Tema 6

Resolubilitat

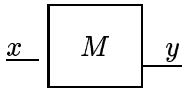
6.1 Resolució de problemes amb màquines de Turing

La màquina de Turing tal i com la va concebre el seu creador es pot veure com un dispositiu abstracte que pot representar qualsevol "computació" o qualsevol càlcul que puga fer qualsevol tipus de dispositiu manual, mecànic, automàtic o mental. Turing pensava en la cinta com una abstracció de la típica fulla (o, més bé, fulles) de paper que un matemàtic pot fer servir per demostrar teoremes o realitzar complicats càlculs matemàtics amb el corresponent ajut del famós llàpis i la goma d'esborrar (que són representats en la màquina mijantçant el capçal de lectura/escriptura).

Altres tipus i formes de càlcul també poden ser representats per la MT. En els computadors, per exemple, la cinta seria l'abstracció dels distints tipus de memòria interna i externa que es fan servir mentre que el capçal representaria la circuiteria que permet d'escriure, modificar i esborrar aquests tipus de memòria[1]

6.1.1 Funcions computables

En aquest capítol, la MT serà vista com un dispositiu que és capaç de calcular un resultat a partir d'una certa entrada.



Òbviament, i tractant-se d'una màquina de Turing, tant l'entrada x com el resultat y són cadenes d'un determinat alfabet. Per tant, podem veure tambe la màquina de Turing, M, com un dispositiu

[1] La correspondència entre la MT i altres abstraccions molt més pròximes als computadors i als programes serà establerta més endavant.

que es capaç de calcular una certa funció de la forma:

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

Per a tota cadena $x \in \Gamma^*$ la màquina M calcula el valor $f_M(x)$ definit com a

$$f_M(x) = y \text{ si i solament si } q_0 x \vdash_M^* qy$$

L'objectiu d'aquest capítol és l'estudi i la caracterització de les funcions que són computables o calculables i les que no ho són. El fet que s'estudien només les funcions definides sobre cadenes no representa cap pèrdua de generalitat en la pràctica ja que molts altres tipus de dades admeten una codificació en forma de cadenes.

Definició 6.1 *Una funció $f : \Gamma^* \longrightarrow \Gamma^*$ s'anomena* **Turing-computable** *si existeix una màquina de Turing, M, tal que $f = f_M$ per a tota cadena del domini de f.*

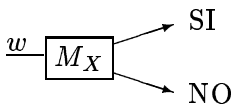
□

Hipòtesi de Church-Turing

6.1.2 Relació entre llenguatges i problemes

Si ens restringim al cas particular de problemes de decisió podem establir una relació directa entre problemes i llenguatges i, més important que això, entre la resolubilitat dels problemes i el tipus dels llenguatges.

Un problema de decisió es planteja en funció d'una certa entrada i la seua resolució consisteix en una decisió. És a dir, consisteix a respondre SI/NO, vertader/fals o 0/1. La solució a un problema de decisió, P_X, des del punt de vista de les MT es representaria com a.



En aquesta representació, la cadena w representa la codificació d'una instància del problema. Per tant, la resolubilitat del problema P_X i la calculabilitat de la funció $f_X : \Gamma^* \longrightarrow \{0,1\}$ estan directament relacionades.

Podem definir també el llenguatge L_X com a

$$L_X = \{w \in \Gamma^* | f_X(w) = 1\}$$

És a dir, L_X és el llenguatge del qual f_X és funció característica. Per tant, la resolubilitat del problema P_X, la calculabilitat de la funció f_X i la recursivitat del llenguatge L_X són la mateixa cosa.

