Université Bordeaux 1
Master d'Informatique 1, 2010/2011

Modèles de Calcul : feuille 4

Problème de Correspondance de Post.

Exercice 4.1

Soit $I := ((u_1, v_1), \ldots, (u_p, v_p))$ une instance du Problème de Post. Notons $\mathrm{S}(I) = \{w \in \{1, 2, \ldots, p\}^* \mid w$ est une solution du problème $I\}$. Que peut-on dire, *en général* du langage $\mathrm{S}(I)$:
1- est-il clos par produit ? clos par facteur ?
2- est-il rationnel ? algébrique ? récursif ? récursivement énumérable ?
3- On appelle solution atomique de I une solution W telle que, pour toute décomposition $w = w_1 \cdot w_2$, avec $w_1, w_2 \in \mathrm{S}(I)$, $w_1 = \varepsilon$ ou $w_2 = \varepsilon$. On note $\mathrm{A}(I)$ l' ensemble des solutions atomiques de I. Montrer que $\mathrm{S}(I) = \mathrm{A}(I)^*$.
4- Que peut-on dire, *en général* du langage $\mathrm{A}(I)$?

Exercice 4.2

On considère les instances suivantes du PCP :
$I_1 := ((bbb, bb), (abb, babbb))$ $I_2 := ((ba, bab, (abb, bb), (bab, abb))$
Calculer les ensembles $\mathrm{A}(I)$ et $\mathrm{S}(I)$ pour ces deux instances.

Exercice 4.3

Le professeur Cosinus a une preuve de décidabilité du Problème de Correspondance de Post : “ Soit I une instance du PCP. Considerons l'ensemble $\mathrm{M}(I)$ des solutions de longueur minimale de I. Comme $\mathrm{M}(I)$ est fini, $\mathrm{M}(I)$ est rationnel. Soit $\mathcal{A}(I)$ un automate fini reconnaissant $\mathrm{M}(I)$. On teste si le langage reconnu par $\mathcal{A}(I)$ est vide ou non. S'il est vide I n'a pas de solution, sinon I a une solution.”
1- Que pensez-vous des affirmations de Cosinus ?
2- Le PCP est-il décidable ?

Exercice 4.4

On cherche ici à réduire le problème de l'accessibilité pour les systèmes de réécriture semi-Thuéiens au PCP.
Soit $S := \{(\ell_i, r_i) \mid 1 \leq i \leq n\}$ un système de réecriture sur $\{a, b\}^*$ et soient $u, v \in \{a, b\}^*$. Le problème de l' accessibilité pour l' instance (S, u, v) consiste à répondre à la question : $u \rightarrow_S^* v$?
On définit $\Phi(S, u, v)$ comme l'instance suivante du PCP :

$$((\#xu^x\#, \#x), (x\#, \#xv^x\#), (xa, ax), (xb, bx), (x\#, \#x), ({}^x r_1, \ell_1^x), \ldots, ({}^x r_n, \ell_n^x)$$

où les exposants ont la signification suivante : pour tout mot $w = x_1 x_2 \ldots x_m$

$$w^x = x_1 x x_2 x \ldots x_m x, \quad {}^x w = x x_1 x x_2 \ldots x x_m.$$

1- Montrer que, si $u = u_0 \rightarrow_S u_1 \ldots \rightarrow_S u_p = v$, alors $\Phi(S, u, v)$ a une solution de longueur $p + 2$.
2- On note $D, F, L_a, L_b, L_\#, R_1, \ldots, R_n$ les couples de $\Phi(S, u, v)$.

Montrer que si $H \in \{D, F, L_a, L_b, L_\#, R_1, \ldots, R_n\}^*$ est une solution atomique, alors H est de la forme

$$H = D \cdot H' \cdot F$$

avec

$$u^x \# \varphi_1(H') = \varphi_2(H') \# \, ^x v$$

Ici φ_1 (resp. φ_2) est l' homomorphisme de monoides libres qui envoie chaque symbole $D, F, L_a, L_b, L_\#, R_1, \ldots, R_n$ sur le premier mot (respectivement le second mot) du couple correspondant. Par exemple $\varphi_1(D) = \#xu^x\#, \varphi_2(D) = \#x$.

