Exemple des problèmes indécidables (le PCP)

Introduction Soit Σ un alphabet fini et P $\subseteq \Sigma^* \times \Sigma^*$ un ensemble fini de dominos étiquetés par des mots sur l'alphabet Σ (c'est à dire des paires de mots). Le problème de correspondance de Post (le PCP) introduit par Emil Post en 1946, consiste à déterminer s'il existe une séquence de dominos de P tel que le mot obtenu par la concaténation des premières composantes est identique à celui formé par la concaténation des secondes composantes. Plus formellement, on cherche à déterminer l'existence d'une suite $(u_i, v_i)_{0\leq i\leq n}$ tel que : $\forall 0 \leq i \leq n, (u_i, v_i) \in P$ et $u_0u_1u_2...u_n = v_0v_1v_2...v_n$.

Exemple :
Soit P $= \{(a, aaa), (aaaa, a)\}$, on peut aussi écrire P $= \{\frac{a}{aaa}, \frac{aaaa}{a}\}$ sachant que $\frac{a}{aaa}$ représente le domino $\frac{u_1}{v_1}$ et $\frac{aaaa}{a}$ représente le domino $\frac{u_2}{v_2}$.
Dans ce cas, on a une correspondance de Post qui est la suivante :
$\frac{a}{aaa}\ \frac{a}{aaa}\ \frac{a}{aaa}\ \frac{aaaa}{a}\ \frac{aaaa}{a}$ qui donne $\frac{aaaaaaaaaaa}{aaaaaaaaaaa}$ c'est à dire le nombre de a en haut est égale au nombre de a en bas et on dit qu'il y a une correspondance de Post.

On prend un deuxième exemple, soit $P_1 = \{(a, ab), (ba, aba), (b, aba), (bba, b)\}$.
Question : trouver une correspondance de Post.
Dans cet exemple, la correspondance est la suivante :
$\frac{a}{ab}\ \frac{bba}{b}\ \frac{ba}{aba}$ qui donne abbaba = abbaba.
$P_2 = \{(aab, ab), (bab, ba), (aab, abab)\}$, dans cet exemple la correspondance n'existe pas.
Preuve :
Déjà, on ne peut pas prendre en premier les paires (aab,ab) et (aab,abab), car dans les deux cas le mot de gauche est différent du mot de droite. Si on prend la paire (aab,ab), on aura aab... $\neq$ ab..., et si on prend la paire (aab,abab)on aura aab..$\neq$abab...
Maintenant, si on commence par la deuxième paire c'est à dire (bab,ba), alors à gauche on aura un "bab" et à droite un "ba" et comme les deux autres paires (la paire 1 et 3) ne commencent pas par un "b", on est obligé de rajouter une occurrence de la paire 2 et comme les mots de la paire 2 ont des tailles différentes, on ne pourra jamais obtenir une correspondance.

Le problème du PCP est d'une manière générale indécidable mais on peut décider le PCP dans le cas où Σ contient un seul élément ou une seule lettre.

théorème : Soit $\Sigma = \{a\}$, pour tout mot w $\in \Sigma^*$, on a w $= a^{|w|}$. On peut montrer qu'il existe une correspondance dans P si et seulement si :
- Soit on a $\frac{u}{v} \in$ P tel que : $|u| = |v|$ par exemple P $= \{\frac{aa}{aa}\}$ donc la correspondance est le domino lui même,
- Soit il existe $\frac{u_1}{v_1}, \frac{u_2}{v_2} \in$ P tel que $|u_1| > |v_1|$ et $|u_2| < |v_2|$.