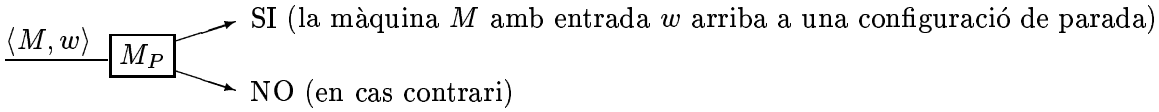
Com que hi ha llenguatges que són acceptats per MT que poden no parar, també hi haurà problemes per als quals es pot trobar una MT (o, de forma més general, un algorisme) que dóna la solució correcta quan aquesta és "SI". Aquests problemes (i els llenguatges a ells associats) reben el nom de **semi-decidibles**.

El problema de la parada, P_P

Dades: Una MT $M = \{Q, \Sigma, \Gamma, \delta, q_0, \triangle, F\}$ i una cadena $w \in \Sigma^*$.

Enunciat: Pararà la màquina M amb entrada w?

El problema de la parada serà resoluble si existeix una màquina de Turing M_P de la forma



Anem a considerar una instància particular del problema de la parada. Siga la següent MT:
...EXEMPLE...

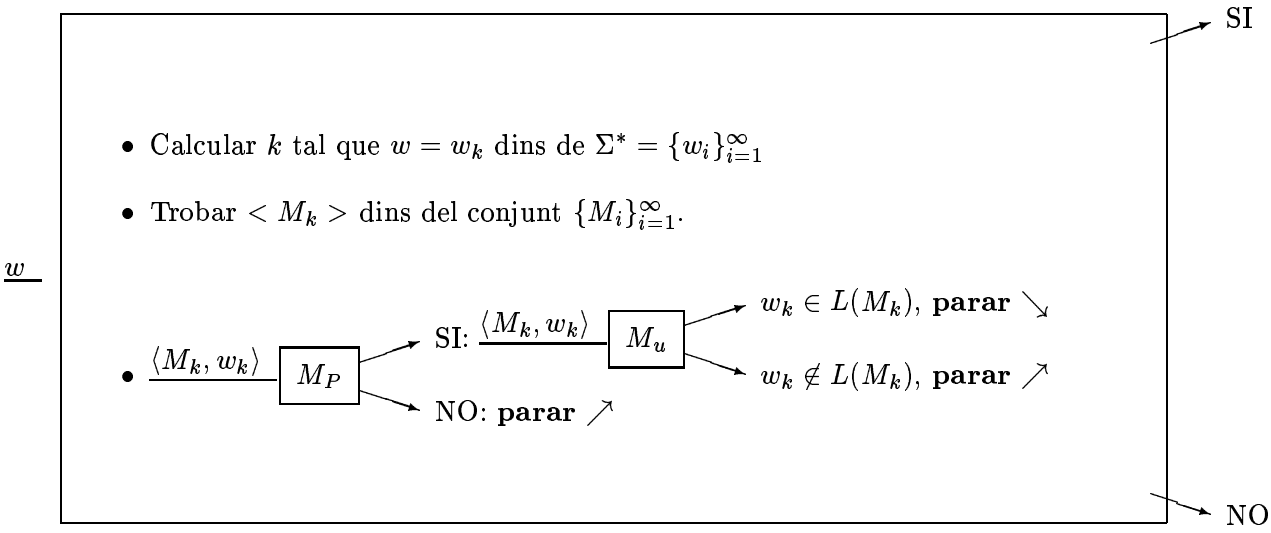
Després d'una inspecció de la MT arribem a la conclusió de que la MT sempre para si la cadena d'entrada conté un símbol b mentre que mai pararà quan la cadena no continga símbols b.

Hem resolt el problema de la parada per a qualsevol cadena però amb una MT concreta. Açò no vol dir que el problema en general siga resoluble. La pregunta és: es pot fer la mateixa anàlisi per a qualsevol MT?

Teorema 6.1 El problema de la parada és irresoluble

Prova:

Anem a suposar que la màquina M_P abans esmentada existeix. Aleshores, construirem la següent màquina que anomenarem M':



A partir d'una cadena w qualsevol, la màquina M' enumera el conjunt $\Sigma^* = \{w_i\}_{i=1}^{\infty}$ i troba el número d'ordre que li correspon a w dins d'aquest conjunt. A continuació enumera el conjunt de totes les màquines de Turing (enumerant totes les codificacions possibles) fins que troba la màquina

k-èsima.

