DCM 13

IV

$0-$ $w \longmapsto {}^{x}w$ et $w \longmapsto w^{x}$ sont des homomorphismes injectifs.

Notons $L : \{a,b\}^* \longrightarrow \{L_a, L_b\}^*$ (hom.) $\quad \mathcal{R}_0 = \{R_1, \dots, R_i, \dots, R_n\}$

$\begin{cases} a \longmapsto L_a \\ b \longmapsto L_b \end{cases}$

1.1 Traitons le cas où $p = 1$:

Supposons $u = \alpha\, l_i\, \beta$, $\quad = \alpha\, r_i\, \beta$ $\qquad \alpha, \beta \in \{a,b\}^*$, $(l,r) \in S$

Alors $(\#\#x)\cdot(\alpha^x)\cdot(l_i^x)\cdot(\beta^x)\cdot(\#^x \vee x\#\#)$

$= (\#\#x\, u^x \#)$ $\qquad$ $({}^x\alpha)\cdot({}^x r_i)\cdot({}^x\beta)\cdot(x\#\#)$

i.e. $W = D\,L(\alpha)\cdot R_i\, L(\beta)\, F$ est solution du PCP (3).

et $|W|_{\mathcal{R}_0} = 1$

1.2 p quelconque, $p \geq 1$

Supposons $u = u_0 \longrightarrow u_1 \longrightarrow \cdots \longrightarrow u_j \longrightarrow u_{j+1} \longrightarrow \cdots \longrightarrow u_n$

$u_j = \alpha_j\, l_{i_j}\, \beta_j$, $u_{j+1} = \alpha_j\, r_{i_j}\, \beta_j$

On a alors :

$$(u_0^x, {}^x u_1) = \left(\varphi\left(L(\alpha_0) R_{i_0} L(\beta_0)\right), \psi\left(L(\alpha_0) R_{i_0} L(\beta_0)\right)\right)$$

$$(u_j^x, {}^x u_{j+1}) = \left(\varphi\left(L(\alpha_j) R_{i_j} L(\beta_j)\right), \psi\left(L(\alpha_j) R_{i_j} L(\beta_j)\right)\right)$$

$$(u_{p-1}^x, {}^x u_p) = \left(\varphi\left(L(\alpha_{p-1}) R_{i_{p-1}} L(\beta_{p-1})\right), \psi\left(L(\alpha_{p-1}) R_{i_{p-1}} L(\beta_{p-1})\right)\right)$$

Posons $K_j = L(\alpha_j) R_{i_j} L(\beta_j)$ pour $0 \leq j \leq p-1$.

$$\begin{cases} \varphi\left(D K_0 L_\# K_1 \cdots L_\# K_{p-1} F\right) = (\#\#x)\cdot(u_0^x)\cdot\#x\cdot(u_1^x)\cdot\#x\cdot\cdots\cdot(u_{p-1}^x)\cdot\#x\vee^x\#\# \\ \psi\left(D K_0 L_\# K_1 \cdots L_\# K_{p-1} F\right) = \#\#x\, u^x\, \#\cdot\ ({}^x u_1)\cdot x\#\cdot\cdots\cdot x\#\cdot({}^x u_p)\cdot x\#\# \end{cases}$$

Les membres droits sont égaux. Donc

$W = D K_0 L_\# K_1 \cdots L_\# K_{p-1}$ est solution du PCP (3).

DCH 1/4

De plus $|W|_{Sb} = p$ (chaque K_j a exactement une occurrence de lettre de Sb)

1.3 $\underline{p=0}$: $u=v$

$W = D\,L(u)\,F$ est solution du PCP (3) et $|W|_{Sb} = 0$.

2 – Soit $H \in X^*$ une solution atomique.

Notons $H^{(1)} = x$ (resp. $H^{(1)} = x'$) la première (resp. dernière) lettre du mot H : $x, x' \in X_0$

$\varphi(x), \psi(x)$ sont comparables pour l'ordre préfixe $\leq_p$: donc $x = D$
$\varphi(x'), \psi(x')$ ——— suffixe $\leq_s$: donc $x' = F$.

