

6. Màniques de Turing

Teoria de la Computació

FIB

Antoni Lozano
Q1 2024–2025

Màquines de Turing

- 1 Introducció
- 2 Teoria de conjunts
- 3 La màquina de Turing
- 4 Problemes indecidibles

Màquines de Turing

- 1 Introducció
- 2 Teoria de conjunts
- 3 La màquina de Turing
- 4 Problemes indecidibles

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

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 $\{0, 1\}$.

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 $\{0, 1\}$.

Màquines de Turing

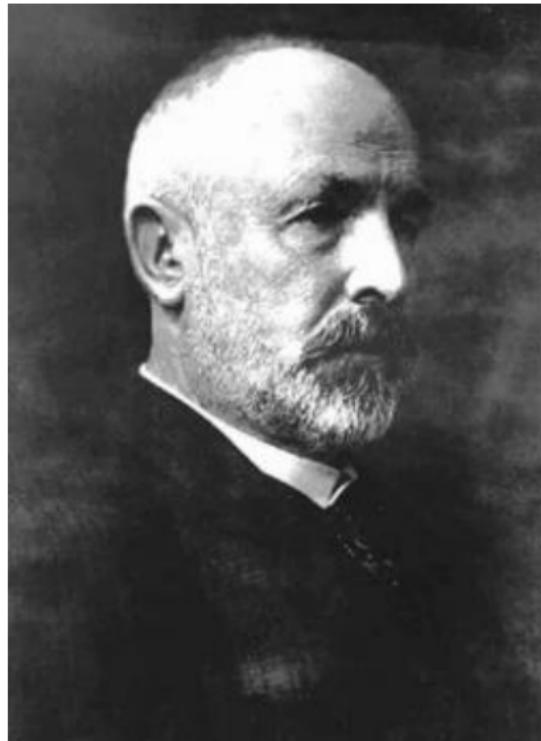
1 Introducció

2 Teoria de conjunts

3 La màquina de Turing

4 Problemes indecidibles

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

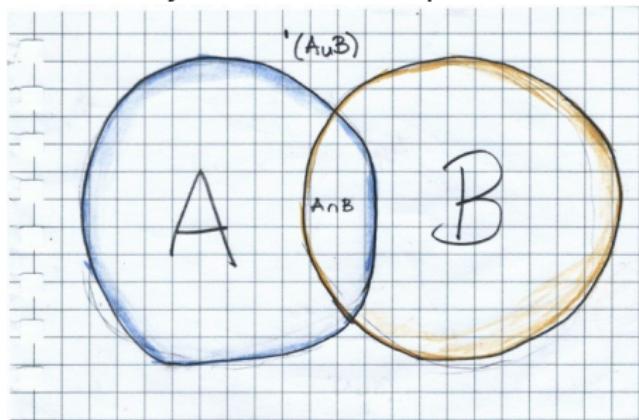
Sobre una propietat característica de
tots els nombres reals algebraics

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"

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"

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 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 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 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 biecció $f : A \rightarrow B$.

Exemples

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

Cantor respon que sí.

Mateixa cardinalitat

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

Exemples

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

Cantor respon que sí.

Mateixa cardinalitat

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

Exemples

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

Cantor respon que sí.

