

La MT com a model computacional

Es tracta d'estudiar els límits del que és computable basant-se en el model computacional de la MT.

Considerem la MT com un model de computació que es capaç de computar funcions definides sobre qualsevol domini

$$f : \mathcal{D} \longrightarrow \mathcal{R}$$

$$\langle x \rangle \quad \boxed{M} \quad \langle y \rangle$$

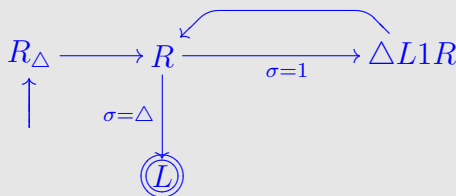
on $x \in \mathcal{D}$ i $y \in \mathcal{R}$.

$$f_M : \Gamma^* \longrightarrow \Gamma^*$$

és la funció de cadena associada a M .

MT com a MC: exemples

MT que suma dos enters:



Com que la potència d'una MT no depèn de la codificació utilitzada, es farà servir en cada cas la més convenient. Codificarem normalment els enters en **unari**

Altres exemples: multiplicar, restar, dividir, passar de unari a qualsevol altra base i al revés, etc.

Tesi de Church-Turing

Diem que una funció és (intuitivament) computable si existeix alguna forma metòdica i sistemàtica de calcular el valor d'aquesta funció per a tot valor del domini on està definida.

La idea de la MT captura d'alguna manera aquesta definició encara que, òbviament, no es pot donar cap demostració.

Se suposa com a certa l'anomenada tesi de Church-Turing:

Una funció és computable si i només si és Turing-computable

Una funció és Turing-computable si \exists una MT que calcula els seus valors (i para quan la entrada no pertany al seu domini).

Funcions Computables. Problemes Resolubles.

Diem que un problema és **resoluble** si \exists una funció computable que dona la solució correcta per a tota **instància** del problema.

Si ens restringim a problemes de decisió (equivalents a llenguatges) estem en el cas de funcions de la forma

$$f : \Gamma^* \longrightarrow \{0, 1\}$$

Aleshores es parla de problemes, funcions o llenguatges **decidibles**.

Exemple: Problema de l'anàlisi i funció característica d'un llenguatge.

Exemple: Donada G , és $L(G)$ buit?

Semi-decidibilitat

Es diu que un problema (de decisió) és **semi-decidible** si \exists una MT que dóna la resposta correcta quan és afirmativa però que pot no parar quan és negativa.



A nivell de llenguatges es té que

semi-decidible \Rightarrow r.e.

Semi-decidibilitat

Exemple:

$$L_r = \{w_i | w_i \in L(M_i)\}$$

$$f(w) = \begin{cases} 1 & \text{si } w \in L_r \\ 0 & \text{si } w \notin L_r \end{cases}$$

La funció f és χ_{L_r} , la funció característica de L_r .

f i L_r són semi-decidibles.

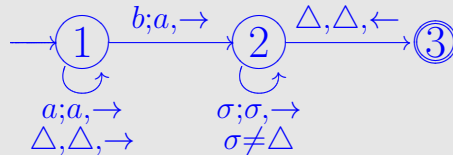
Indecidibilitat

És obvi que existeixen problemes irresolubles (indecidibles) com calcular la funció χ_{L_r} (o χ_{L_d}).

L'objectiu ara és donar un exemple de problema irresoluble no lligat (directament) a un llenguatge no recursiu.

El problema de la parada (P_P)

Donada una MT, M , i una cadena, w , ¿Pararà M amb w com a cadena d'entrada?