Donc $H = D \cdot H_0 \cdot F$ où $H_0 \in X^*$. $(\mathcal{D}_0)$

Montrons par l'absurde que $H_0 \in (X \setminus \{D, F\})^*$. Sinon

$$H = D \cdot u_1 X_1 u_2 X_2 \cdots u_p X_p u_{p+1} F \quad (\mathcal{D}_H)$$

où $X_1, X_2, \dots, X_p \in \{D, F\}$.

si $\underline{X_1 = D}$:

$\varphi(D)\varphi(u_1)$ est le plus court préfixe de $\varphi(H)$ qui appartienne à $\#\#\{a,b,c,\#\}^*\#\#$

$\psi(D)\psi(u_1)$ est aussi le plus court préfixe de $\psi(H)$ qui ... (idem).

Donc $\varphi(Du_1) = \psi(Du_1)$. Ce qui n'est pas possible puisque Du_1 doit avoir la forme $(\mathcal{D}_0)$ alors qu'il ne se termine pas par F. Contradiction.

si $\underline{X_1 = F}$:

$\varphi(Du_1F)$ est le plus ——— préfixe de $\varphi(H)$ dans $\#\#\{a,b,c,\#\}^*\#\#$
$\psi(Du_1F)$

Donc $\varphi(Du_1F) = \psi(Du_1F)$ et, par simplification à gauche, $\varphi(u_2X_2\cdots u_{p+1}F) = \psi(u_2X_2\cdots u_{p+1}F)$; donc H n'est pas atomique.

Contradiction

DCM15

On a démontré : $H_0 \in (X \setminus \{D, F\})^*$

3- Soit $H \in (X \setminus \{D, F, L_\#\})^*$. Alors il existe $k \geq 0$, $w_1, \dots, w_{k+1} \in \{a, b\}^+$, $i_1, \dots, i_k \in [\![1, n]\!]$,

$$H = L(w_1) R_{i_1} L(w_2) R_{i_2} \dots L(w_k) R_{i_k} L(w_{k+1})$$

Posons : $u_0 = \left(\prod_{j=1}^{k} w_j \ell_{i_j}\right) w_{k+1}$ $\quad v_0 = \left(\prod_{j=1}^{k} w_j r_{i_j}\right) w_{k+1}$

On a bien : $\varphi(H) = u_0^x$, $\psi(H) = v_0^x$ et $u_0 \xrightarrow[S]{k} v_0$
et $k = |H|_{\mathcal{R}_0}$.

4- On montre par récurrence sur $|H|_{L_\#} = k$ que :

$$\varphi(H) \#^x v_1 = u_1^x \# \psi(H) \Rightarrow \left[u_1 \xrightarrow{\mu} v_1 \text{ où } \mu = |H|_{\mathcal{R}_0}\right]$$

Base : $|H|_{L_\#} = 0$

Par Q3 : $\varphi(H) = u_0^x$, $\psi(H) = v_0^x$ et $u_0 \xrightarrow[S]{\mu} v_0$

où $\mu = |H|_{\mathcal{R}_0}$.

$$\varphi(H) \#^x v_1 = u_1^x \# \psi(H) \Rightarrow u_0^x \#^x v_1 = u_1^x \#^x v_0$$

donc $u_0 = u_1$, $v_0 = v_1$ et $\left[u_1 \xrightarrow{\mu} v_1 \text{ où } \mu = |H|_{\mathcal{R}_0}\right]$

Induction : $|H|_{L_\#} = k+1$.

$H = H_0 L_\# H_1$ où $|H_0|_{L_\#} = 0$, $|H_1|_{L_\#} = k$

$$\begin{cases} \varphi(H_0) \#_x \varphi(H_1) \#^x v_1 = u_1^x \# \psi(H_0)_x \# \psi(H_1) & (1) \\ \varphi(H_0) = u_0^x, \ \psi(H_0) = v_0^x, \ u_0 \xrightarrow[S]{\mu_0} v_0 \text{ où } \mu_0 = |H_0|_{\mathcal{R}_0} \text{ (par Q3)} & (2) \end{cases}$$

DCM16

(1) ∧ (2) entraînent :

$$u_0^x \#^x \varphi(H_1) \#^x v_1 = u_1^x \#^x v_0 x \# \psi(H_1)$$

donc $u_0^x = u_1^x$ (plus long préfixe dans $\{a,b,x\}^*$) (Eu)

et $\#^x \varphi(H_1) \#^x v_1 = \#^x v_0 x \# \psi(H_1)$ (3)