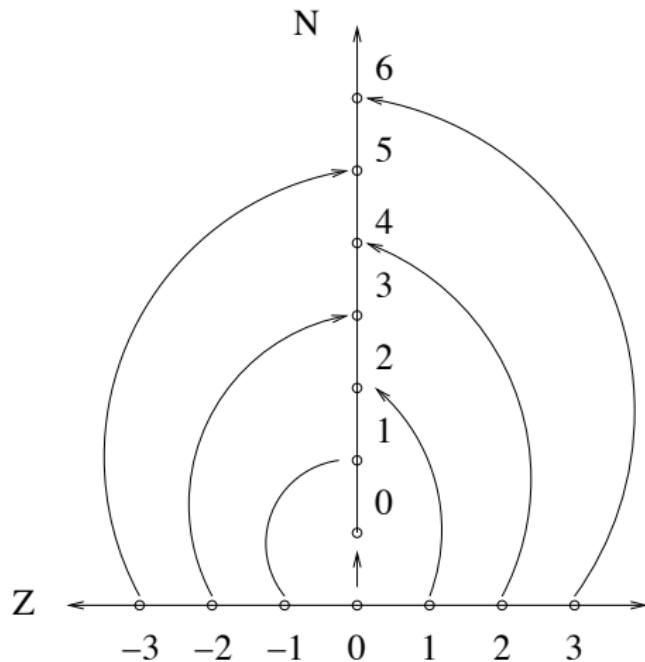
Mateixa cardinalitat

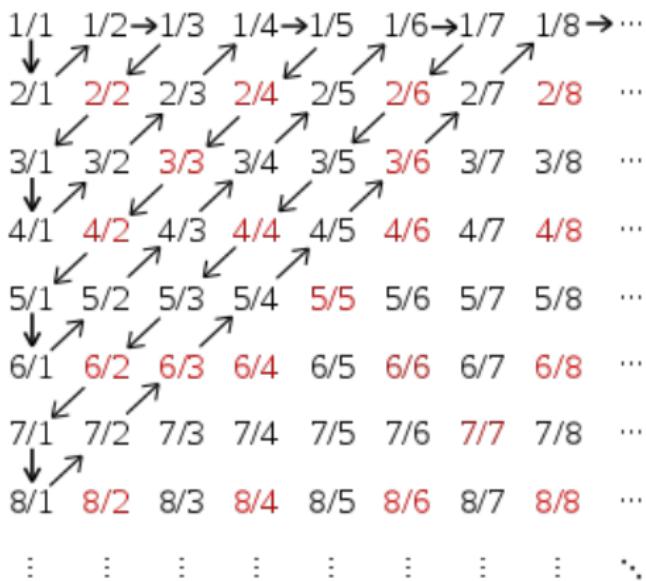
Donats dos conjunts A i B , $|A| = |B|$ si existeix una biecció $f : A \rightarrow B$.

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?

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?

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?

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.

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.

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

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

Sigui $r_i = 0, x_{i0}x_{i1}x_{i2} \dots$ 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 $r = 0, y_0y_1y_2 \dots$

Llavors, $r \neq r_i$ perquè difereixen en l' i -èssim lloc decimal.

Contradicció: $r \in (0, 1)$ però no és a la llista.

1891: Argument diagonal de Cantor

\mathbb{R} no és enumerable

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

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

Sigui $r_i = 0, x_{i0}x_{i1}x_{i2} \dots$ 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 $r = 0, y_0y_1y_2 \dots$

Llavors, $r \neq r_i$ perquè difereixen en l' i -èssim lloc decimal.

Contradicció: $r \in (0, 1)$ però no és a la llista.

1891: Argument diagonal de Cantor

\mathbb{R} no és enumerable

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

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

Sigui $r_i = 0, x_{i0}x_{i1}x_{i2} \dots$ 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 $r = 0, y_0y_1y_2 \dots$

Llavors, $r \neq r_i$ perquè difereixen en l' i -èssim lloc decimal.

Contradicció: $r \in (0, 1)$ però no és a la llista.

1891: Argument diagonal de Cantor

\mathbb{R} no és enumerable

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

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

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

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

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

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 $r = 0,77373\dots$

\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 $r = 0,77373\dots$

$\mathcal{P}(\mathbb{N})$ 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.

$\mathcal{P}(\mathbb{N})$ 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} ?

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} ?

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>

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>

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>

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

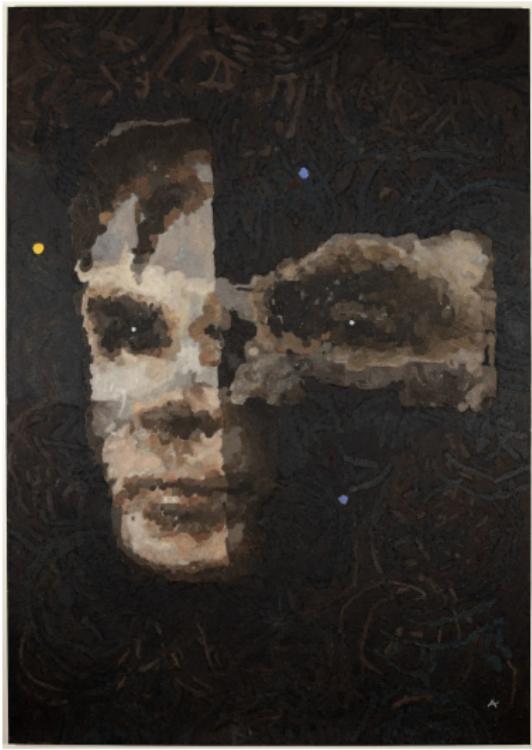
How Many Numbers Exist? Infinity Proof Moves Math Closer to an Answer.

