7. Indecidibilitat

Teoria de la Computació

FIB

Antoni Lozano

Q1 2024–2025

Indecidibilitat

Definició

Definició de reducció

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

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

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

Exemples

Paritat (1)

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 $\leq_m$ SENARS) amb una funció f tal que $f(x) = x + 1$. És evident que per a tot x:

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

Exemples

Paritat (1)

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 $\leq_m$ 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 $\leq_m$ PARELLS via f. En general, però, la relació $\leq_m$ no és simètrica.

Exemples

Paritat (1)

La funció $f(x) = x + 1$ no només és computable i total. També és computable en temps polinòmic, però això no es demana en les reduccions $\leq_m$.

Si volem demostrar $A \leq_m B$ i tenim potència de càlcul il·limitada, no cal que B tingui relació amb A. Només cal que no sigui trivial ($\neq \emptyset$ i $\neq \Sigma^*$) si A és decidible.

Exercici

Demostreu que si A és decidible i B no és trivial ($B \neq \emptyset$ i $B \neq \Sigma^*$), llavors $A \leq_m B$.

Exemples

Paritat (1)

La funció $f(x) = x + 1$ no només és computable i total. També és computable en temps polinòmic, però això no es demana en les reduccions $\leq_m$.

Si volem demostrar $A \leq_m B$ i tenim potència de càlcul il·limitada, no cal que B tingui relació amb A. Només cal que no sigui trivial ($\neq \emptyset$ i $\neq \Sigma^*$) si A és decidible.

Exercici

Demostreu que si A és decidible i B no és trivial ($B \neq \emptyset$ i $B \neq \Sigma^*$), llavors $A \leq_m B$.

Exemples

Paritat (2)

La funció característica d'un conjunt A es defineix com

$$\chi_A(x) = \begin{cases} 0, & \text{si } x \notin A \\ 1, & \text{si } x \in A \end{cases}$$

Per tant, $\chi_{\text{PARELLS}}(x) = 1$ si i només si x és parell, és a dir,

$$x \in \text{PARELLS} \Leftrightarrow \chi_{\text{PARELLS}}(x) \in \{1\}.$$

Com que χ_{PARELLS} és computable i total, tenim que, segons la definició de reducció,

$$\text{PARELLS} \leq_m \{1\}$$

mitjançant la funció de reducció χ_{PARELLS}.

Tancament dels decidibles

Teorema

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

Demostració (1)

Sigui M una TM que decideix B i f una funció de reducció que demostra $A \leq_m B$. Definim una TM N que decideix A:

$N(x)$

1 $y \leftarrow f(x)$
2 **simular** $M(y)$
3 **acceptar** $\Leftrightarrow M(y)$ accepta

Clarament,

$$N \text{ accepta } x \Leftrightarrow M \text{ accepta } y = f(x) \Leftrightarrow f(x) \in B \Leftrightarrow x \in A.$$

Per tant, $L(N) = A$. Com que N és d'aturada segura, decideix A.

Tancament dels decidibles

Observació

Un llenguatge L és decidible si i només si χ_L és computable.

Teorema

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

Demostració (2)

Suposem que f és una funció de reducció que demostra $A \leq_m B$.
Aleshores, són computables:

- f (per definició de reducció)
- χ_B (per l'observació anterior)

Però llavors $\chi_A = f \circ \chi_B = \chi_B(f(\cdot))$ és computable i, per tant, A és decidible.

Tancament dels decidibles

Corol·lari

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

Tancament dels decidibles

Corol·lari

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

Exemple 1: HALT és indecidible

Veiem que $\mathrm{K} \leq_m \mathrm{HALT}$. Definim la funció

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

que és computable i total. 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.

Com que K és indecidible, HALT també.

Tancament dels decidibles

Corol·lari

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

Exemple 2: $\mathrm{K} \leq_m \{p \mid \exists y \;\; M_p(y)\downarrow\}$

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 f computable total 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, $p \notin A$.

Tancament dels semidecidibles

Teorema

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

Demostració

Sigui M una TM que reconeix B i f una funció per la qual $A \leq_m B$.
Definim una TM N que reconeix A:

$N(x)$

1. $y \leftarrow f(x)$
2. **simular** $M(y)$
3. **acceptar** $\Leftrightarrow M(y)$ accepta

Clarament,

$$N \text{ accepta } x \Leftrightarrow M \text{ accepta } y = f(x) \Leftrightarrow f(x) \in B \Leftrightarrow x \in A.$$

Per tant, $L(N) = A$ i A és semidecidible. Notem que N no és d'aturada segura ($N(x)\!\uparrow \Leftrightarrow M(x)\!\uparrow$).