(3) se simplifie (par simplification à gauche) en :

$$\varphi(H_1) \#^x v_1 = v_0^x \# \psi(H_1) \quad (4)$$

Comme $|H_1|_{L_\#} = k$, par (HR) :

$$v_0 \xrightarrow{\uparrow \rho} v_1 \quad \text{où} \quad \rho = |H_1|_{\mathcal{R}_0} \quad (5)$$

Par (2)(5) (Eu) :

$$u_1 = u_0 \xrightarrow{\uparrow \rho_0} v_0 \xrightarrow{\uparrow \rho} v_1 \quad \text{et} \quad \rho_0 + \rho = |H_0|_{\mathcal{R}_0} + |H_1|_{\mathcal{R}_0} = |H|_{\mathcal{R}_0}$$

(qed).

5- Par Q1, $u \xrightarrow[S]{*} v \implies \phi(S,u,v)$ a une solution

Par Q2 : si $\phi(S,u,v)$ a une solution, alors $\exists H \in (X \setminus \{D,F\})^*$,

$$\varphi(H) \#^x v = u^x \# \psi(H)$$

par Q4 : cela entraîne $u \xrightarrow[S]{\uparrow \rho} v$ avec $\rho = |H|_{\mathcal{R}_0}$

Finalement : $u \xrightarrow[S]{*} v \iff \phi(S,u,v)$ a une solution.

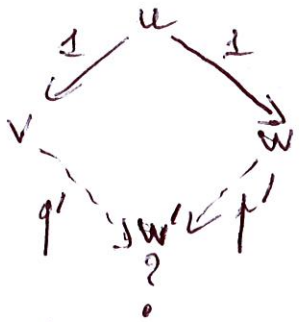
6- Comme (ACC-ST) est indécidable (III, Q6) pour les SST sur $\{a,b\}$, et comme ϕ réduit (ACC-ST) à (PCP), (PCP) est indécidable.

7- Voir I, Q4 : $W = D \cdot L_a R_1 L_b L_1 \cdot L_\# \cdot R_1 R_1 L_b \cdot L_\# \cdot L_b R_1 R_1 \cdot L_\# \cdot L_b L_b R_{1a} \cdot F$ est solution.

DHC17

Partie V

1 -



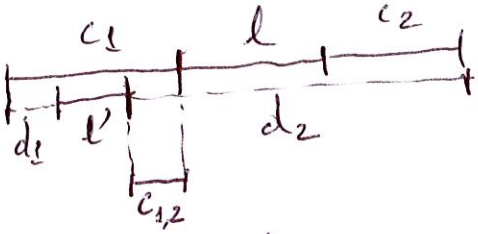
$\exists c_1, c_2, d_1, d_2 \in A^*$:

$$\begin{cases} u = c_1 \cdot l \cdot c_2 = d_1 \cdot l' \cdot d_2 & \text{avec } (l, r), (l', r') \in S \\ v = c_1 \cdot r \cdot c_2 \quad w = d_1 \cdot r' \cdot d_2 \end{cases}$$

La condition d'orthogonalité entraîne que :

$l = l'$, $c_1 = d_1$, $c_2 = d_2$ (cas 1) ou

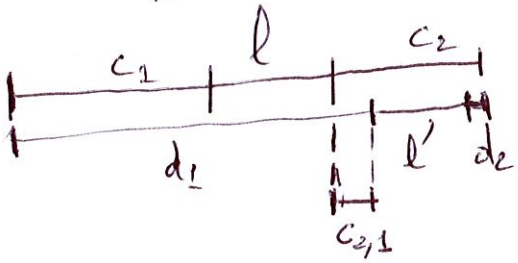
$\exists c_{1,2} \in A^*$, $c_1 = d_1 l' c_{1,2}$, $c_{1,2} l c_2 = d_2$



(cas 2)

ou

$\exists c_{2,1} \in A^*$, $c_2 = c_{2,1} l' d_2$, $c_1 l c_{2,1} = d_1$.