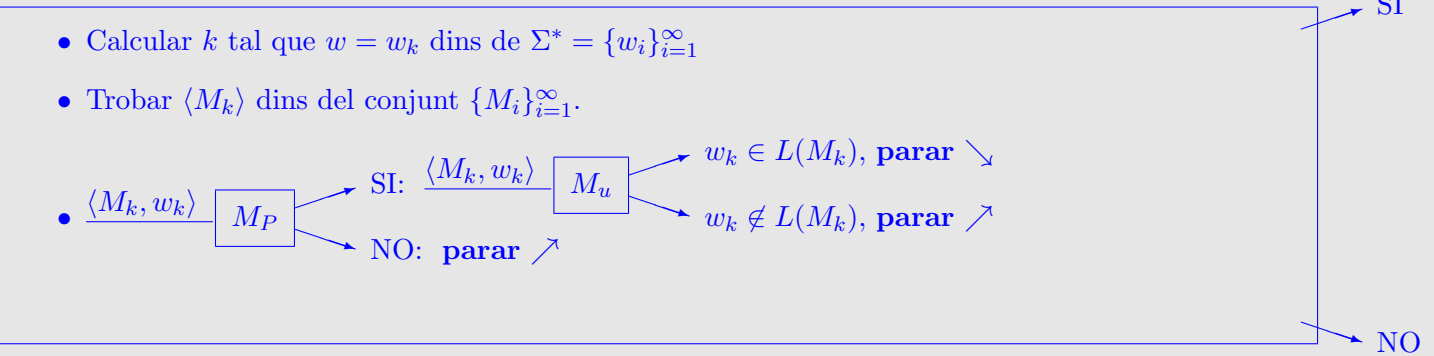
El P_P és indecidible

La demostració és per reducció a l'absurd i fa ús del fet que L_d és indecidible.

Suposem que el P_P és decidable, aleshores

$\langle M, w \rangle$ $\xrightarrow{M_P}$ SI (la màquina M amb entrada w arriba a una configuració de parada)

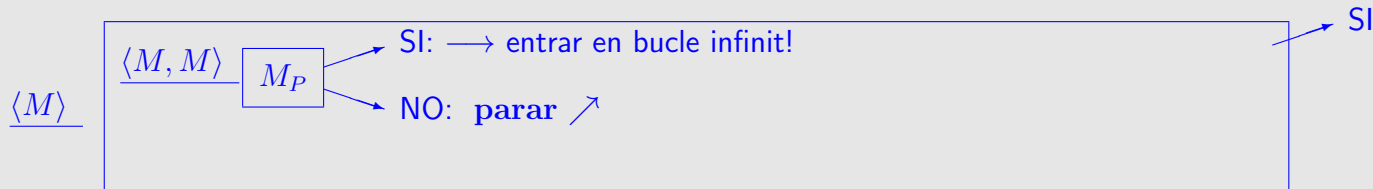
Si $\exists M_P$ es pot fer la següent construcció (MT que sempre para) que anomenarem M' .



Així definida, es té que $L(M') = L_d \implies L_d \in \mathcal{L}_{rec}$! IMPOSSIBLE.

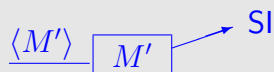
El P_P és indecidible fins i tot sense L_d !

Suposem que $\exists M_P$, i definim la construcció M'



M' serà potser absurda però està perfectament definida i funcionarà (parant o no) amb qualsevol entrada de la forma $\langle M \rangle$.

Per definició, M' PARA amb $\langle M \rangle \Leftrightarrow M$ NO PARA amb $\langle M \rangle$ $\boxed{\forall M!!}$. Aleshores si fem



tenim que passe el que passe entrem en contradicció!

Reducció entre problemes

Un problema P es redueix al problema Q si

- resoldre P es redueix (consisteix) a resoldre Q .
- la solució de Q implica la solució de P .
- Q resoluble $\implies P$ resoluble.
- P irresoluble $\implies Q$ irresoluble.

Ho escrivim com a $P \preceq Q$.

Si $P \preceq Q$ i $Q \preceq P$ aleshores es diu que P i Q són equivalents ($P \asymp Q$).

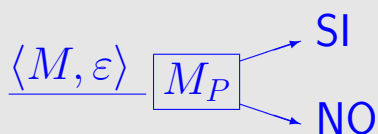
El Problema de la cinta en blanc

El problema de la cinta en blanc (P_Δ)

Donada una MT, M , ¿Pararà M quan comence amb la cinta en blanc?

- $P_\Delta \preceq P_P$?

Si, perquè si existira la MT M_P que resol P_P només caldria fer



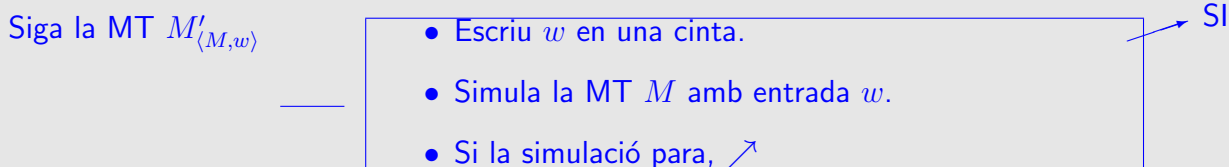
per saber si qualsevol M para o no amb la cinta en blanc.

