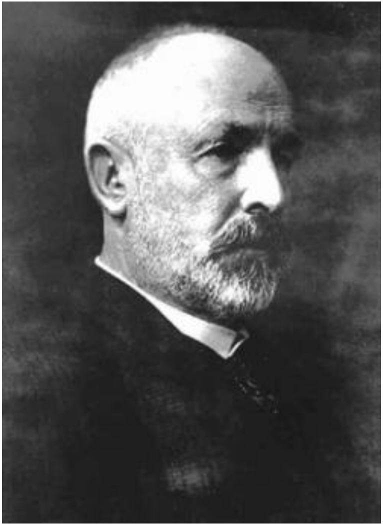
Els models de càlcul formals representen el concepte de computació:

1. Autòmats finits (FA)
2. Gramàtiques incontextuals (CFG)
3. Autòmats amb pila (PDA)
4. Màquines de Turing (TM)

Tots els models precedents es poden codificar amb cadenes de símbols sobre $\{0, 1\}$.

# Contingut

# Georg Cantor (Sant Petersburg 1845 – Halle 1918)



# 1874: Teoria de conjunts

El 1874, Georg Cantor publica:

Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen

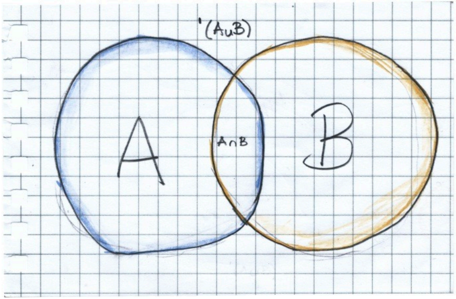
Sobre una propietat característica de tots els nombres reals algebraics

i funda la teoria de conjunts.

A partir d'aquí, les matemàtiques ja no serien el mateix.

Cantor defineix un conjunt com una col·lecció d'objectes, que pot ser finita o infinita.

Desenvolupa la teoria de conjunts *naïve* on qualsevol col·lecció és un conjunt




amb les operacions habituals: $\cup$, $\cap$, $\setminus$, $\times$, $\mathcal{P}$.

La teoria de conjunts de Cantor va ser objecte de controvèrsies:

- L. Kronecker
  *"Déu creà els nombres naturals; la resta, és obra de l'home"*
- D. Hilbert
  *"Ningú ens farà mai fora del paradís que Cantor ha creat per nosaltres"*

Cantor compara cardinalitats mitjançant bijeccions:

- Comptar ovelles
- Paradoxa de Galileu: es pot establir la correspondència

| | |
|---|---|
| $1 - 1$ | $6 - 36$ |
| $2 - 4$ | $7 - 49$ |
| $3 - 9$ | $8 - 64$ |
| $4 - 16$ | $9 - 81$ |
| $5 - 25$ | $10 - 100$ |

Això vol dir que hi ha tants quadrats com naturals?

Cantor respon que sí.

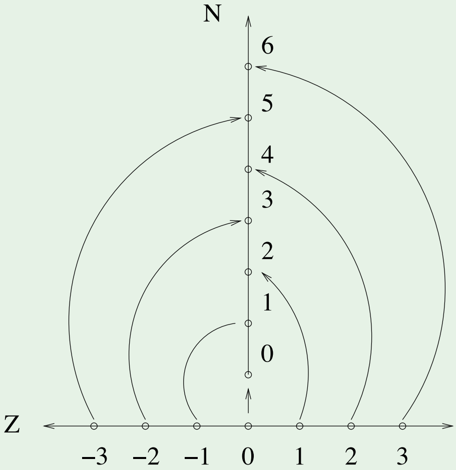
**Mateixa cardinalitat**

Donats dos conjunts $A$ i $B$, $|A| = |B|$ si existeix una bijecció $f : A \to B$.

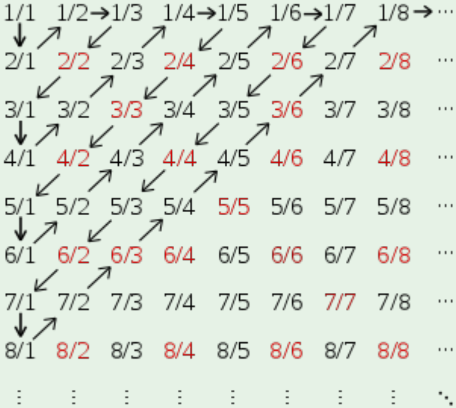
**Exemples**

- $|\{a, b, c\}| = |\{1, 2, 3\}|$
- $|\{1, 2, 3, 4, \dots\}| = |\{0, 1, 2, 3, \dots\}|$
- $|\{0, 2, 4, 6, \dots\}| = |\{1, 3, 5, 7, \dots\}|$