- S'il existe $\frac{u}{v} \in$ P tel que $|u| = |v|$, alors la séquence $\frac{u}{v}$ est une correspondance puisque u $= a^{|u|} = a^{|v|} =$ v.
- S'il existe $\frac{u_1}{v_1}, \frac{u_2}{v_2} \in$ P tel que $|u_1| > |v_1|$ et $|u_2| < |v_2|$, alors $|v_2| - |u_2| > 0$ et $|u_1| - |v_1| > 0$ et dans ce cas la séquence $\frac{u_1}{v_1}^{|v_2|-|u_2|}\ \frac{u_2}{v_2}^{|u_1|-|v_1|}$ forme une correspondance de Post.

Exemple : Soient $\Sigma = \{a\}$ et P $= \{\frac{aaaa}{a}, \frac{aaa}{aaaa}\}$, donc $\frac{u_1}{v_1} = \frac{aaaa}{a}$ et $\frac{u_2}{v_2} = \frac{aaa}{aaaa}$. Comme on a $|u_1| = |aaaa| > |v_1| = |a|$ et $|v_2| = |aaaa| > |u_2| = |aaa|$, alors la correspondance de

Post dans ce cas est comme suit :

$\frac{u_1}{v_1}^{|v_2|-|u_2|}$ $\frac{u_2}{v_2}^{|u_1|-|v_1|}$ sachant que :
$u_1 = aaaa$, $v_1 = a$, $u_2 = aaa$ et $v_2 = aaaa$, donc :
$\frac{u_1}{v_1}^{|v_2|-|u_2|} = \frac{u_1}{v_1}^1 = \frac{aaaa}{a}$ et $\frac{u_2}{v_2}^{|u_1|-|v_1|} = \frac{u_2}{v_2}^3 = \frac{aaa}{aaaa}\ \frac{aaa}{aaaa}\ \frac{aaa}{aaaa}$, si on fait la concaténation, on aura :
$\frac{aaaa}{a}\ \frac{aaa}{aaaa}\ \frac{aaa}{aaaa}\ \frac{aaa}{aaaa} \Longrightarrow$ aaaaaaaaaaaaa = aaaaaaaaaaaaa.

Preuve :
En haut, on a :
$a^{|u_1|\times(|v_2|-|u_2|)} \times a^{|u_2|\times(|u_1|-|v_1|)}$
$\Longrightarrow a^{|u_1||v_2|-|u_1||u_2|} \times a^{|u_2||u_1|-|u_2||v_1|}$
$\Longrightarrow a^{|u_1||v_2|-|u_1||u_2|+|u_2||u_1|-|u_2||v_1|}$
$\Longrightarrow a^{|u_1||v_2|-|u_2||v_1|}$
Et dans la partie du bas, on trouve :
$a^{|v_1|\times(|v_2|-|u_2|)} \times a^{|v_2|\times(|u_1|-|v_1|)}$
$\Longrightarrow a^{|v_1||v_2|-|v_1||u_2|} \times a^{|v_2||u_1|-|v_2||v_1|}$
$\Longrightarrow a^{|v_1||v_2|-|v_1||u_2|+|v_2||u_1|-|v_2||v_1|}$
$\Longrightarrow a^{|v_2||u_1|-|v_1||u_2|}$

Conclusion : $a^{|u_1||v_2|-|u_2||v_1|} = a^{|v_2||u_1|-|v_1||u_2|}$.

En revanche, si on n'est pas dans cette situation, cela signifie que :
- Soit $\forall \frac{u}{v} \in P$ on a $|u| > |v|$,
- Soit $\forall \frac{u}{v} \in P$ on a $|u| < |v|$

Les deux cas sont symétriques. Alors pour toute séquence de dominos $\frac{u_0}{v_0}\frac{u_1}{v_1}...\frac{u_n}{v_n}$ on a : $|u_0u_1...u_n| = |u_0| + |u_1| + ... + |u_n| > |v_0| + |v_1| + ... + |v_n| = |v_0v_1...v_n|$ et on déduit que : $u_0u_1...u_n = a^{|u_0u_1...u_n|} \neq a^{|v_0v_1...v_n|} = v_0v_1...v_n$.