La màquina M_P (que sempre ha de respondre) ens dirà si la màquina M_k amb entrada $w = w_k$ arriba o no a una configuració de parada. En cas afirmatiu, podem simular la computació corresponent mijantçant la màquina universal, M_u. Com a resultat sabrem si la cadena $w = w_k$ pertany o no a $L(M_k)$. En el cas que M_P ens diga que no s'arriba a cap configuració de parada, podem estar segurs de que $w_k \notin L(M_k)$.

La màquina M' així construida sempre arriba a una configuració de parada i, a més a més, només acceptarà aquelles cadenes $w = w_k$ que complesquen la condició $w_k \notin L(M_k)$. És a dir,

$$L(M') = \{w \mid w = w_k \ \wedge \ w_k \notin L(M_k)\} = L_d$$

O en altres paraules, la màquina M' accepta el llenguatge L_d que sabem que no és ni tan sols recursivament enumerable.

Arribem, per tant, a una contradicció per la qual cosa la suposició inicial sobre l'existència de la màquina M_P ha de ser necessàriament falsa. □

Teorema 6.2 El problema de la parada és semi-decidible.

Prova:

Només cal trobar una MT amb entrada $\langle M, w\rangle$ que pare per a tota màquina M i cadena w tal que M pare amb w com a entrada. Aquesta màquina no és altra que la màquina universal que simula la computació de M amb w. Quan aquesta simulació arriba a una configuració de parada (tant si és d'acceptació com si no) la màquina para i accepta. □

6.1.3 Reducció de problemes

Definició 6.2 *Diem que un problema P es* **redueix** *al problema Q (i s'escriu $P \preceq Q$) si la solució del problema Q implica la solució del problema P. És a dir,*

$$P \preceq Q \ \Leftrightarrow \ Q \textit{ decidible} \Rightarrow P \textit{ decidible}$$

També es pot dir que la solució de P es redueix a solucionar Q.

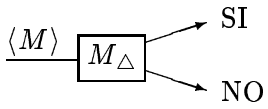
Com a conseqüència de la definició es dedueix

$$P \preceq Q \ \Leftrightarrow \ P \text{ indecidible} \Rightarrow Q \text{ indecidible}$$

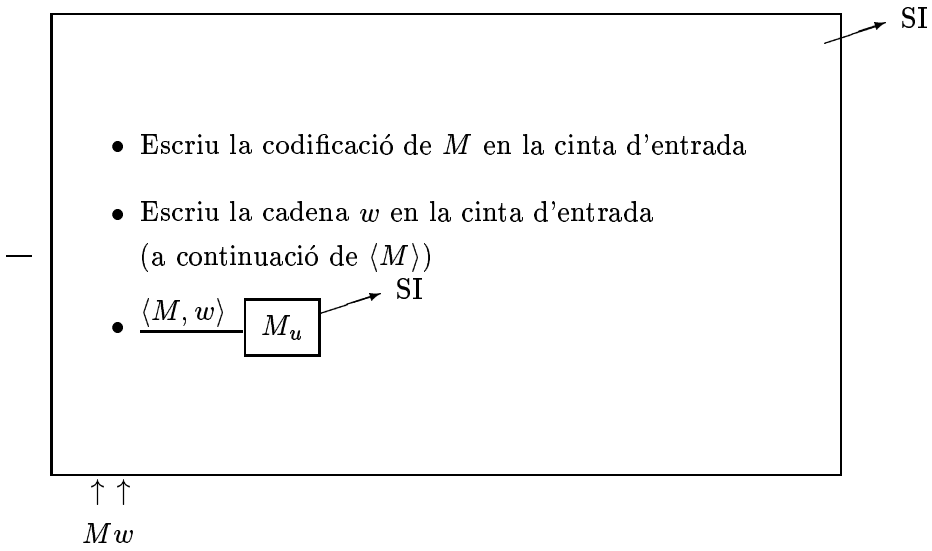
□

Exemple 6.1 *El problema de la cinta en blanc, $P_\triangle$, consisteix a saber si una determinada MT pararà o no si comença a funcionar amb la cinta d'entrada en blanc. Anem a demostrar que $P_P \preceq P_\triangle$.*