# Enters: $\mathbb{Z}$

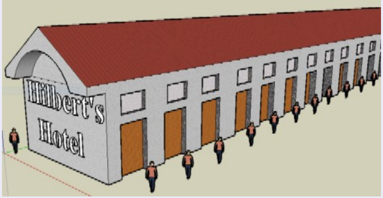


# Racionals: $\mathbb{Q}$



## Hotel de Hilbert

Un hotel té tantes habitacions com nombres naturals.




Un dia, l'hotel és ple. Com es farà lloc a

- Un hoste més?
- Tants hostes més com nombres naturals?
- Tants hostes més com subconjunts de naturals?

## Enumerabilitat

Un conjunt $A$ és enumerable si $A$ és finit o $|A| = |\mathbb{N}|$.

## Conjunts enumerables

Els conjunts $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$ i $\mathbb{Q}$ són enumerables.

## Conjunts no enumerables

Els conjunts $\mathcal{P}(\mathbb{N})$ i $\mathbb{R}$ no són enumerables.

# 1891: Argument diagonal de Cantor

### $\mathbb{R}$ no és enumerable

Si $\mathbb{R}$ fos enumerable, $(0,1)$ també. Per tant, es pot escriure

$$(0,1) = \{r_0, r_1, r_2, \ldots\}.$$

Sigui $r_i = 0, x_{i0}x_{i1}x_{i2}\ldots$ l'expansió decimal de $r_i$.

Definim $y_i = \begin{cases} 7, & \text{si } x_{ii} \neq 7, \\ 3, & \text{si } x_{ii} = 7. \end{cases}$

i formem el nombre $r = 0, y_0y_1y_2\ldots$

Llavors, $r \neq r_i$ perquè difereixen en l'$i$-èssim lloc decimal.
Contradicció: $r \in (0,1)$ però no és a la llista.

## $\mathbb{R}$ no és enumerable

Amb les expansions decimals de $(0,1) = \{r_0, r_1, r_2, \dots\}$:

| | 0 | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|---|
| $r_0$ | 5 | 9 | 2 | 0 | 1 | ... |
| $r_1$ | 1 | 0 | 4 | 3 | 9 | ... |
| $r_2$ | 7 | 8 | 7 | 6 | 0 | ... |
| $r_3$ | 0 | 8 | 3 | 2 | 2 | ... |
| $r_4$ | 1 | 2 | 7 | 5 | 7 | ... |

tindríem $r = 0,77373$...

## $\mathcal{P}(\mathbb{N})$ no és enumerable

Amb la llista de conjunts de $\mathcal{P}(\mathbb{N}) = \{A_0, A_1, A_2, \dots\}$:

| | 0 | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|---|
| $A_0$ | 0 | 1 | 1 | 0 | 1 | ... |
| $A_1$ | 1 | 0 | 1 | 1 | 0 | ... |
| $A_2$ | 0 | 1 | 1 | 0 | 0 | ... |
| $A_3$ | 0 | 1 | 0 | 0 | 1 | ... |
| $A_4$ | 1 | 1 | 1 | 0 | 0 | ... |

El conjunt representat per

| | | | | | | |
|---|---|---|---|---|---|---|
| $A$ | 1 | 1 | 0 | 1 | 1 | ... |

no apareix a la llista.

## Teorema de Cantor

Donat un conjunt $C$,

$$|C| < |\mathcal{P}(C)|.$$

## Corol·lari

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$$

- Es pot demostrar que $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.
- Però hi ha algun infinit entre el de $\mathbb{N}$ i el de $\mathbb{R}$?

## Hipòtesi del continu (CH)

No hi ha cap conjunt $C$ tal que $|\mathbb{N}| < |C| < |\mathbb{R}|$.

Cantor va treballar molt de temps sobre la CH sense èxit.

Ara sabem que la CH no es pot

- refutar (Gödel, 1940) ni
- demostrar (Cohen, 1963)

dins del sistema axiomàtic actual (ZFC). Diem que CH és *independent* de ZFC.

