Exercice 1

Afin de montrer que PCP est indécidable, on introduit une variante très proche de PCP. Elle diffère seulement par le fait que le premier domino de la solution est imposé. Son intérêt principal est de faciliter la preuve de l'indécidabilité de PCP.
Définition [PCPm] :
Le problème de la correspondance de Post modifié est le suivant :
– une instance est la donnée d'un entier m et de deux suites $u_1, \dots, u_m$ et $v_1, \dots, v_m$ sur un alphabet Σ;
– une solution est une suite d'indices $i_1, \dots, i_n$ de $\{1, \dots, m\}$ telle que :
$i_1 = 1$ et $u_{i_1}, \dots, u_{i_n} = v_{i_1}, \dots, v_{i_n}$
– les instances positives sont celles ayant au moins une solution.
Montrer alors que :
– PCP est décidable ssi PCPm est décidable

D'abord, montrons que si PCPm est décidable, alors PCP est aussi décidable.
Dans ce cas nous considérons le fait suivant :
Soit donc une instance de PCP formée par les deux suites de mots $u_1, \dots, u_m$ et $v_1, \dots, v_m$ sur un alphabet Σ. Une solution $i_1, \dots, i_n$ de cette instance de PCP est aussi une solution de l'instance PCPm donnée par les suites $u_{i_1}, u_1, \dots, u_m$ et $v_{i_1}, v_1, \dots, v_m$ où les mots u_{i_1} et v_{i_1} ont été placés en tête.
L'instance de PCP a une solution ssi une des m instances de PCPm obtenues en mettant en tête l'un des dominos a une solution. Ceci montre que si PCPm est décidable, alors PCP est décidable.

Maintenant, montrons que que si PCP est décidable, alors PCPm aussi est décidable.
Soit une instance de PCPm donnée par un entier m et de deux suites $u_1, \dots, u_m$ et $v_1, \dots, v_m$ sur un alphabet Σ. Nous introduisons nouveau symbole $\$ \notin \Sigma$, et nous posons $\Sigma' = \Sigma \cup \{\$\}$.
Soit alors les deux fonctions :

$$p : \Sigma^* \to \Sigma'^*$$

donnée par : $a_1 a_2 \dots a_n \to \$a_1\$a_2 \dots \$a_n$, et

$$s : \Sigma^* \to \Sigma'^*$$

donnée par : $a_1 a_2 \dots a_n \to a_1\$a_2\$ \dots a_n\$$.
On a alors que pour tout mot $w \in \Sigma^*$, $p(w)\$ = \$s(w)$.
On définit donc l'instance de PCP donnée par l'entier $m' = 2m + 1$ et les deux suites de mots $u'_1, \dots, u'_{2m+1}$ et $v'_1, \dots, v'_{2m+1}$ définies sur l'alphabet Σ de la manière suivante :

$$u'_k = \begin{cases} p(u_k) & \text{si} \quad 1 \leqslant k \leqslant m \\ p(u_{k-m})\$ & \text{si} \quad m < k \leqslant 2m \\ p(u_1) & \text{si} \quad k = 2m+1 \end{cases} \quad \text{et} \quad v'_k = \begin{cases} p(v_k) & \text{si} \quad 1 \leqslant k \leqslant m \\ p(v_{k-m}) & \text{si} \quad m < k \leqslant 2m \\ \$p(v_1) & \text{si} \quad k = 2m+1 \end{cases}$$

Soit $1, i_2, \dots, i_n$ une solution de l'instance de PCPm, c'est-`a-dire une suite telle que l'égalité $u_1 u_{i_2} \dots u_{i_n} = v_1 v_{i_2} \dots v_{i_n}$ soit vérifiée. En utilisant la relation $p(w)\$ = \$s(w)$, on obtient l'égalité $p(u_1)p(u_{i_2}) \cdots p(u_{i_n})\$ = \$s(v_1)s(v_{i_2}) \cdots s(v_{i_n})$ qui se traduit par l'égalité $u'_{2m+1}u'_{i_2} \cdots u'_{i_{n-1}}u'_{i_{n+m}} = v'_{2m+1}v'_{i_2} \cdots v'_{i_{n-1}}v'_{i_{n+m}}$. On constate que la suite $2m + 1, i_2, \dots, i_{n-1}, i_{n+m}$ est une solution de l'instance de PCP.

On vérifie que les seules solutions minimales de cette instance de Pcp sont les suites d'indices $i_1, \dots, i_n$ en verifiant les conditions suivantes :
– $i_1 = 2n + 1$,
– $1 \leq i_k \leq m$ pour tout $2 \leq k \leq n - 1$,
– $m + 1 \leq i_n \leq 2m$.
et alors, par construction, $1, i_2, \dots, i_{n-1}, i_{n-m}$ est a chaque fois une solution de l'instance de Pcpm.
Ceci montre que l'instance de départ de Pcpm a une solution si et seulement si l'instance de Pcp associée a une solution. La fonction qui calcule l'instance de Pcp associée à l'instance de

Pcpm donnée est calculable par machine de Turing déterministe. On en déduit que PCP est bien décidable ssi PCPm est décidable.