- $P_P \preceq P_\Delta$? Ara no és tan senzill!

Si, si, però... $P_P \preceq P_\Delta$!?

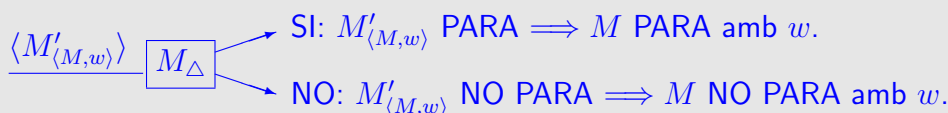
Cal demostrar que la solució de P_Δ implica la de P_P .

O siga, suposant la existència de la MT M_Δ que resol el P_Δ s'ha de conseguir solucionar el P_P per a qualsevol entrada de la forma $\langle M, w \rangle$.



Aquesta MT són en realitat moltes MT (tantes com possibles parelles (M, w)). Cada, $M'_{\langle M, w \rangle}$ està ben definida i per tant existeix la seua codificació.

El P_P es pot resoldre doncs $\forall M, w$ fent



Aleshores, $P_P \preceq P_\Delta$ i, per tant P_Δ és indecidable (per ser-ho P_P)

El Problema Universal

El problema universal (P_U)

Donada una MT, M , i una cadena, w , ¿ $w \in L(M$?

Llenguatge associat a P_U : $L_U = \{\langle M, w \rangle | w \in L(M)\}$

- És obvi que $P_U \preceq P_P$. (sabent que una MT para, es pot fer una simulació)
- $P_P \preceq P_U$?

es pot demostrar de dues formes ... EXERCICI

... el P_U és **indecidible**

En realitat P_U només és semi-decidible

¿Existeix una MT M_U que, donade qualssevol M i w conteste SI quan $w \in L(M)$? (quan $w \notin L(M)$ ens dóna igual el que faça la MT)

$\langle M, w \rangle$ M_U → SI

Aquesta MT és (en aquest cas) exactament la MT universal que simula qualsevol M amb qualsevol cadena d'entrada.

Com que M_U existeix, P_U és **semi-decidible**.

O, el que és el mateix, L_U és r.e. i no recursiu.

També són semi-decidibles P_P i P_Δ (es poden fer raonaments similars).

El teorema de Rice

Qualsevol propietat (no trivial) per als llenguatges r.e. és indecidible

És a dir, no es pot construir una MT que, donat qualsevol L r.e., conteste si L compleix la propietat o no.

- Propietat: predicat associat a un llenguatge. Queda caracteritzada pel conjunt de llenguatges que la compleixen, $\mathcal{P} \subseteq 2^{\Sigma^*}$.
- Una propietat \mathcal{P} és **trivial** si $\mathcal{P} = \emptyset$ o si $\mathcal{P} = \mathcal{L}$ (família considerada).
- “donat L ” significa que es té una descripció **finita** de L (normalment la codificació de la MT que l'accepta) que és l'entrada a una MT.

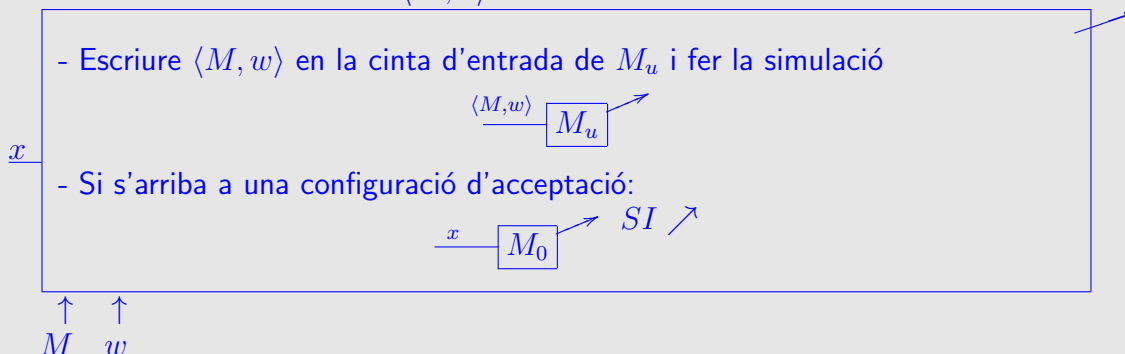
El teorema de Rice. Enunciat

Siga $\mathcal{P} \subseteq \mathcal{L}_{re}$, $\mathcal{P} \neq \emptyset$ i $\mathcal{P} \neq \mathcal{L}_{re}$, aleshores \mathcal{P} és indecidible.