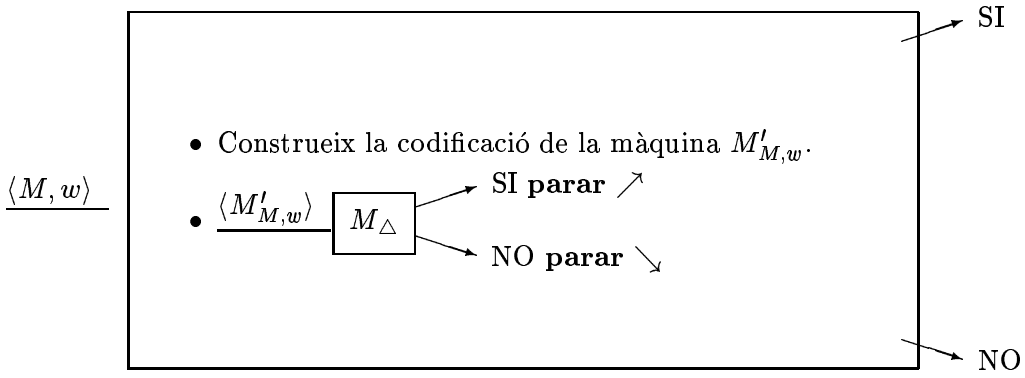
Suposem que $P_\triangle$ és resoluble. Aleshores existira una MT de la forma



A continuació construirem la màquina $M'_{M,w}$ que té com a paràmetres una màquina M i una cadena w qualssevol. Aquesta màquina, no pren cap entrada i comença a funcionar a partir d'una cinta en blanc.



És clar que la màquina $M'_{M,w}$ no té per què parar. Però, tal i com s'ha definit, aquesta màquina existeix i es pot codificar. Aleshores podem construir la següent MT



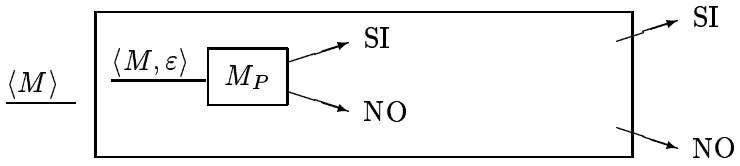
Aquesta MT sempre para i resol el problema de la parada amb entrades M i w. Com que la resolubilitat de $P_\triangle$ és condició necessària per a la resolubilitat de P_P, es dedueix que $P_P \preceq P_\triangle$.

□

Definició 6.3 *Dos problemes, P i Q, són* **equivalents** *si i solament si $P \preceq Q$ i $Q \preceq P$.*

□

Exemple 6.2 *El problema de la parada i el de la cinta en blanc són equivalents.*
Ja s'ha demostrat que $P_P \preceq P_\triangle$. La demostració de $P_\triangle \preceq P_P$ és trivial ja que la màquina



permetria resoldre $P_\triangle$ si P_P fóra resoluble.

□

6.2 Problemes irresolubles

6.2.1 El problema universal

6.2.2 El problema del llenguatge buit

6.2.3 El teorema de Rice

Siga $\mathcal{L}_{re}$ la classe dels llenguatges recursivament enumerables. Normalment una propietat d'un llenguatge és un predicat que pot ser vertader o fals per a un llenguatge determinat. Una propietat queda perfectament definida pel conjunt de llenguatges que la compleixen.