a <https://www.quantamagazine.org>

Màquines de Turing

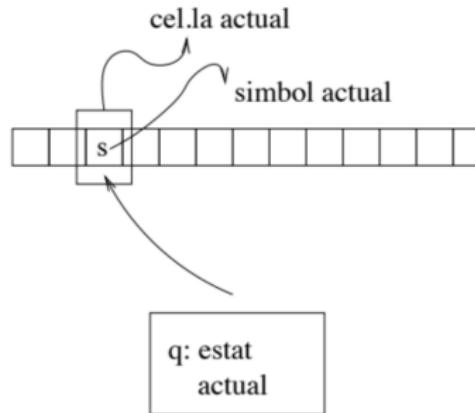
- 1 Introducció
- 2 Teoria de conjunts
- 3 La màquina de Turing
- 4 Problemes indecidibles

Alan Turing (Londres 1912 – Cheshire 1954)



Màquina de Turing

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



Una **màquina de Turing** (TM) és un sèxtuple $(Q, \Sigma, \Gamma, \delta, q_0, q_{acc})$, on

- Q és un conjunt finit (d'estats) i $q_0, q_{acc} \in Q$
- Σ i Γ són alfabets (Σ d'entrada, $\Gamma \supseteq \Sigma$ de cinta)
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{E, D, N\}$

Màquina de Turing

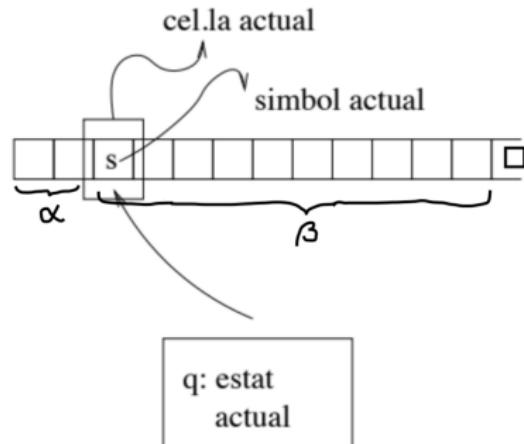
El **funcionament** d'una TM es pot dividir en 3 fases:

- ① **Inici.** La cinta conté \triangleright , seguit de l'entrada, seguida d'infinitis blancs (\square).
- ② **Pas de càlcul.** En funció de l'estat i el símbol actuals,
 - ① canvia l'estat actual,
 - ② sobreescriu un nou símbol en la cel·la actual i
 - ③ pot moure el capçal (E: esquerra, D: dreta, N: no moure'l).
- ③ **Final.** S'atura quan no hi ha transició definida o es vol moure el capçal a l'esquerra de la primera cel·la. Si s'atura en
 - q_{acc} , **accepta** l'entrada
 - $q \neq q_{acc}$, **rebutja** l'entrada

Màquina de Turing

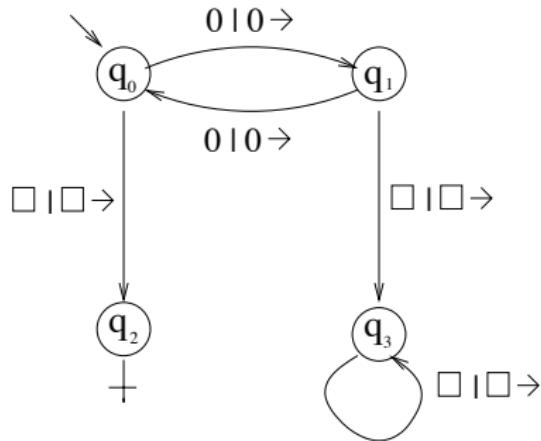
Per formalitzar el funcionament de la TM es defineix el concepte de **configuració**: la informació necessària per reconstruir la situació d'una TM (i poder-la simular), per exemple, el mot $\alpha q \beta$ indica que

- el contingut de la cinta és $\alpha \beta$
- l'estat actual és q
- el capçal apunta al primer símbol de β



Màquina de Turing

Màquina de Turing: nombre parell de 0's



Llenguatge reconegut

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.