Demostració: Suposem que existeix $\langle M \rangle \xrightarrow{M_{\mathcal{P}}} \begin{cases} L \in \mathcal{P} \\ L \notin \mathcal{P} \end{cases}$

suposem que $\emptyset \notin \mathcal{P}$ (altrament considerem $\overline{\mathcal{P}}$) i siga $L_0 = L(M_0) \in \mathcal{P}$.

Considerem la MT $M'_{\langle M, w \rangle}$:

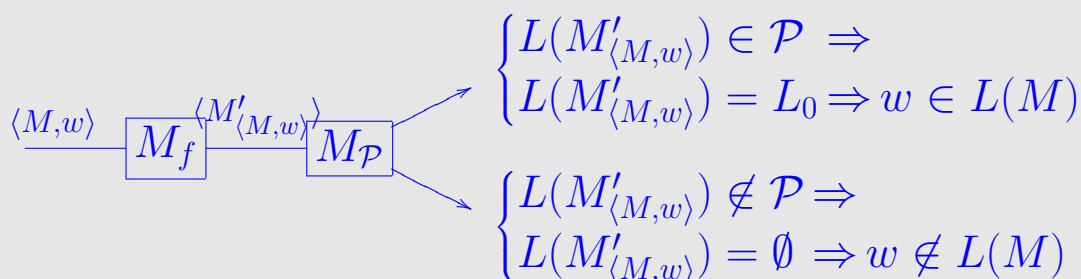


El teorema de Rice. Enunciat

Segons aquesta descripció es compleix que

$$L(M'_{\langle M, w \rangle}) = \begin{cases} L_0 & \text{si } w \in L(M) \\ \emptyset & \text{si } w \notin L(M) \end{cases}$$

Per tant, si anomenem M_f la MT que calcula $M'_{\langle M, w \rangle}$ a partir de $\langle M, w \rangle$ es té que



El problema de la correspondència de Post

Anomenem sistema de correspondència de Post (SCP) dues seqüències de k cadenes de Σ^+ .

$$A = \{u_1, \dots, u_k\}, \quad B = \{v_1, \dots, v_k\}$$

Es diu que un SCP té solució si existeix una seqüència d'índexs, i_1, \dots, i_m ($m \geq 1$) tal que

$$u_{i_1} u_{i_2} \cdots u_{i_m} = v_{i_1} v_{i_2} \cdots v_{i_m}$$

Per exemple, el SCP format per $A = \{a, abaaa, ab\}$ i $B = \{aaa, ab, b\}$ té una solució que ve donada per la seqüència $(2, 1, 1, 3)$.

$$abaaa \cdot a \cdot a \cdot ab = u_2 u_1 u_1 u_3 = v_2 v_1 v_1 v_3 = ab \cdot aaa \cdot aaa \cdot b$$

El problema de la correspondència de Post

Un SCP gràficament,

1	2	...	k
u_1	u_2	...	u_k
v_1	v_2	...	v_k

L'exemple anterior i la seua solució:

1	2	3
a	$abaaa$	ab
aaa	ab	b

2	1	1	3
$abaaa$	a	a	ab
ab	aaa	aaa	b

El problema de la correspondència de Post

Un altre exemple sense solució:

1	2	3
ab	baa	aba
aba	aa	baa

1	3	3	...
ab	aba	aba	...
aba	baa	baa	...