Per notícies actuals sobre la hipòtesi del continu, veure l'article

> *How Many Numbers Exist? Infinity Proof Moves Math Closer to an Answer.*

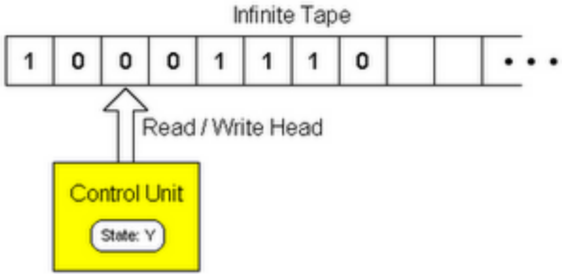
a `https://www.quantamagazine.org`

# Contingut

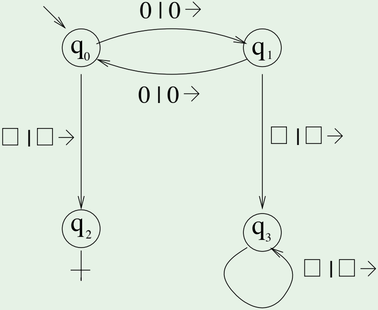
# Alan Turing (Londres 1912 – Cheshire 1954)

# Màquina de Turing

Model teòric d'ordinador, equivalent a un sistema formal.



# Màquina de Turing: nombre parell de 0's



# La màquina de Turing

## Definició de llenguatge reconegut

Diem que una TM $M$ accepta un mot $x \in \Sigma^*$ si, a partir de la configuració inicial i $x$ escrit a la cinta d'entrada, arriba a una configuració final.

## Notació

$L(M) = \{x \mid M \text{ accepta } x\}$.
$M(x)\downarrow$: $M$ s'atura amb entrada $x$
$M(x)\uparrow$: $M$ no s'atura amb entrada $x$

## Aturada segura

Diem que una TM $M$ és *d'aturada segura* si $M$ s'atura per a tota entrada $x$, és a dir, si $\forall x \in \Sigma^*\ M(x)\downarrow$.

**Definició**

En el cas que $M$ sigui una TM d'aturada segura, diem que $L(M)$ és el llenguatge decidit per $M$.

**Definició**

Un llenguatge és *decidible* si és decidit per alguna TM.
Un llenguatge és *semidecidible* si és reconegut per alguna TM.

**Proposició**

Tot llenguatge decidible és semidecidible.

# La màquina de Turing

## Codificació de les TM

- Les TM es poden codificar com a mots sobre $\{0, 1\}$.
- Hi ha una bijecció entre $\{0, 1\}^*$ i $\mathbb{N}$.
- El natural associat a una TM se'n diu *nombre de Gödel* de la TM.

## Notació

La TM amb nombre de Gödel $i$ es representa amb $M_i$.

# La màquina de Turing

**Teorema**

Existeixen llenguatges indecidibles.

**Demostració**

- El conjunt de TM és enumerable.
- El conjunt de llenguatges sobre $\{0, 1\}$ no és enumerable.

Per tant, hi ha llenguatges que no són decidits per cap TM.

# La màquina de Turing

**Definició**

Diem que una TM $M_i$ computa una funció $f$ si, per a tot mot $x \in \Sigma^*$:

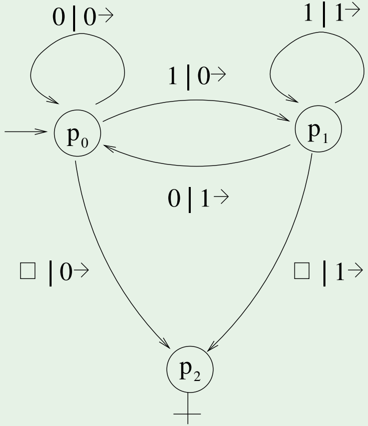
- $M_i(x) \downarrow$ i deixa a la cinta $f(x)$ si $f$ està definida en $x$
- $M_i(x) \uparrow$ si $f$ està indefinida en $x$

**Notació**

La funció computada per la màquina $M_i$ es representa amb $\varphi_i$.

## Exemple

Aquesta TM computa la funció $f : \{0,1\}^* \to \{0,1\}^*$ tal que $f(x) = 0x$, per a tot $x \in \{0,1\}^*$.



# La màquina de Turing

**Tesi de Church-Turing.** *Qualsevol algorisme concebible es pot implementar en el model de màquina de Turing.*

En particular, qualsevol algorisme codificat en qualsevol llenguatge de programació es pot convertir en una màquina de Turing.

En les demostracions no construïrem màquines de Turing sinó pseudocodi, sabent que es pot arribar a codificar com a TM.