Definició 6.4 *Una* **propietat** *sobre $\mathcal{L}_{re}$ és un conjunt $\mathcal{P} \subseteq \mathcal{L}_{re}$. Si $L \in \mathcal{P}$ es diu que L compleix $\mathcal{P}$ i si $L \notin \mathcal{P}$ es diu que no la compleix. Una propietat $\mathcal{P}$ és* **no trivial** *si i solament si $\mathcal{P} \neq \emptyset \wedge \mathcal{P} \neq \mathcal{L}_{re}$.*

□

Donada una propietat $\mathcal{P}$ es defineix un llenguatge associat a $\mathcal{P}$ com

$$L_{\mathcal{P}} = \{\langle M \rangle \mid L(M) \in \mathcal{P}\}$$

Es diu que una propietat és decidible si existeix una MT que calcule el predicat associat. O, el que és el mateix, si existeix una MT, $M_{\mathcal{P}}$ tal que $L_{\mathcal{P}} = L(M_{\mathcal{P}})$.

Teorema 6.3 (Teorema de Rice) Tota propietat no trivial sobre $\mathcal{L}_{re}$ és indecidible.

□

6.2.4 El problema de la correspondència de Post

Definició 6.5 *Anomenem* **sistema de correspondència de Post** *(SCP) dues seqüències de k cadenes de Σ^+.*

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

Es diu que un SCP té solució si existeix una seqüència d'índexs, $i_1, \ldots, i_m$ $(m \geq 1)$ *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 $(2, 1, 1, 3)$.

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

Una forma més gràfica que veure un SCP es com k blocs formats per parells de cadenes de la forma

1	2	k
u_1	u_2	u_k
v_1	v_2	v_k

Aleshores, el SCP anterior seria:

1	2	3
a	$abaaa$	ab
aaa	ab	b

i la seua solució es pot veure com a

2	1	1	3
$ab\underline{aaa}$	$\underline{a}$	a	ab
ab	aaa	$aa\underline{a}$	b

Gràficament, la solució es pot veure com una concatenació de blocs de forma que van emparellant-se símbols dalt i baix. En aquesta representació, hem subratllat en cada bloc els símbols que no estan encara emparellats.

Considerem ara un altre SCP donat pels següents blocs:

1	2	3
ab	baa	aba
aba	aa	baa

Si intentem construir una solució per a aquest SCP, arribem a la conclusió que qualsevol seqüència d'índex ha de començar per 1 perque només u_1 i v_1 comparteixen prefixos. Com a conseqüència, es queda un símbol a desemparellat baix. L'únic bloc que es pot posar doncs a continuació és el 3, amb la qual cosa es torna a obtenir un símbol a desemparellat baix, i així successivament. Gràficament,

1	3	3	
ab	aba	aba	$\ldots$
$ab\underline{a}$	$ba\underline{a}$	$ba\underline{a}$	

En altres paraules, aquest SCP no té solució.

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

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

Enunciat: Existeix solució per al SCP de la forma $i_1, \dots i_m$ $(m \geq 1)$?

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

Anem a demostrar que els dos problemes són equivalents. Primer veurem que $P_{CP} \preceq P_{CPM}$ que és més fàcil encara que no trivial.

Si P_{CPM} fóra resoluble, donat qualsevol SCP sabríem si té solucio de la forma $1, \dots$. Per saber si el mateix SCP té o no solució en general només hauríem de resoldre k vegades el P_{CPM} col·locant l'i-èsim bloc en primera posició cada vegada.

La reducció en el sentit contrari no és tan fàcil ja que el fet de conéixer que el P_{CP} té solució no implica que aquesta es conega explícitament.

Teorema 6.4 $P_{CPM} \preceq P_{CP}$

Prova:

Ara suposem que P_{CP} és resoluble, per tant, donat un SCP podrem saber si existeix o no solució general.

Siga $A = \{u_1, \dots, u_k\}, B = \{v_1, \dots, v_k\}$ un SCP sobre Σ. Siguen $\sharp$ i \$ dos símbos que no estan en Σ.