3- Montrer, par récurrence su la longueur du mot H, que

$$(u^x \# \varphi_1(H) = \varphi_2(H) \# \, ^x v) \Rightarrow (u \to_S^* v).$$

4- Montrer que $u \to_S^* v$ si et seulement si $\Phi(S, u, v)$ a une solution.

5- Que peut-on en déduire sur le PCP ?

6- Décrire l' ensemble des solutions de $\Phi(S, u, v)$ à partir de la réécriture $\to_S$.

7- Considérons l' instance suivante du PCP :

$$I := ((\#xaxaxbxbxbx\#, \#x), (x\#, \#xbxbxbxaxax\#), (xa, ax), (xb, bx), (x\#, \#x), (\ xbxa, axbx))$$

Donner une solution de cette instance. Décrire $\mathrm{A}(I), S(I)$.

Exercice 4.5

On note $X := \{a.b, c, D, F\}$. On considère le système de réécriture semi-Thuéien S suivant :

$$ab \to bba, \quad cb \to bcc, \quad Db \to b, \quad aF \to F, \quad cF \to F.$$

1- Montrer que le système S est confluent c'est à dire que : pour tous $u, u', u'' \in X^*$, si ($u \to_S^* u'$ et $u \to_S^* u''$) alors, il existe $v \in X^*$, tel que ($u' \to_S^* v$ et $u'' \to_S^* v$).

2- Montrer que le système S est noethérien c'est à dire qu'il n'existe pas de suite de mots $(u_n)_{n \in \mathbb{N}}$ telle que

$$u_0 \to_S \ldots \to_s u_n \to_S u_{n+1} \to_s \ldots$$

3- On appelle mot *irréductible* pour S, tout mot v tel que , il n' existe aucun mot w tel que $v \to_S w$. Montrer que, pour tout mot $u \in X^*$ il existe un unique mot $v \in X^*$, tel que

$$u \to_S^* v \text{ et } v \text{ est irréductible pour } S.$$

On note $\rho_S(u)$ le mot v défini ci-dessus.

4- Montrer que, pour tout mot $u \in X^*$, toutes les chaînes de réécriture de u à $\rho_S(u)$ modulo $(\to_S)$ utilisent exatement le même nombre de fois chaque règle

de S.
5- Montrer que, pour tout entier $n \geq 0$:

$$a^n b \to_S^* b^{2^n} a^n \qquad cb^n \to_S^* b^n c^{2^n}$$

6- En déduire que

$$Dca^n bF \to_S^* Db^{2^n} c^{2^{2^n}} aF \to_S^* DF$$

Quel est le nombre d'applications de la règle $cF \to F$ dans une chaine $Dca^n bF \to_S^* DF$?
7- Écrire explicitement une instance de PCP dont la plus petite solution est de longueur $>= 2^{256}$. Peut-on espérer écrire explicitement une solution de cette instance à la main ? avec un ordinateur capable d' écrire $2 \cdot 10^9$ caractères par seconde ?

Exercice 4.6

Ambiguïté d'une grammaire. Montrer que l'on ne peut pas décider si une grammaire algébrique est ambiguë, en réduisant le Problème de Correspondance de Post à ce problème.

Exercice 4.7

Intersection de deux grammaires. Montrer que l'on ne peut pas décider si les langages engendrés par deux grammaires algébriques données ont une intersection non-vide.

Exercice 4.8

Peut-on décider, à partir d' une grammaire algébrique G, les propriétés suivantes du langage L engendré par G :
P1 : L possède au moins un palindrome (i.e. un mot w tel que $w = \tilde{w}$).
P2 : L possède au moins un carré (i.e. un mot w de la forme $w = u \cdot u$).
P3 : L est un langage préfixe (i.e. $\forall u, v \in L$, si u est préfixe de v, alors $u = v$).
P4 : $L \cap \{a^n b^n \mid n \geq 0\} = \emptyset$
P5 : $L \cap \{a^n b^n c^n \mid n \geq 0\} = \emptyset$