### Proposició

Existeix una TM universal. És a dir, hi ha un nombre de Gödel $u$ tal que

$$L(M_u) = \{\langle i, j\rangle \mid M_i \text{ accepta } j\}.$$

L'existència de la màquina universal situa automàticament el seu llenguatge $L(M_u)$ —el llenguatge universal— entre els semidecidibles.

És a dir, es pot "semidecidir" si una màquina de Turing donada accepta una certa entrada: $L(M_u) = \{\langle i, j\rangle \mid M_i \text{ accepta } j\}$.

# La màquina de Turing

El problema de l'aturada s'assembla a $L(M_u)$ però consisteix només a decidir l'aturada d'una TM amb una entrada. El veiem en dues versions:

- El que anomenem pròpiament *problema de l'aturada*, més general
$$\text{HALT} = \{\langle i, j\rangle \mid M_i(j)\downarrow\}.$$
- L'anomenat *problema de l'autoaturada* que consisteix a decidir si una TM s'atura quan se li proporciona la seva pròpia codificació com a entrada:
$$\text{K} = \{i \mid M_i(i)\downarrow\}.$$

# Contingut

# Problema de l'aturada

Com saber si un programa s'atura?

- Executant-lo?
- Inspeccionant-ne el codi?
- Amb un altre programa?

Veurem que no existeix cap programa que pugui decidir l'aturada.

# Problema de l'aturada

Com saber si un programa s'atura?

- Executant-lo?
- Inspeccionant-ne el codi?
- Amb un altre programa?

Veurem que no existeix cap programa que pugui decidir l'aturada.

# Problema de l'aturada

Com saber si un programa s'atura?

- Executant-lo?
- Inspeccionant-ne el codi?
- Amb un altre programa?

Veurem que no existeix cap programa que pugui decidir l'aturada.

# Problema de l'aturada

Com saber si un programa s'atura?

- Executant-lo?
- Inspeccionant-ne el codi?
- Amb un altre programa?

Veurem que no existeix cap programa que pugui decidir l'aturada.

# Exemple

## Conjectura dels primers bessons

Existeixen infinits primers bessons, és a dir, primers que difereixen en un valor de 2 (com 3 i 5, 5 i 7, 11 i 13, 17 i 19,...)

### PRIMERS BESSONS($n$)

$p \leftarrow n$<br>
**mentre** (**no** PRIMER($p$)) **o** (**no** PRIMER($p+2$))<br>
    $p \leftarrow p + 1$<br>
**retornar** $p$, $p+2$

# Problemes indecidibles

**Teorema**

K i HALT són semidecidibles.

Considerem la TM següent:

$M(\langle i, j \rangle)$

1 **simular** $M_i(j)$
2 **acceptar**

Com que la línia 2 s'executa només si la simulació de la línia 1 s'ha aturat, la màquina $M$ accepta exactament les entrades $\langle i, j \rangle$ de HALT. Per tant $L(M) = \text{HALT}$ i, per tant, HALT és semidecidible.

De manera semblant, es pot veure que K és semidecidible.

# Aturada de les TM

| | 0 | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|---|
| $M_0$ | $\uparrow$ | $\downarrow$ | $\downarrow$ | $\downarrow$ | $\uparrow$ | |
| $M_1$ | $\uparrow$ | $\downarrow$ | $\uparrow$ | $\uparrow$ | $\downarrow$ | |
| $M_2$ | $\downarrow$ | $\uparrow$ | $\uparrow$ | $\downarrow$ | $\downarrow$ | |
| $M_3$ | $\downarrow$ | $\downarrow$ | $\downarrow$ | $\uparrow$ | $\uparrow$ | |
| $M_4$ | $\uparrow$ | $\downarrow$ | $\uparrow$ | $\downarrow$ | $\downarrow$ | ... |

Si la diagonal es pogués calcular amb aturada segura,

$$\exists k\ \forall i \quad M_k(i)\!\downarrow \Leftrightarrow M_i(i)\!\uparrow$$

Però llavors $M_k(k)\!\downarrow \Leftrightarrow M_k(k)\!\uparrow$.

# Problemes indecidibles

### Teorema

K és indecidible.