(cas 3).

cas 1 : $v = w$

On pose $p' = q' = 0$, $w' = v = w$

cas 2 : $u = d_1 l' c_{1,2} l c_2$, $v = d_1 r' c_{1,2} l c_2$, $w = d_1 l' c_{1,2} r c_2$

On pose $p' = q' = 1$, $w' = d_1 r' c_{1,2} r c_2$

On a bien $u = d_1 l' c_{1,2} l c_2 \longrightarrow d_1 r' c_{1,2} l c_2 \longleftarrow d_1 r' c_{1,2} l c_2 = w$.

cas 3 : analogue au cas 2.

□

DCM18

2 – On prouve cette propriété par récurrence sur $p+q=n$.

$n=0$: alors $u=v=w$. On choisit $p'=q'=0$, $w'=u=v$

$n=1$: $(u \to v$ et $u=w)$ (cas 1) ou $(u \to w$ et $v=v)$

cas 1 : on pose $w'=v$, $p'=1$, $q'=0$ on a bien : $w \xrightarrow{1} w'$ et $v \xrightarrow{0} w'$.

cas 2 : on pose $w'=w$, $p'=0$, $q'=1$ on a bien : $w \xrightarrow{0} w'$ et $v \xrightarrow{1} w'$.

$n=m+1$ (avec $m \geq 1$) :

* si $p=0$ ou $q=0$, on conclut comme pour $n=1$
* $p=p_1+1$, $q=q_1+1$ $\quad p_1+q_1=m-1<n$

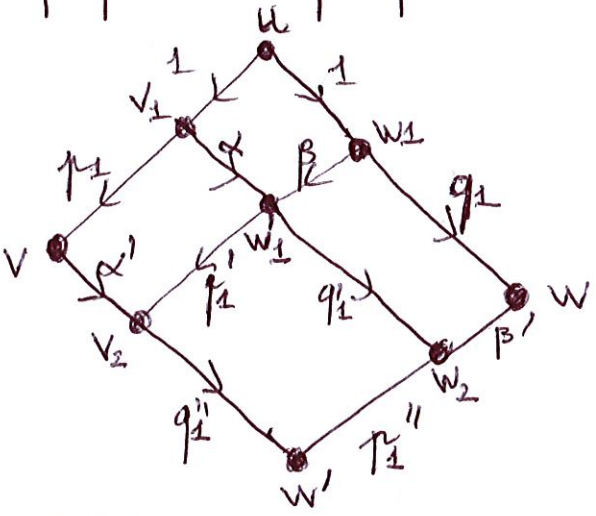


figure V.2

On décompose :

$\begin{cases} u \xrightarrow{1} V_1 \xrightarrow{p_1} V \\ u \to W_1 \xrightarrow{q_1} W \end{cases}$

Par hyp de récurrence :

$V_1 \xrightarrow{\alpha} W_1' \xleftarrow{\beta} W_1$ avec $\alpha, \beta \leq 1$, $\underbrace{1+\alpha=1+\beta}_{e1}$

comme $p_1+\alpha \leq p_1+1 < (q_1+1)+(q_1+1)$, par Hyp de réc :

$V \xrightarrow{\alpha'} V_2 \xleftarrow{p'_1} W_1'$ et $W_1' \xrightarrow{q'_1} W_2 \xleftarrow{\beta'} W$

avec $\underbrace{p_1+\alpha'=\alpha+p'_1}_{e2}$, $p'_1 \leq p_1$, $\alpha' \leq \alpha$, $\underbrace{\beta+q'_1=q_1+\beta'}_{e3}$, $\beta' \leq \beta$, $q'_1 \leq q_1$

comme $p'_1 \leq p_1$ et $q'_1 \leq q_1$, $p'_1+q'_1 \leq p_1+q_1=m-1$ et par Hyp de réc,

$V_2 \xrightarrow{q''_1} W' \xleftarrow{p''_1} W_2$

avec $\underbrace{p'_1+q''_1=q'_1+p''_1}_{e4}$, $p''_1 \leq p'_1$, $q''_1 \leq q'_1$. (Voir figure V.2)

DCM19

La somme, membre à membre, des égalités e_1, e_2, e_3, e_4 donne :

$$1+\alpha+p_1+\alpha'+\beta+q_1'+p_1'+q_1''=1+\beta+\alpha+p_1'+q_1+\beta'+q_1'+p_1'' \quad (E)$$

Après simplification par $\alpha+\beta+q_1'+p_1'$ on obtient :

$$(1+p_1)+(\alpha'+q_1'')=(1+q_1)+(\beta'+p_1'') \quad (E')$$

Posons :

$q' = \alpha' + q_1''$, $\quad p' = \beta' + p_1''$

On a bien, par (E') : $p + q' = q + p'$.