Diem que $L(M) = \{x \mid M \text{ accepta } x\}$ és el **llenguatge reconegut** per M .

Notació

$M(x) \downarrow$: 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 $\forall x \in \Sigma^* M(x) \downarrow$.

Llenguatge reconegut

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.

Diem que $L(M) = \{x \mid M \text{ accepta } x\}$ és el **llenguatge reconegut** per M .

Notació

$M(x) \downarrow$: 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 $\forall x \in \Sigma^* M(x) \downarrow$.

Llenguatge reconegut

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.

Diem que $L(M) = \{x \mid M \text{ accepta } x\}$ és el **llenguatge reconegut** per M .

Notació

$M(x) \downarrow$: 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 $\forall x \in \Sigma^* M(x) \downarrow$.

Llenguatge reconegut

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.

Llenguatge reconegut

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.

Llenguatge reconegut

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.

Llenguatge reconegut

Codificació de les TM

- Les TM es poden codificar com a mots sobre $\{0, 1\}$.
- Hi ha una biecció 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 .

Llenguatge reconegut

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.

Llenguatge reconegut

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.

Funció computada

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 φ_i .

Funció computada

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

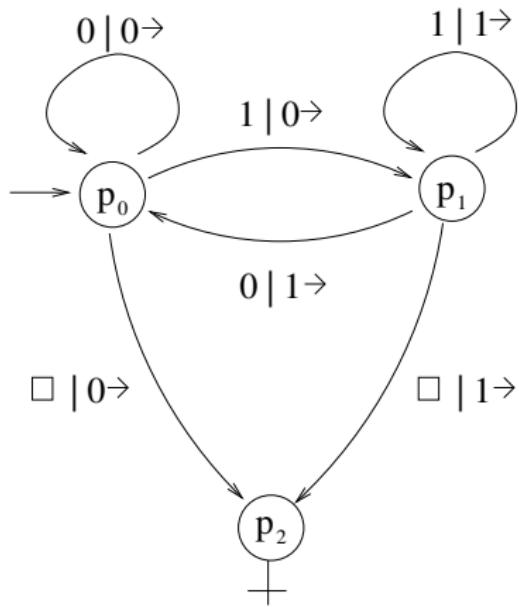
Notació

La **funció computada** per la màquina M_i es representa amb φ_i .

Funció computada

Exemple

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



Tesi de Church-Turing

Al 1900, David Hilbert va proposar 23 problemes matemàtics com a repte per al nou segle. El 10è tenia a veure amb algorismes.

Una equació diofàntica és una equació amb coeficients enters, com ara

$$3x^2 - 2xy - y^2z - 7 = 0 \quad (1)$$

$$x^2 + y^2 + 1 = 0 \quad (2)$$

(1) té arrels enteres $x = 1, y = 2, z = -2$, però (2) no té solució entera.

Tesi de Church-Turing

Al 1900, David Hilbert va proposar 23 problemes matemàtics com a repte per al nou segle. El 10è tenia a veure amb algorismes.

Una **equació diofàntica** és una equació amb coeficients enters, com ara

$$3x^2 - 2xy - y^2z - 7 = 0 \quad (1)$$

$$x^2 + y^2 + 1 = 0 \quad (2)$$

(1) té arrels enteres $x = 1, y = 2, z = -2$, però (2) no té solució entera.

Tesi de Church-Turing

El **10è problema de Hilbert** consisteix a trobar un algorisme per decidir si una equació diofàntica té solució entera. Però Hilbert va demanar trobar

un procés d'acord amb el qual es pugui determinar en un nombre finit d'operacions si una equació diofàntica té solució entera

La definició que es buscava era la de la idea d'algorisme, que va aparèixer en articles de 1936 d'Alonzo Church (λ -càlcul) i Alan Turing (TM).

Yuri Matijasevič finalment demostra al 1970 que el problema és irresoluble.