El problema de la correspondència de Post

Problema de la correspondència de Post (P_{CP})

Dades: Un SCP, $\{u_1, \dots, u_k\}, \{v_1, \dots, v_k\}$

Enunciat: Existeix una solució per al SCP de la forma

$$i_1, \dots, i_m \quad (m \geq 1)?$$

El problema de la correspondència de Post

Problema de la correspondència de Post modificat (P_{CPM})

Dades: Un SCP, $\{u_1, \dots, u_k\}, \{v_1, \dots, v_k\}$

Enunciat: Existeix solució per al SCP de la forma

$$1, i_2, \dots, i_m \quad (m \geq 1)?$$

El P_{CP} és equivalent al P_{CPM}

$$P_{CP} \preceq P_{CPM}$$

més fàcil

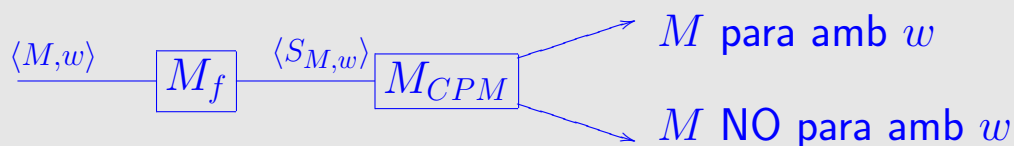
$$P_{CPM} \preceq P_{CP}$$

???

El Problema de Post és indecidible

La demostració consisteix en fer $P_P \preceq P_{CPM}$

A partir de qualsevol MT M i qualsevol cadena w , construïrem un SCP, $S_{M,w}$ de tal manera que



SCP corresponent a M i w

$$\begin{array}{c}
 \begin{array}{|c|} \hline 1 \\ \hline \end{array} \quad \begin{array}{|c|} \hline 2 \\ \hline \end{array} \quad \dots \\
 \begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline \sigma \\ \hline \end{array} \\
 \hline
 \begin{array}{|c|} \hline \$q_1w\$ \\ \hline \end{array}, \begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline \sigma \\ \hline \end{array} \quad \forall \sigma \in \Gamma. \\
 \\
 \text{si } \delta(q, \sigma) = (p, \tau, \rightarrow), \quad \begin{array}{|c|} \hline q\sigma \\ \hline \tau p \\ \hline \end{array}. \\
 \\
 \text{si } \delta(q, \sigma) = (p, \tau, \leftarrow), \quad \begin{array}{|c|} \hline \gamma q\sigma \\ \hline p\gamma\tau \\ \hline \end{array} \quad \forall \gamma \in \Gamma. \\
 \\
 \text{si } \delta(q, \Delta) = (p, \tau, \rightarrow), \quad \begin{array}{|c|} \hline q\$ \\ \hline \tau p\$ \\ \hline \end{array}. \\
 \\
 \text{si } \delta(q, \Delta) = (p, \tau, \leftarrow), \quad \begin{array}{|c|} \hline \gamma q\$ \\ \hline p\gamma\tau\$ \\ \hline \end{array} \quad \forall \gamma \in \Gamma. \\
 \\
 \begin{array}{|c|} \hline \sigma q\tau \\ \hline q \\ \hline \end{array}, \begin{array}{|c|} \hline \sigma q\$ \\ \hline q\$ \\ \hline \end{array}, \begin{array}{|c|} \hline \$q\tau \\ \hline \$q \\ \hline \end{array}, \begin{array}{|c|} \hline q\$\$ \\ \hline \$ \\ \hline \end{array} \quad \forall q \in F, \forall \sigma, \tau \in \Gamma.
 \end{array}$$

Equivalència entre computacions i solucions del SCP

$$\begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline q_1\sigma_1 \\ \hline \tau q_2 \\ \hline \end{array} \quad \begin{array}{|c|} \hline \sigma_2 \\ \hline \underline{\sigma}_2 \\ \hline \end{array} \quad \dots \quad \begin{array}{|c|} \hline \sigma_k \\ \hline \underline{\sigma}_k \\ \hline \end{array} \quad \begin{array}{|c|} \hline \$ \\ \hline \$ \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline q_1\sigma_1 \cdots \sigma_k\$ \\ \hline \tau q_2\sigma_2 \cdots \sigma_k\$ \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline \$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline q_1w\$ \\ \hline \alpha_1q_{i_1}\beta_1\$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline \alpha_{n-1}q_{i_{n-1}}\beta_{n-1}\$ \\ \hline \alpha_nq_{i_n}\beta_n\$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline ..\$ \\ \hline q_{i_n}\$ \\ \hline \end{array} \quad \begin{array}{|c|} \hline q_{i_n}\$\$ \\ \hline \$ \\ \hline \end{array}$$

Problemes sobre gramàtiques

Problema de la intersecció buida, P_{IB}

Dades:

Dues gramàtiques incontextuals, $G_A = \langle \Sigma, N_A, P_A, S_A \rangle$ i $G_B = \langle \Sigma, N_B, P_B, S_B \rangle$.