Per reducció a l'absurd i diagonalització. Suposem que K és decidible: existeix una TM d'aturada segura $M$ t.q. $L(M) = K$. Llavors, podríem definir la TM:

$N(x)$

**simular** $M(x)$
**si** accepta
    **bucle infinit**

$\exists k \; N = M_k$. Per a tot $x$,

$$M_k(x)\downarrow \;\Leftrightarrow\; M \text{ rebutja } x \;\Leftrightarrow\; M_x(x)\uparrow,$$

Amb $x = k$, $M_k(k)\downarrow \Leftrightarrow M_k(k)\uparrow$, contradicció!

## Teorema

HALT és indecidible.

Per reducció a l'absurd. Si HALT fos decidible, existiria una TM d'aturada segura $M$ t.q. $L(M) = \text{HALT}$. Llavors, podríem definir la TM:

$N(i)$

**simular** $M(\langle i, i \rangle)$
**si** accepta
  **acceptar**
**si no**
  **rebutjar**

Per a tot $x$,

$$N \text{ accepta } i \iff M \text{ accepta } \langle i, i \rangle \iff \langle i, i \rangle \in \text{HALT} \iff i \in K.$$

$N$ és una TM d'aturada segura que reconeix K, contradicció!

# Problemes indecidibles

## Teorema

El complementari d'un llenguatge decidible és decidible.

Sigui $A$ un llenguatge decidible. Llavors, existeix una TM d'aturada segura $M$ t.q. $L(M) = A$. Sigui $M'$ la TM:

$M'(x)$

```
simular M(x)
si accepta
    rebutjar
si no
    acceptar
```

$M'$ és una TM d'aturada segura tal que

$$L(M') = \{x \mid M(x) \text{ rebutja } \} = \{x \mid x \notin A\} = \overline{A}.$$

# Problemes indecidibles

## Teorema (del complementari)

Un llenguatge $A$ és decidible si i només si $A$ i $\overline{A}$ són semidecidibles.

$\Rightarrow$: Si $A$ és decidible, és trivial deduir que tant $A$ com $\overline{A}$ són semidecidibles.
Simularem $M_A$ i $M_{\overline{A}}$ en "paral·lel" de manera que la primera que accepti indicarà si $x$ pertany a $A$ o al complementari.

# Problemes indecidibles

**Teorema (del complementari)**

Un llenguatge $A$ és decidible si i només si $A$ i $\overline{A}$ són semidecidibles.

$\Leftarrow$: Suposem que $A$ i $\overline{A}$ són semidecidibles.

Llavors existeixen dues TM $M_A$ i $M_{\overline{A}}$ t.q.

$$L(M_A) = A \text{ i } L(M_{\overline{A}}) = \overline{A}.$$

Simularem $M_A$ i $M_{\overline{A}}$ en "paral·lel" de manera que la primera que accepti indicarà si $x$ pertany a $A$ o al complementari.

Definim la TM següent:

$N(x)$

$k = 0$<br>
**repetir**<br>
    **simular** $M_A(x)$ i $M_{\overline{A}}$ durant $k$ passos<br>
    **si** $M_A(x)$ ha acceptat<br>
        **acceptar**<br>
    **si** $M_{\overline{A}}(x)$ ha acceptat<br>
        **rebutjar**<br>
    $k = k + 1$<br>
**fins fals**

Clarament, $L(N) = A$ i $N$ és d'aturada segura. Per tant, $A$ és decidible.

# Problemes indecidibles

Recordem que K i HALT són semidecidibles. Per tant, el teorema del complementari implilca la propietat següent.

**Corol·lari**

Els problemes $\overline{\text{K}}$, $\overline{\text{HALT}}$ no són semidecidibles.

# Problemes indecidibles

- **Llenguatges decidibles.**
  REC $= \{L \mid L$ és un llenguatge decidible$\}$, la classe que conté tots els llenguatges decidibles, com ara el conjunt dels primers, el buit, el total, el llenguatge dels mots sobre $\{a, b\}$ que contenen el mateix nombre d'as que de bes, un conjunt que representa els llistats de notes de la FIB en tota la seva història (és un conjunt finit, és clar) o qualsevol conjunt finit.
- **Llenguatges semidecidibles.**
  RE $= \{L \mid L$ és un llenguatge semidecidible$\}$, la classe que conté tots els llenguatges semidecidibles, com ara K, HALT, el llenguatge universal, el problema de la correspondècia de Post, qualsevol llenguatge decidible o el conjunt d'enunciats d'afirmacions matemàtiques demostrables.