D'autre part :

$q' = \alpha' + q_1'' \leq \alpha + q_1' \leq 1 + q_1 = q$

$p' = \beta' + p_1'' \leq \beta + p_1' \leq 1 + p_1 = p$

□

3 - Supposons $u \xrightarrow[S]{p} v$ et $u \xrightarrow[S]{q} w$, v, w irréductibles.

Par la Q2, $v \xrightarrow{q'} w' \xleftarrow{p'} v$ avec $p + q' = q + p'$.

Comme v, w sont irréductibles : $p' = q' = 0$, $v = w' = v$

Donc $p = q$ et $v = w$.

4 - Soit $MG(S) = \{ab, cb, DB, aF, cF\}$

l'ensemble des membres-gauches de S. On vérifie que si $m = xy \in MG(S)$ alors y n'est pas la première lettre d'un autre membre-gauche

$y \in \{b, B, F\}$ et les premières lettres sont $\{a, c, D\}$

on a bien $\{b, B, F\} \cap \{a, c, D\} = \emptyset$.

(qed)

DCM20

5- Par récurrence sur $k \geq 0$:

D1(k) : $a\,b^k \xrightarrow{*} b^{2^k}\,a$ (en utilisant la première règle de S)

D2(k) : $c^k\,b \xrightarrow{*} b\,c^{2^k}$ (——— deuxième règle de S)

* Supposons $a^n b \xrightarrow[S]{*} b^{2^n} a^n$

$a^{n+1} b = a\,(a^n b) \xrightarrow{*} a\,b^{2^n} a^n$

$(a b^{2^n})\,a^n \longrightarrow b^{2^{n+1}}\,a\,a^n$ (par D1(2^n))

donc $a^{n+1} b \xrightarrow{*} b^{2^{n+1}}\,a^n$

* Supposons $c\,b^n \xrightarrow[S]{*} b^n\,c^{2^n}$

$(c\,b^n)\,b \xrightarrow[S]{*} b^n\,c^{2^n}\,b$

$b^n\,(c^{2^n} b) \xrightarrow{*} b^n\,(b\,c^{2^{n+1}})$ (par D2(2^n))

donc $c\,b^{n+1} \xrightarrow{*} b^{n+1}\,c^{2^{n+1}}$.

(qed)

6- $D c a^n b F \xrightarrow[S]{*} D c\,b^{2^n}\,a^n F$ (par Q5.1)

$\xrightarrow[S]{*} D\,b^{2^n}\,c^{2^{2^n}}\,a^n F$ (par Q5.2)

Or : $D b^n \xrightarrow{*} D$, $a^n F \xrightarrow{*} F$, $c^n F \to F$

Donc : $D\,b^{2^n}\,c^{2^{2^n}}\,a^n F \xrightarrow{*} DF$.

⚠ erreur dans l'énoncé : $Db \to D$ (au lieu de $Db \to b$)

DCM21

7. $Dc\,a^n b\,F \xrightarrow{*} Db^{2^n} c^{2^{2^n}} a^n F$ (par Q5)

$Db^{2^n} c^{2^{2^n}} a^{2^n} F \xrightarrow{2^n} D\,c^{2^{2^n}} a^n F$

$\xrightarrow{n} D\,c^{2^{2^n}} F$

$\boxed{2^{2^n}}$ DF (2^{2^n} applications de $cF \to F$)

8 – DF est irréductible et S est orthogonal.
Par Q3, toute dérivation $u = Dc\,a^n b\,F \xrightarrow{\varphi} DF = v$ doit avoir une longueur p égale à la dérivation de Q7.
Donc $p \geq 2^{2^n}$.