Tesi de Church-Turing

El **10è problema de Hilbert** consisteix a trobar un algorisme per decidir si una equació diofàntica té solució entera. Però Hilbert va demanar trobar

un procés d'acord amb el qual es pugui determinar en un nombre finit d'operacions si una equació diofàntica té solució entera

La definició que es buscava era la de la idea d'algorisme, que va aparèixer en articles de 1936 d'Alonzo Church (λ -càlcul) i Alan Turing (TM).

Yuri Matijasevič finalment demostra al 1970 que el problema és irresoluble.

Tesi de Church-Turing

Tesi de Church-Turing. *Qualsevol algorisme conceivable 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 construirem màquines de Turing sinó pseudocodi, sabent que es pot arribar a codificar com a TM.

Tesi de Church-Turing

Tesi de Church-Turing. *Qualsevol algorisme conceivable 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 construirem màquines de Turing sinó pseudocodi, sabent que es pot arribar a codificar com a TM.

Tesi de Church-Turing

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

Tesi de Church-Turing

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

Decidibilitat

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:

$$\kappa = \{i \mid M_i(i) \downarrow\}.$$

Màquines de Turing

- 1 Introducció
- 2 Teoria de conjunts
- 3 La màquina de Turing
- 4 Problemes indecidibles

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.

Problema de l'aturada

Conjectura dels primers bessons

Existeixen infinitos 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)

- 1 $p \leftarrow n$
- 2 mentre (**no PRIMER**(p)) o (**no PRIMER**($p + 2$))
- 3 $p \leftarrow p + 1$
- 4 **retornar** $p, p + 2$

Problema de l'aturada

Conjectura dels primers bessons

Existeixen infinitos 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)

- 1 $p \leftarrow n$
- 2 **mentre** (**no** PRIMER(p)) **o** (**no** PRIMER($p + 2$))
- 3 $p \leftarrow p + 1$
- 4 **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.

Problemes indecidibles

Teorema

κ 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 κ és semidecidible.

Aturada de les TM

| | 0 | 1 | 2 | 3 | 4 | ... |
|-------|---|---|---|---|---|-----|
| M_0 | ↑ | ↓ | ↓ | ↓ | ↑ | |
| M_1 | ↑ | ↓ | ↑ | ↑ | ↓ | |
| M_2 | ↓ | ↑ | ↑ | ↓ | ↓ | |
| M_3 | ↓ | ↓ | ↓ | ↑ | ↑ | |
| M_4 | ↑ | ↓ | ↑ | ↓ | ↓ | ... |

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 $M_k(k) \downarrow \Leftrightarrow M_k(k) \uparrow$.

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 $M_k(k) \downarrow \Leftrightarrow M_k(k) \uparrow$.

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

κ 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:

$N(x)$

- 1 **similar $M(x)$**
- 2 **si accepta**
- 3 **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!

Problemes indecidibles

Teorema

κ 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:

$N(x)$

- 1 **similar $M(x)$**
- 2 **si accepta**
- 3 **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!

Problemes indecidibles

Teorema

κ 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:

$N(x)$

- 1 **similar** $M(x)$
- 2 **si** accepta
- 3 **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!

Problemes indecidibles

Teorema

κ 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:

$N(x)$

- 1 **similar** $M(x)$
- 2 **si** accepta
- 3 **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 decidable, existiria una TM d'aturada segura M t.q. $L(M) = \text{HALT}$. Llavors, podríem definir la TM:

$N(i)$

- 1 **similar** $M(\langle i, i \rangle)$
- 2 **si** accepta
- 3 **acceptar**
- 4 **si** no
- 5 **rebutjar**

Per a tot x ,

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

N és una TM d'aturada segura que reconeix K , 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:

$N(i)$

- 1 **similar** $M(\langle i, i \rangle)$
- 2 **si** accepta
- 3 **acceptar**
- 4 **si no**
- 5 **rebutjar**

Per a tot x ,

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

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

Teorema

HALT és indecidible.

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

$N(i)$

- 1 **similar** $M(\langle i, i \rangle)$
- 2 **si** accepta
- 3 **acceptar**
- 4 **si no**
- 5 **rebutjar**

Per a tot x ,

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

N és una TM d'aturada segura que reconeix K , 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:

$N(i)$

- 1 **similar** $M(\langle i, i \rangle)$
- 2 **si** accepta
- 3 **acceptar**
- 4 **si no**
- 5 **rebutjar**

Per a tot x ,

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

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

Problemes indecidibles

Teorema

El complementari d'un llenguatge decidable és decidable.