Definim ara un nou SCP $A' = \{y_0, \dots, y_{k+1}\}, B' = \{z_0, \dots, z_{k+1}\}$ sobre $\Sigma \cup \{\sharp, \$\}$ on

$y_i = a_{i_1}\$a_{i_2}\$ \dots \$a_{i_{m_i}}\$$ si $u_i = a_{i_1}a_{i_2} \dots a_{i_{m_i}}$

$z_i = \$b_{i_1}\$b_{i_2}\$ \dots \$b_{i_{n_i}}$ si $v_i = b_{i_1}b_{i_2} \dots b_{i_{n_i}}$

$y_0 = \$y_1$, $y_{k+1} = \sharp$, $z_0 = z_1$, $z_{k+1} = \$\sharp$

Si P_{CP} és resoluble podrem saber si existeix una solució per a (A', B') i, aleshores tenim dos casos:

(A', B') **té solució:** Encara que no es conega la solució, és necessari (per construcció de A' i B' que els índexs primer i últim siguen 0 i $k+1$, respectivament. Com que els blocs de (A, B) i de (A', B') es corresponen exactament llevat dels separadors, es tindrà una solució per a (A,B) el primer índex de la qual serà 1.

(A', B') **no té solució:** En aquest cas és impossible que existesca una solució per a (A, B) que comence per l'índex 1 (encara que podria haver altres tipus de solucions).

Com a conclusió, hem sigut capaços de resoldre P_{CPM} mijantçant l'extensió del SCP corresponent i la (suposada) solució del P_{CP} sobre el SCP estés. □

Teorema 6.5 P_{CPM} és indecidible

Prova: Demostrarem que $P_P \preceq P_{CPM}$

Suposem que P_{CPM} és resoluble. Siga aleshores $M = (Q, \Sigma, \Gamma, \delta, \triangle, q_1, F)$ una MT de cinta semi-infinita que suposarem (sense pèrdua de generalitat) que només para en estats de F i entra en bucles infinits en qualsevol altre cas.

A partir de M i d'una cadena $w \in \Sigma^*$ qualsevol definirem un SCP format pels següents blocs:

$$\overset{1}{\left[\begin{array}{|c|}\hline \$ \\ \hline \$q_1 w\$ \\ \hline\end{array}\right]}, \overset{2}{\left[\begin{array}{|c|}\hline \$ \\ \hline \$ \\ \hline\end{array}\right]} \text{ i } \overset{\ldots}{\left[\begin{array}{|c|}\hline \sigma \\ \hline \sigma \\ \hline\end{array}\right]} \quad \forall \sigma \in \Gamma.$$

A més a més, per cada transició de δ relacionada amb estats *finals* de M, inclourem els següents blocs o conjunts de blocs:

$$\text{si} \quad \delta(q,\sigma) = (p,\tau,\rightarrow), \quad \left[\begin{array}{|c|}\hline q\sigma \\ \hline \tau p \\ \hline\end{array}\right].$$

$$\text{si} \quad \delta(q,\sigma) = (p,\tau,\leftarrow), \quad \left[\begin{array}{|c|}\hline \gamma q\sigma \\ \hline p\gamma\tau \\ \hline\end{array}\right] \quad \forall \gamma \in \Gamma.$$

$$\text{si} \quad \delta(q,\triangle) = (p,\tau,\rightarrow), \quad \left[\begin{array}{|c|}\hline q\$ \\ \hline \tau p\$ \\ \hline\end{array}\right].$$

$$\text{si} \quad \delta(q,\triangle) = (p,\tau,\leftarrow), \quad \left[\begin{array}{|c|}\hline \gamma q\$ \\ \hline p\gamma\tau\$ \\ \hline\end{array}\right] \quad \forall \gamma \in \Gamma.$$