Enunciat: $L(G_A) \cap L(G_B) = \emptyset$?

Problemes sobre gramàtiques

$P_{CP} \preceq P_{IB}$

Siga $A = \{u_1, \dots, u_k\}$ i $B = \{v_1, \dots, v_k\}$ un SCP qualsevol sobre Σ . (que voldrem resoldre), i siga $\Delta = \{a_1, \dots, a_k\}$, $\Sigma \cap \Delta = \emptyset$. Definim

$$G_A = \langle \{S_A\}, \Sigma \cup \Delta, S_A, \{S_A \rightarrow u_i S_A a_i \mid u_i a_i, i = 1, \dots, k\} \rangle$$

$$G_B = \langle \{S_B\}, \Sigma \cup \Delta, S_B, \{S_B \rightarrow v_i S_B a_i \mid v_i a_i, i = 1, \dots, k\} \rangle$$

$L(G_A)$ (o $L(G_B)$) està format per seqüències de "blocs" de A (o B) seguides per la mateixa seqüència invertida de símbols corresponents de Δ . Aleshores,

$$\begin{aligned} \exists i_1, \dots, i_n : \\ u_{i_1} \dots u_{i_n} = v_{i_1} \dots v_{i_n} \end{aligned} \iff \begin{aligned} \exists x \in L(G_A) \cap L(G_B) \wedge \\ x = u_{i_1} \dots u_{i_n} a_{i_1} \dots a_{i_n} = v_{i_1} \dots v_{i_n} a_{i_1} \dots a_{i_n} \end{aligned}$$

Com que P_{CP} és indecidible, P_{IB} també!

Problemes sobre gramàtiques

Problema de la ambigüitat d'una gramàtica, P_{AG}

Dades: Una gramàtica incontextual, $G_A = \langle \Sigma, N_A, P_A, S_A \rangle$.

Enunciat: És G_A ambigua?

Problemes sobre gramàtiques

$P_{CP} \preceq P_{AG}$

Siga $A = \{u_1, \dots, u_k\}$ i $B = \{v_1, \dots, v_k\}$ un SCP qualsevol sobre Σ . (que voldrem resoldre), i siga $\Delta = \{a_1, \dots, a_k\}$, $\Sigma \cap \Delta = \emptyset$. Definim $G = \langle \{S, S_A, S_B\}, \Sigma \cup \Delta, S, P \rangle$ on P és

- $S \rightarrow S_A | S_B$
- $S_A \rightarrow u_i S_A a_i | u_i a_i, i = 1, \dots, k.$
- $S_B \rightarrow v_i S_B a_i | v_i a_i, i = 1, \dots, k.$

Aleshores

$$\begin{aligned} S \Rightarrow S_A &\stackrel{*}{\Rightarrow} w_A = u_{i_1} u_{i_2} \cdots u_{i_n} a_{i_n} \cdots a_{i_1} \\ S \Rightarrow S_B &\stackrel{*}{\Rightarrow} w_B = v_{i_1} v_{i_2} \cdots v_{i_n} a_{i_n} \cdots a_{i_1} \end{aligned}$$

G ambigua $\iff \exists w_A = w_B \iff (A, B)$ té solució.

El llenguatge de les computacions d'una MT

Donada $M = \langle Q, \Sigma, \Gamma, \delta, q_0, \Delta, F \rangle$, una computació

$$q_0 w \vdash_M x_1 \vdash_M \cdots \vdash_M x_n$$

on $x_i \in \Gamma^* Q \Gamma^*$ i $w \in \Sigma^*$ s'anomena **vàlida** si x_n és una configuració d'acceptació (i de parada).

Codifiquem les computacions com a cadenes sobre $\Gamma \cup Q \cup \{\$\}$:

$$q_0 w \$ x_1^{-1} \$ x_2 \$ x_3^{-1} \cdots \$ x_n \$$$

definim el llenguatge de les computacions vàlides de M com a:

$$L_M^v = \{ \langle c \rangle \in (\Gamma \cup Q \cup \{\$\})^* \mid c \text{ és vàlida} \}$$

El llenguatge de les computacions d'una MT

Teorema: L_M^v és co-incontextual

Demostrarem que $L_M^v = L_1 \cap L_2 \cap L_3 \cap L_4 \cap L_5$, on els $\overline{L_i}$ són incontextuals.