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

$M'(x)$

- 1 **simular $M(x)$**
- 2 **si accepta**
- 3 **rebutjar**
- 4 **si no**
- 5 **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

El complementari d'un llenguatge decidable és decidable.

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

$M'(x)$

- 1 **simular** $M(x)$
- 2 **si** accepta
- 3 **rebutjar**
- 4 **si no**
- 5 **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 \bar{A} són semidecidibles.

⇒: Si A és decidible, pel teorema anterior (el tancament dels decidibles per complementari), \bar{A} és decidible.

La conclusió ara es deriva del fet que tot decidible és semidecidible.

Problemes indecidibles

Teorema (del complementari)

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

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

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

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

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

Problemes indecidibles

Definim la TM següent:

$N(x)$

1 $k = 0$

2 **repetir**

3 **simular** $M_A(x)$ i $M_{\bar{A}}(x)$ durant k passos

4 **si** $M_A(x)$ ha acceptat

5 **acceptar**

6 **si** $M_{\bar{A}}(x)$ ha acceptat

7 **rebutjar**

8 $k = k + 1$

9 **fins fals**

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

Problemes indecidibles

Teorema (del complementari)

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

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

Corol·lari

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

Problemes indecidibles

- **Llenguatges decidibles.** $\text{REC} = \{L \mid L \text{ és un llenguatge decidible}\}$, 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.** $\text{RE} = \{L \mid L \text{ és un llenguatge semidecidible}\}$, la classe que conté tots els llenguatges semidecidibles, com ara K, HALT, el llenguatge universal, el problema de la correspondència de Post, qualsevol llenguatge decidible o el conjunt d'enunciats d'affirmacions matemàtiques demostrables.

Problemes indecidibles

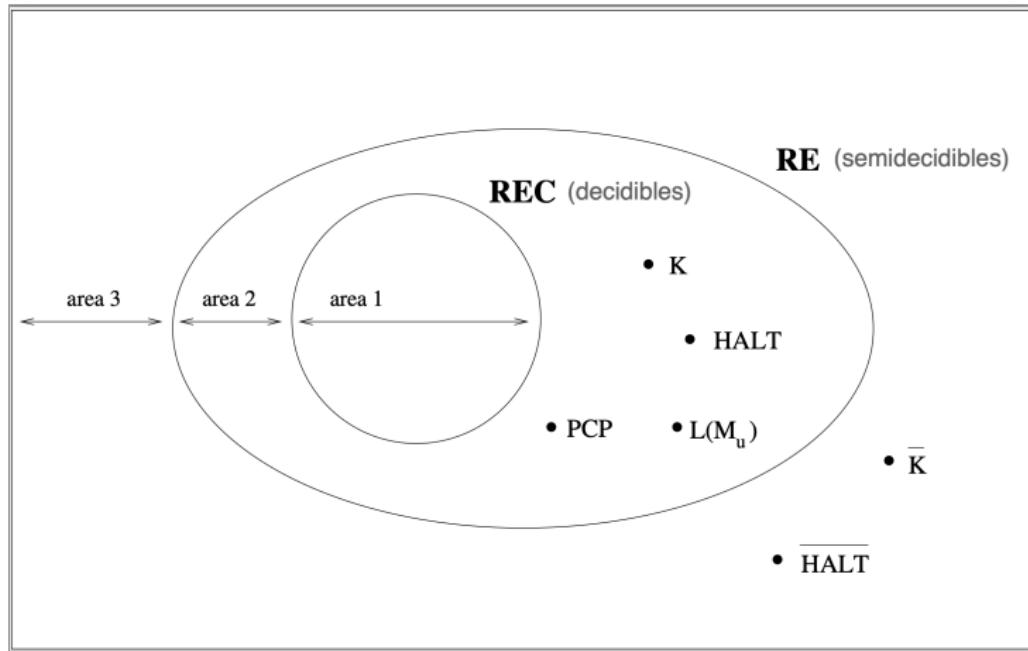


Figura: Classificació de problemes a RE i REC.