9 – Appliquons la réduction ϕ (de la partie IV) à l'instance $(S, Dc\,a^8 b\,F, DF)$ du pb. (ACC-ST):
on obtient une instance de (PCP).
Par (V.Q2, VQ4): si W est solution de $\phi(S, Dc\,a^8 b\,F, DF)$
alors $W = D \cdot H_0 \cdot F$ et $Dc\,a^8 b\,F \xrightarrow{p} DF$
pour $p = |H_0|_{\mathcal{B}_0}$.
Par Q8: $p \geq 2^{2^8}$
Donc : $|H_0| \geq 2^{2^8}$
donc : $\underline{|W| \geq 2^{2^8}}$

DCM 22

L'instance de (PCP) est :

$$\begin{pmatrix} \#\#x \\ \#\#xDxc(ax)^{8}bxFx\# \end{pmatrix} \begin{pmatrix} \#xDxFx\#\# \\ x\#\# \end{pmatrix} \begin{pmatrix} \#x \\ x\# \end{pmatrix} \begin{pmatrix} ax \\ xa \end{pmatrix} \begin{pmatrix} bx \\ xb \end{pmatrix} \begin{pmatrix} cx \\ xc \end{pmatrix} \begin{pmatrix} Dx \\ xD \end{pmatrix} \begin{pmatrix} Fx \\ xF \end{pmatrix}$$

10 - Estimons le temps nécessaire à ce calcul :

* le nbe d'op. par seconde de la machine est :

$$p \leq 1000 \cdot 10^{15} \times 10^{7} = 10^{25} \text{ op/s}$$

* 1 année $\leq 400 \cdot 25 \cdot 4000$ s $\leq 4 \cdot 10^{7}$ s.

* nb d'op à effectuer $\geq 2^{2^8} = 2^{256} \geq (2^{10})^{25} \geq 10^{75}$

* temps-calcul $\geq \frac{10^{75}}{10^{25}}$ s $\geq 10^{50} \times \frac{1}{4 \cdot 10^{7}}$ années

$$\geq 10^{42} \text{ années}$$

$$= 10^{33} \cdot 10^{9} \text{ années}$$

$$= 10^{31} \cdot (100 \text{ milliards}) \text{ années.}$$

Sachant que le soleil se transforme (disait [Hubert Reeves, patience dans l'azur]) en géante rouge dans 15 milliard d'années, le calcul ne pourra pas être achevé d'ici-là ...

DCM23

Partie VI

1 – $S_1 = \{(ab, bba)\}$, $u_1 = abb$

$u_1 \longrightarrow bbab \longrightarrow bbbba$

l'arbre de toutes les dérivations commençant en u_1 est réduit à cette branche. Donc S_1 termine sur abb.

$S_2 = \{(ab, bba)\}$, $u_2 = aba$

$u_2 = aba \longrightarrow bbaa$

l'arbre de toutes les dérivations (mod S_2) commençant en u_2 est réduit à cette branche. Donc S_2 termine sur aba

S_3 : $bc \to dc$ (R1), $bd \to db$ (R2), $ad \to abb$ (R3) $u_3 = abc$

Lemme: $\forall i \in \mathbb{N}, i \geq 1 \Rightarrow ab^ic \xrightarrow[S_3]{+} ab^{i+1}c$

preuve: $ab^ic = ab^{i-1}(bc) \longrightarrow ab^{i-1}dc$ (par R1)

$\xrightarrow{i-1} adb^{i-1}c$ (par R2, utilisée $i-1$ fois)

$\longrightarrow abbb^{i-1}c$ (par R3)

$= ab^{i+1}c$

□

Donc $abc \xrightarrow{+} ab^2c \xrightarrow{+} \dots ab^ic \xrightarrow{+} ab^{i+1}c \xrightarrow{+} \dots$
est une dérivation infinie (mod S_3) partant de abc.
Donc S_3 ne termine pas sur abc.

DCII 24

S_4 : $bad \longrightarrow dadcbabb$ (R1), $bd \to db$ (R2) $u_4 = babad$

Lemme : $\forall i \geq 1$, $ba\,b^i ad \xrightarrow[S_4]{+} (dabc)\, bad^{i+1} ad\,(cbabb)$

preuve :

$ba\,b^i ad = ba\,b^{i-1}(bad) \longrightarrow ba\,b^{i-1}(dadcbabb)$ (R1)

$= ba(b^{i-1}d)adcbabb \xrightarrow{*} ba(d\,b^{i-1})adcbabb$ (R2, $i-1$ fois)

$= (bad)\,b^{i-1}adcbabb \longrightarrow (dadcbabb)\,b^{i-1}adcbabb$ (R1)

$= (dadc)\,ba\,b^{i+1}ad\,(cbabb)$

□

Donc S_4 ne termine pas sur $babad$:

$babad \xrightarrow{+} \alpha\, bab^2 ad\, \beta \xrightarrow{+} \alpha^i\, bab^{i+1} ad\, \beta^i \xrightarrow{+} \dots$

où $\alpha = dadc$, $\beta = cbabb$.