$$(\overline{L_M^v} = \overline{L_1} \cup \cdots \cup \overline{L_5}, \text{unió d'incontextuals})$$

$$L_1 = (\Gamma^* Q \Gamma^* \$)^+, \text{ regular, } \overline{L_1} \text{ regular} \Rightarrow \text{incontextual}$$

$$L_2 = q_0 \Sigma^* \$ \Delta^*, \text{ idem}$$

$$L_3 = \Delta^* \Gamma^* F \Gamma^* \$, \text{ idem}$$

$$L_4 = \{ z = y_0 \$ y_1 \$ \cdots \$ y_k \mid y_{2\ell} \vdash_M y_{2\ell+1}^{-1}, \ell = 0, 1, \dots, \lfloor \frac{k-1}{2} \rfloor \}$$

$$L_5 = \{ z = y_0 \$ y_1 \$ \cdots \$ y_k \mid y_{2\ell+1}^{-1} \vdash_M y_{2\ell+2}, \ell = 0, 1, \dots, \lfloor \frac{k-2}{2} \rfloor \}$$

El llenguatge de les computacions d'una MT

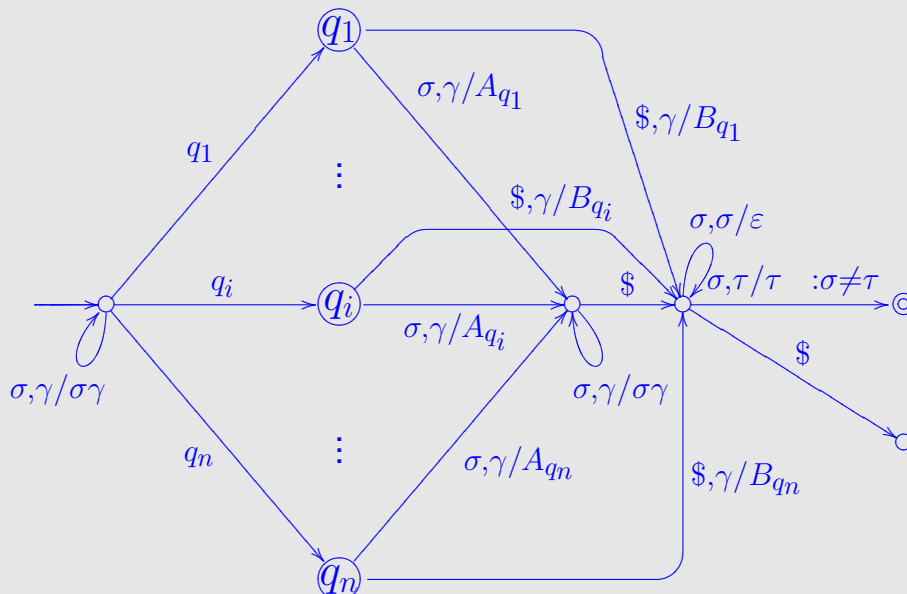
És incontextual $\overline{L_4}$?

Dues configuracions consecutives $y_{2\ell}$ i $y_{2\ell+1}$ han de complir:

$$\sigma_1 \cdots \sigma_{j-1} \underbrace{\sigma_j q \sigma_{j+1}} \sigma_{j+2} \cdots \sigma_\ell \vdash_M \left\{ \begin{array}{l} \sigma_1 \cdots \sigma_{j-1} \sigma_j \overbrace{\sigma' q'} \sigma_{j+2} \cdots \sigma_\ell \\ \quad \text{si } \delta(q, \sigma_{j+1}) = (q', \sigma', \rightarrow) \\ \sigma_1 \cdots \sigma_{j-1} \underbrace{q' \sigma_j \sigma'} \sigma_{j+2} \cdots \sigma_\ell \\ \quad \text{si } \delta(q, \sigma_{j+1}) = (q', \sigma', \leftarrow) \end{array} \right.$$

El llenguatge de les computacions d'una MT

Autòmat amb pila indeterminista que accepta $\overline{L_4}$



El llenguatge de les computacions d'una MT

$$A_{q_i} = \begin{cases} q'\gamma\sigma' & \text{si } \delta(q_i, \sigma) = (q', \sigma', \leftarrow) \\ \gamma\sigma'q' & \text{si } \delta(q_i, \sigma) = (q', \sigma', \rightarrow) \end{cases}$$

$$B_{q_i} = \begin{cases} q'\gamma\sigma' & \text{si } \delta(q_i, \Delta) = (q', \sigma', \leftarrow) \\ \gamma\sigma'q' & \text{si } \delta(q_i, \Delta) = (q', \sigma', \rightarrow) \end{cases}$$

És incontextual L_M^v ?