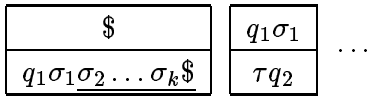
I, per últim, per cada estat final inclourem

$$\left[\begin{array}{|c|}\hline \sigma q\tau \\ \hline q \\ \hline\end{array}\right], \left[\begin{array}{|c|}\hline \sigma q\$ \\ \hline q\$ \\ \hline\end{array}\right], \left[\begin{array}{|c|}\hline \$q\tau \\ \hline \$q \\ \hline\end{array}\right], \left[\begin{array}{|c|}\hline q\$\$ \\ \hline \$ \\ \hline\end{array}\right] \quad \forall \sigma, \tau \in \Gamma.$$

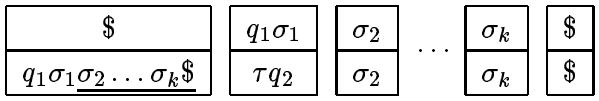
Definit d'aquesta manera, la construcció d'una solució per a aquest SCP té una relació directa amb les possibles computacions de M. Siga una cadena $w = \sigma_1\sigma_2 \ldots \sigma_k$.

Qualsevol solució per a P_{CPM} ha de començar necessàriament pel bloc 1. Per tant el següent bloc ha de contenir en la part superior el prefix $q\sigma_1$ la qual cosa implica que haurà d'existir una

transició $\delta(q_1, \sigma_1) = (\tau, q_2, \rightarrow)$. La solució podria començar a construir-se de la següent manera:



Utilitzant ara blocs de la forma $\begin{array}{|c|}\hline \sigma \\ \hline \sigma \\ \hline \end{array}$ $\forall \sigma \in \Gamma$ arribaríem a

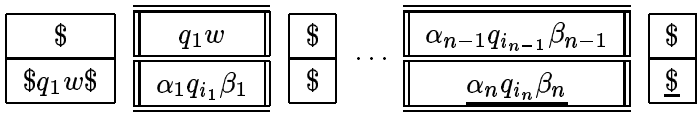


on la cadena de la part de baix dels blocs que no està emparellada correspon a la configuració de la MT després de la primera computació simple.

Es pot demostrar fàcilment per inducció que, si es té una configuració per a M de la forma

$$q_1 w \vdash_M \alpha_1 q_{i_1} \beta_1 \vdash_M \cdots \vdash_M \alpha_n q_{i_n} \beta_n$$

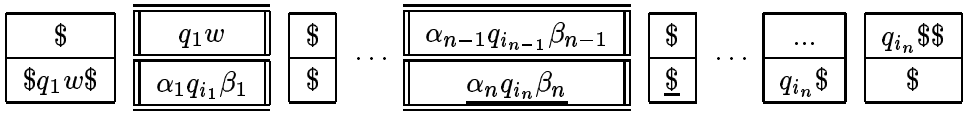
aleshores es pot obtenir una solució *parcial* per al corresponent P_{CPM} de la forma



En altres paraules, les possibilitats per anar construint una solució per al P_{CPM} es corresponen exactament amb les possibles computacions de la MT.

Per construcció del P_{CPM}, la única possibilitat per completar la solució és que la màquina arribe a una configuració de parada $\alpha_n q_{i_n} \alpha_n$ on $q_{i_n} \in F$.

En eixe cas, es podrien concatenar a la solució parcial blocs de l'últim tipus per anar eliminant símbols (un a un) de les cadenes α_n i β_n fins a arribar a



Amb la qual cosa la solució és completa.

□

6.2.5 Problemes irresolubles sobre gramàtiques incontextuals

Hi ha alguns problemes que es plantegen sobre els llenguatges incontextuals (o sobre les corresponents gramàtiques) que són irresolubles. Una forma convenient de demostrar la irresolubilitat d'alguns

d'aquests problemes consisteix a relacionarlos amb el P_{CP}.

Considerarem dos problemes:

Problema de la intersecció buida, P_{IB}

Dades: Dues gramàtiques incontextuals, $G_A = \{\Sigma, N_A, P_A, S_A\}$ i $G_B = \{\Sigma, N_B, P_B, S_B\}$.