2 - Reprenons les notations de IV-Q1.

Ici : $\varphi(L_a) = ax$, $\varphi(L_a) = xa$ pour $a \in A$

Supposons : $u = u_0 \longrightarrow u_1 \longrightarrow \dots \longrightarrow u_j \longrightarrow u_{j+1} \longrightarrow \dots$

$u_j = \alpha_j\, l_j\, \beta_j$ / $u_{j+1} = \alpha_j\, r_j\, \beta_j$

Posons : $K_j := L(\alpha_j)\, R_j\, L(\beta_j)$ pour $0 \leq j$

$$\begin{cases} \varphi\left(D \prod_{j=0}^{+\infty} K_j L_\# \right) = \#\#x \cdot \prod_{j=0}^{+\infty} \left(x\, u_j^x \#\, x\right) \\ \varphi\left(D \prod_{j=0}^{+\infty} K_j L_\# \right) = \#\#x\, u^x \# \prod_{j=0}^{+\infty} \left(x\, u_{j+1}^x\, x\#\right) \end{cases}$$

DCM25

Les deux mots infinis ci-dessus sont égaux car :

$$u_\infty = \#\#x u_0^x \#x u_1^x \#\cdots \#x u_j^x \#x u_{j+1}^x \#\cdots$$

(car $x u_j x = x u_j^x$).

Donc $\phi_1(S,u)$ a une solution.

3 - Remarquons que $\phi_2(S,u)$ a aussi une solution "triviale" :

$W = D \prod_{j=0}^{\neq 0} L(u) L_\#$ tel que

$$\varphi(W) = \psi(W) = \#\#x u^x \#x u^x \#\cdots \#x u^x \#\cdots$$

Donc, pour (S_1, u_1) de la question VI-1 on a :

S_1 termine sur u_1

(PCP-INF) sur $\phi_2(S_1,u_1)$ a une solution.

Donc (PCP-INF) a une sol. sur $\phi(S,u) \not\Rightarrow$ (S termine sur u).

4 - Reprenons les notations de VI Q2 (ou IV-Q1)

comme u et S sont marqués, pour tout $j \geq 1$:

$\alpha_j, \beta_j \in A_0^*$, $l_j, r_j \in A_0^* \# A_0^*$

Maintenant $L(w)$ n'est défini que pour $w \in (A_0 \cup \{\#\})^*$.

Posons $K_j := L(\alpha_j) R_j L(\beta_j)$

$$W := D \prod_{j=0}^{\neq 0} K_j L_\#$$

On a encore $\varphi(W) = \psi(W)$, donc PCP-INF

DCM26

a une solution sur $\Phi_2(S,u)$.

5- Supposons que $\Phi_2(S,u)$ a une solution $W \in X^\infty$
ici $X = \{D, L_a\ (a \in A_0), L_\#, R_1, \dots, R_n\}$

Comme la seule lettre de X $x \in X$ vérifiant que $\varphi(x)$, $\psi(x)$ sont comparables pour l'ordre préfixe est D:

$W = DW'$ où $W' \in X^\omega$

Comme en IV.2, W' ne peut avoir une occurrence de D.

$W = D.H_0$ et $H_0 \in (\{L_a \mid a \in A_0\} \cup \{L_\#, R_1, \dots, R_n\})^\omega$

Lemme: Soit $v \in A_0^* \# A_0^*$, $H \in (X \setminus \{D\})^\omega$ tels que

$$\varphi(H) = v^x \# \psi(H) \qquad (E_1)$$

Alors $\exists \alpha, \beta \in A_0^*$, $i \in [1,n]$ (numéro de règle de S)
$H' \in (X \setminus \{D\})^\omega$, $v' \in A_0^* \# A_0^*$ tels que

$$\begin{cases} v = \alpha l_i \beta, \quad v' = \alpha r_i \beta & (E_2) \\ H = L(\alpha) R_i L(\beta) L_\# H' & (E_3) \\ \varphi(H') = v'^x \# \psi(H') & (E_4). \end{cases}$$

preuve: (E_1) entraîne que H commence par un mot V tel que $\varphi(V) = v^x$. Comme v a exactement une lettre marquée, $V \in L(A_0^* R_i A_0^*)$. Donc