Exercice 2

Montrer que PCP est indécidable

Aide : Par l'exercice précédent il suffit de montrer que PCPm n'est pas décidable.
Soit L un langage reconnu par une machine de Turing universelle.
L'idée est d'exhiber une réduction du langage L à PCPm. Soit donc une instance de L donnée par une MT M et une entrée w. Supposons que la dernière configuration acceptante est la configuration q_{acc}. Ainsi, le mot w est accepté par M ssi il existe un calcul $q_0w = C_0 \vdash C_1 \vdash \dots C_l = q_{acc}$. On construit une instance de PCPm telle que ses solutions minimales produisent le mot $C_0\$C_1\$\dots\$C_l$.
Cette instance est formée par toutes les paires (u_i, v_i) :
- la première paire $u_1 = \$q_0w\$$ et $v_1 = \$$ pour initier le calcul ;
- une paire $u_a = a$ et $v_a = a$ pour tout $a \in \Gamma$ pour recopier cette lettre ;
- une paire $u = \$$ et $v = \$$ pour passer à la configuration suivante ;
- une paire $u = \$$ et $v = \#\$$ pour passer à la configuration suivante en ajoutant un $\#$ implicite à la fin de la configuration ;
- une paire $u_{\delta(p,a)} = pa$ et $v_{\delta(p,a)} = bq$ pour toute transition $\delta(p, a) = (q, b, R)$ de M ;
- une paire $u_{\delta(p,a)} = cpa$ et $v_{\delta(p,a)} = cbq$ pour toute transition $\delta(p, a) = (q, b, L)$ de M et toute lettre $c \in \Gamma$;
- une paire $u = aq_{acc}$ et $v = q_{acc}$ et une autre paire $u = q_{acc}a$ et $v = q_{acc}$ pour toute lettre $a \in \Gamma$ afin de réduire la configuration une fois l'état q_{acc} atteint ;
- une paire $u = q_{acc}\$$ et $v = \epsilon$ pou terminer.

Discuter alors brièvement comment et pourquoi toute solution de cette instance de PCPm provient nécessairement d'un calcul acceptant le mot w.

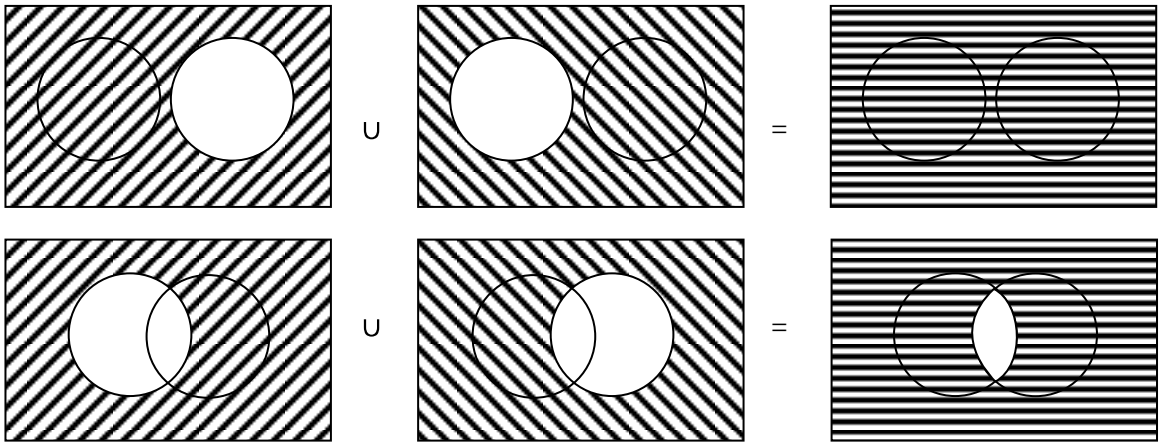
On ramène le problème de la correspondance de Post modifié à une machine de Turing qui s'arrête sur un input spécifique w. Une solution à l'instance de PCPm n'apparaîtra que si le mot w est accepté par la MT. Comme le problème de la halte de la MT est indécidable, on prouve que PCPm est indécidable aussi.

3.1

3.2

(a) Les grammaires engendrant les langages L_u et L_v peuvent être calculées par une machine de Turing déterministe à partir de l'instance de PCP, mais celui-ci n'a une solution si et seulement si l'intersection $L_u \cap L_v$ est non vide. On a donc construit une réduction de PCP au problème considère. Et montré qu'il est indécidable.

(b) On peut décomposer $(A+\Sigma)^* = (A+\Sigma)^* \backslash L_u \cup (A+\Sigma)^* \backslash L_v$ si est seulement si $L_u \cap L_v = \emptyset$.



Ce qui nous réduit le problème au cas (a), donc il est également indécidable.

(c) Si l'on applique (b) on arrive à une même équation que (b) que l'on peut de nouveau ramener à (a) et donc cette troisièmes proposition est également indécidable. $L(G_1) = L(G_2)? => A^* = L(G_2)?$ ...