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

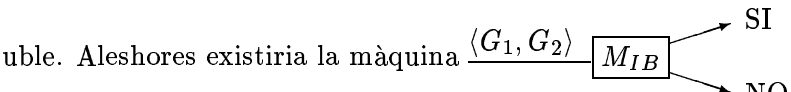
Problema de la ambiguitat d'una gramàtica, P_{AG}

Dades: Una gramàtiqua incontextual, $G_A = \{\Sigma, N_A, P_A, S_A\}$.

Enunciat: És G_A ambigua?

Teorema 6.6 El problema P_{IB} és indecidible

Prova:

Suposem que fóra resoluble. Aleshores existiria la màquina 

Siga (A, B) un SCP qualsevol sobre Σon $A = \{u_1, \ldots, u_k\}$ i $B = \{v_1, \ldots, v_k\}$ i siga Δ un alfabet tal que $\Sigma \cap \Delta = \emptyset$, $\Delta = \{a_1, \ldots, a_k\}$.

Construim aleshores les següents gramàtiques incontextuals:

$$G_A = (S_A, \Sigma \cup \Delta, S_A, \{S_A \to u_i S_A a_i | u_i a_i,\ i = 1, \ldots k\})$$

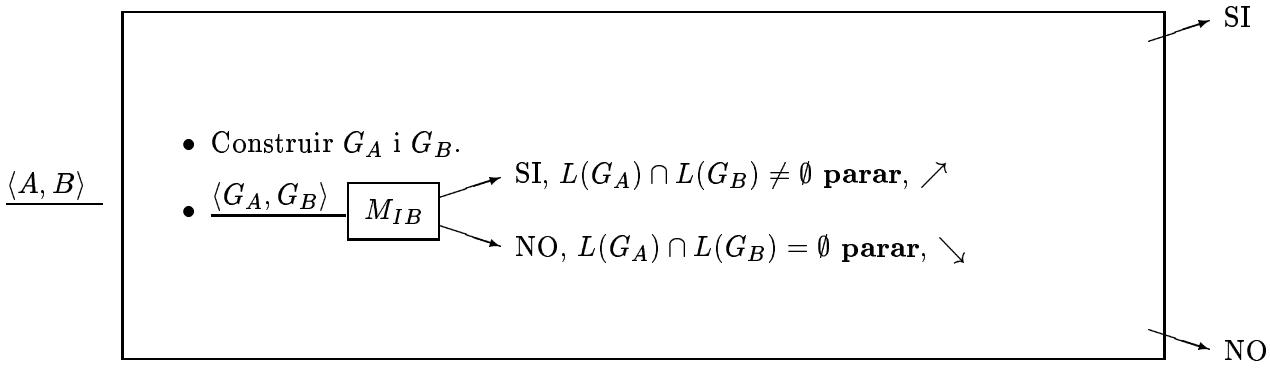
$$G_B = (S_B, \Sigma \cup \Delta, S_B, \{S_B \to v_i S_B a_i | v_i a_i,\ i = 1, \ldots k\})$$

Si el SCP anterior té solució aleshores existeix una permutació d'índex tal que $u_{i_1} \ldots u_{i_n} = v_{i_1} \ldots v_{i_n}$ la qual cosa implica necessàriament que

$$u_{i_1} \ldots u_{i_n} a_{i_1} \ldots a_{i_n} = v_{i_1} \ldots v_{i_n} a_{i_1} \ldots a_{i_n} \in L(G_A) \cap L(G_B)$$

En sentit contrari, si $w \in L(G_A) \cap L(G_B)$ ha d'existir una factorització de w, $w = w' \cdot a_{i_1} \ldots a_{i_n}$ de forma que $w' = u_{i_1} \ldots u_{i_n} = v_{i_1} \ldots v_{i_n}$ la qual cosa implica necessàriament que el SCP té solució.

Aleshores, podríem fer



la qual cosa permetria resoldre el P_{CP}. Per tant, la màquina M_{IB} no pot existir.

□

Teorema 6.7 El problema P_{AG} és indecidible.

Prova:

...

□