# Problemes indecidibles

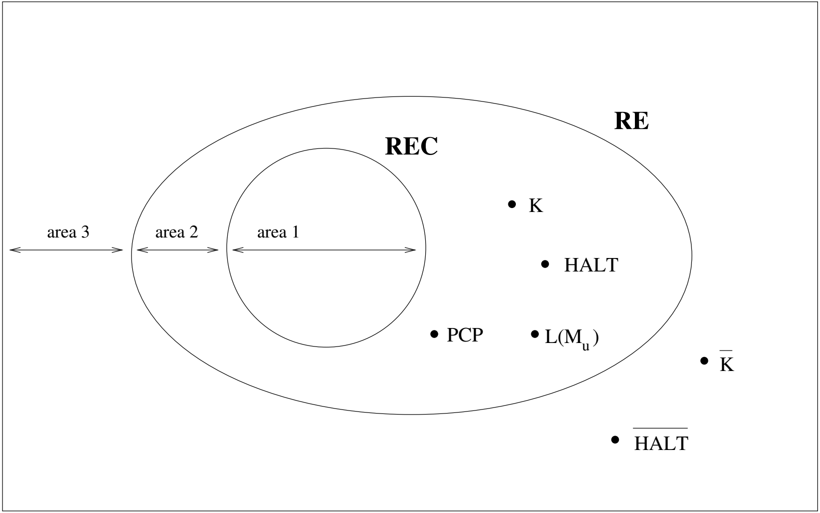



Figura: Classificació de problemes a RE i REC.

# Contingut

# Reduccions

### Reduccions

Donats dos llenguatges $A$ i $B$ sobre un alfabet $\Sigma$, diem que *$A$ es redueix a $B$* si existeix una funció computable $f$ tal que, per a tot $x \in \Sigma^*$,

$$x \in A \Leftrightarrow f(x) \in B.$$

En aquest cas, escrivim $A \leqslant_m B$ (*via* $f$) i diem que $f$ és una reducció de $A$ a $B$.

## Paritat

Considerem el llenguatge dels nombres parells

$$\text{PARELLS} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} \quad x = 2y\ \}$$

i el dels senars

$$\text{SENARS} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} \quad x = 2y + 1\ \}$$

Veiem que podem reduir PARELLS a SENARS (PARELLS $\leqslant_m$ SENARS) amb una funció $f$ tal que $f(x) = x + 1$. És evident que per a tot $x$:

$$x \in \text{PARELLS} \Leftrightarrow f(x) \in \text{SENARS}.$$

Fixem-nos que podem reduir SENARS a PARELLS amb la mateixa funció $f$, és a dir, SENARS $\leqslant_m$ PARELLS via $f$. En general, però, la relació $\leqslant_m$ no és simètrica.

# Reduccions

## Tancament dels decidibles per reduccions

Si $A \leqslant_m B$ i $B$ és decidible, $A$ també és decidible.

## Corol·lari

Si $A \leqslant_m B$ i $A$ és indecidible, $B$ també és indecidible.

# Reducciones

**Tancament dels semidecidibles per reduccions**

Si $A \leqslant_m B$ i $B$ és semidecidible, $A$ també és semidecidible.

**Corol·lari**

Si $A \leqslant_m B$ i $A$ no és semidecidible, $B$ tampoc no és semidecidible.

## Exemple 1: $\mathrm{K} \leqslant_m \mathrm{HALT}$

Definim la funció

$$f(x) = \langle x, x \rangle,$$

que és computable. A més, donat un mot $x$,

$$x \in \mathrm{K} \Leftrightarrow M_x(x)\!\downarrow \Leftrightarrow f(x) \in \mathrm{HALT}$$

i, per tant, $f$ és una reducció de K a HALT.

## Example 2: $\mathrm{K} \leqslant_m \{p \mid \exists y \;\; M_p(y)\downarrow\}$

Sigui $A = \{p \mid \exists y \;\; M_p(y)\downarrow\}$, el conjunt de “programes” o TM $p$ que s’aturen per a alguna entrada $y$. Volem trobar una funció computable $f$ t.q. per a tot $x$

$$x \in \mathrm{K} \Leftrightarrow f(x) \in A.$$

Definim $f(x) = p$, on $p$ és el nombre de Gödel de la TM:

$M_p(y)$

1 **simular** $M_x(x)$

Si $x \in \mathrm{K}$ llavors $M_x(x)\downarrow$ i, tal com està definida $M_p$, és evident que s’atura per a tot $y$ i, per tant, $p \in A$.
Si $x \notin \mathrm{K}$, llavors $M_x(x)\uparrow$ i, per tant, $M_p(y)\uparrow$ per a tot $y$. Per tant, $p \notin A$.