Sabem que és coincontextual. En principi, podria ser-ho o no.

Teorema: L_M^v incontextual $\iff L(M)$ és finit

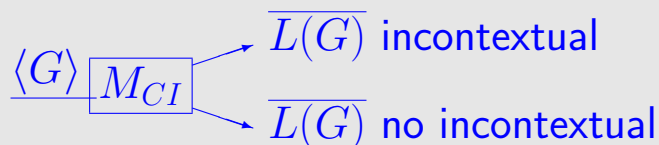
La demostració fa ús d'una generalització del lema del bombament per als incontextuals.

Es requereix, a més a més, que M efectue sempre almenys 3 moviments (no suposarà pèrdua de generalitat).

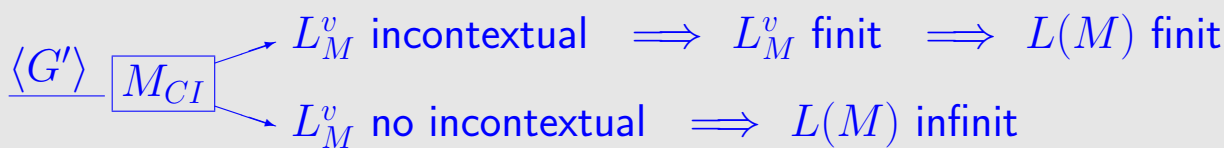
En resum L_M^v no és incontextual (llevat del cas trivial)!

Més problemes: És $\overline{L(G)}$ incontextual?

P_{CI} : És incontextual el complementari d'un incontextual?



Donada M construim G' tal que $\overline{L_M^v} = L(G')$ i aleshores



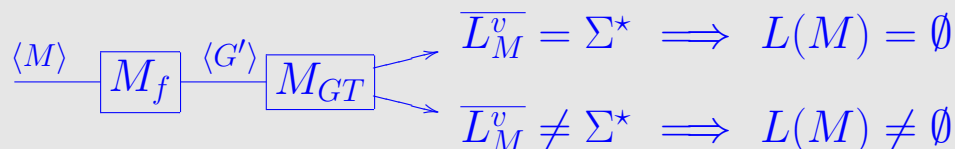
$L(M)$ finit és indecidible (T. Rice) $\implies P_{CI}$ indecidible

Més problemes: És G trivial?

Problema de la gramàtica genera-tot, P_{GT}

Dades: Una gramàtica incontextual, $G = \langle \Sigma, N, P, S \rangle$.

Enunciat: $L(G) = \Sigma^*$?



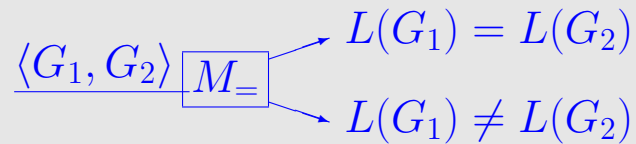
Donada una MT M es podria calcular la G' que genera les computacions **no** vàlides. M_{GT} ens diria aleshores si n'hi ha alguna vàlida o no, la qual cosa és equivalent a saber si $L(M)$ és buit.

Com que $L(M) = \emptyset$ és indecidible pel teorema de Rice, també ho serà P_{GT} .

Més problemes: Són iguals dos llenguatges incontextuals?

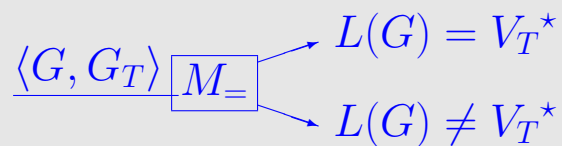
$P_=$: $L(G_1) = L(G_2)$?

Si fóra resoluble, existiria la MT:



Si $G_T = \langle V_T, V_N, \{S \rightarrow aS \mid \varepsilon : a \in V_T\}, S \rangle$, aleshores $L(G_T) = V_T^*$.

Donada qualsevol altra G podriem fer:



Per tant, $P_{GT} \preceq P_=$.

$P_=$ és indecidible per ser-ho P_{GT} .