$V = L(\alpha) R_i L(\beta)$ avec $v = \alpha l_i \beta$

DCM27

(E_2) entraîne que la lettre qui suit V dans H est $L_\#$. Donc

$$H = L(\alpha) R_i L(\beta) L_\# H' \quad \text{où} \quad H' \in (X \setminus D_3)^{\omega}$$

posons $v' = \alpha\, r_i\, \beta$

(E_2) s'écrit: $\alpha^x l_i^x \beta^x \#^x \varphi(H') = (\alpha l_i \beta)^x \#^x \alpha^x r_i^x \beta^x \# \psi(H)$

qui se simplifie (à gauche) en: $x\varphi(H') = {}^x\alpha\, {}^x r_i\, {}^x\beta\, x\# \psi(H')$

$$\Leftrightarrow \quad \varphi(H') = v'^x \# \psi(H')$$

On a établi (E_2, E_3, E_4).

□

Revenons à la solution $W = D \cdot H_0$ de (PCP-INI=).

$\varphi|W| = \psi(W)$ s'écrit:

$$\#\#x \cdot \varphi(H_0) = \#\#x u^x \# \psi(H_0)$$

$$\Leftrightarrow \quad \underline{\varphi(H_0) = u^x \# \psi(H_0).}$$

Par le lemme: $\exists i_0, \alpha_0, \beta_0$ tels que.

$$u = \alpha_0 l_{i_0} \beta_0, \quad u_1 = \alpha_0 r_{i_0} \beta_0$$

$$H = L(\alpha_0) R_{i_0} L(\beta_0) L_\# H_1$$

$$\underline{\varphi(H_1) = u_1^x \# \psi(H_1)}$$

DCM28

Par induction on obtient que, $\forall n \geq 0$:

$$H = \left(\prod_{j=0}^{n} L(\alpha_j) R_{ij} L(\beta_j) L_{\#} \right) H_{n+1}$$

$$u_j = \alpha_j l_{ij} \beta_j, \quad u_{j+1} = \alpha_j r_{ij} \beta_j \qquad (\text{pour } 0 \leq j \leq n)$$

$$\psi(H_{n+1}) = u_{n+1}^{R} \# \psi(H_{n+1})$$

Donc $u = u_0 \longrightarrow u_1 \longrightarrow \cdots \longrightarrow u_j \longrightarrow u_{j+1} \longrightarrow \cdots$

est une dérivation infinie partant de u.

6- Soit $\mathcal{M} = \langle \Sigma, Q, q_-, Q_+, \delta \rangle$ une machine de Turing (cf. partie III).

Soit $S_{\mathcal{M}}$ le SST sur $(\Sigma \cup Q \cup \{\#\})^*$ construit à la partie III.

On vérifie que : $\forall u \in T^*$:

$$q_- Du \xrightarrow[S_{\mathcal{M}}]{\infty} \iff \mathcal{M} \text{ a un calcul } \infty \text{ sur } u.$$

Donc $(\mathcal{M}, u) \mapsto (S_{\mathcal{M}}, u)$ est une réduction du PB de la terminaison des M.T. au problème de la terminaison des SST.

Posons $A_0 = \Sigma \cup \{\#\}$, $M = Q$.

$S_{\mathcal{M}}$ est un SST marqué et $q_- Du$ est un mot marqué.

Donc ρ est une réduction du problème de l'arrêt des M.T. au PB (TERM-SS) pour des systèmes marqués et un mot de départ marqué.

DCM 29

7-

(Arrêt des MT) $\xrightarrow{f}$ (TERM-ST) marqué $\xrightarrow{\phi_2}$ (PCP-INF)

N.B. * ϕ_2 est une réduction "many-one" de (TERM-ST) marqué à la négation de (PCP-INF).

* c'est aussi une réduction "truth-table" de (TERM-ST) marqué à (PCP-INF) i.e :

(S, u) termine $\iff$ (PCP-INF) n'a pas de sol sur $\phi_2(S, u)$