Tancament dels semidecidibles

Corol·lari

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

Tancament dels semidecidibles

Corol·lari

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

Exemple 1: $\overline{\mathrm{K}} \leq_m \{p \mid \forall y \;\; M_p(y)\downarrow\}$

Sigui $A = \{p \mid \forall y \;\; M_p(y)\downarrow\}$, el conjunt de codificacions de TMs d'aturada segura. Volem trobar f computable total t.q. $\forall x,\ x \in \overline{\mathrm{K}} \Leftrightarrow f(x) \in A$.

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

$M_p(y)$

1 **si** $M_x(x)$ s'atura en y passos
2 **bucle infinit**

Si $x \in \overline{\mathrm{K}}$, llavors $M_x(x)\uparrow$ i $M_p(y)\downarrow$ per a tot y (la condició del **si** és sempre falsa). Per tant, $p \in A$.

Si $x \notin \overline{\mathrm{K}}$, llavors $M_x(x)\downarrow$ i, per tant, $M_p(y)\uparrow$ per a algun y. Per tant, $p \notin A$.

Indecidibilitat

Teorema de Rice

El teorema de Rice proporciona un mètode alternatiu per demostrar la indecidibilitat.

En termes informals, afirma que un conjunt A no trivial (que no sigui el buit ni el total) és indecidible a condició que tracti d'una propietat que no sigui sintàctica.

Conjunts d'índexs

El teorema fa servir el concepte d'índex d'una funció f, que es refereix a qualsevol nombre de Gödel d'una TM que computa f. És a dir, k és un índex de la funció φ_k.

Definició

Sigui $A \subseteq \mathbb{N}$. Diem que A és un conjunt d'índexs si per a tot x, y tals que $x \in A$ i $\varphi_x = \varphi_y$, es compleix que $y \in A$.

Així, un conjunt és d'índexs si, per a cada funció, conté tots els seus índexs o no en conté cap.

Conjunt d'índexs

Exemple 1: $A = \{i \mid \forall j \;\; \varphi_i(j) = j\}$

A és un conjunt d'índexs. Si $x \in A$, llavors φ_x és la funció identitat.

Per a qualsevol y, si ara suposem que $\varphi_x = \varphi_y$, tenim que φ_y també és la funció identitat. Per tant, $y \in A$.

Conjunt d'índexs

Exemple 2: $B = \{i \mid \varphi_i(i) = i\}$

B **no** és un conjunt d'índexs:

1. Si $x \in B$, llavors $\varphi_x(x) = x$.
2. Per a qualsevol y, si suposem que $\varphi_x = \varphi_y$, podem assegurar que $\varphi_y(x) = x$, però caldria veure que $\varphi_y(y) = y$.

   Podem construir una *TM* amb codificació x_0 que computi la identitat fins a un valor constant $x_1 > x_0$ (per entrades més grans, entra en bucle). És a dir, per a tot $z \leq x_1$ tenim que $\varphi_{x_0}(z) = z$ i, en particular, $\varphi_{x_0}(x_0) = x_0$. Per tant, $x_0 \in B$.

   En canvi, existirà un nombre de Gödel $y > x_1$ tal que $\varphi_y = \varphi_x$ (tota TM té infinits nombres de Gödel). Però llavors $M_y(y)\uparrow$ perquè $y > x_1$. Per tant, $y \notin B$.

Conjunt d'índexs

Exemple 3: $\mathrm{K} = \{i \mid i \in \mathrm{Dom}(\varphi_i)\} = \{i \mid M_i(i)\downarrow\}$

K **no** és un conjunt d'índexs:

1. Si $x \in \mathrm{K}$, llavors $x \in \mathrm{Dom}(\varphi_x)$.
2. Per a qualsevol y, si suposem que $\varphi_x = \varphi_y$, podem assegurar que $x \in \mathrm{Dom}(\varphi_y)$, però caldria veure que $y \in \mathrm{Dom}(\varphi_y)$.

   El teorema de recursió assegura que existeix un x_0 tal que $\mathrm{Dom}(\varphi_{x_0}) = \{x_0\}$. Aleshores, per a $y \neq x_0$ tal que $\varphi_y = \varphi_{x_0}$, tenim que $y \notin \mathrm{K}$.

Teorema de Rice

Teorema (de Rice)

Sigui A un conjunt d'índexs. Llavors A és decidible si i només si $A = \emptyset$ o $A = \mathbb{N}$.

Demostració

Veure Serna *et al*.

Exemple: $A = \{i \mid \forall j \;\; \varphi_i(j) = j\}$

A és indecidible. Ja hem vist que és un conjunt d'índexs. A més:

- $A \neq \emptyset$ perquè la funció identitat és computable.
- $A \neq \mathbb{N}$ perquè hi ha funcions computables que no són la identitat.