Calculabilité & Complexité

Calculabilité (5/5) : indécidabilité (suite)

Nicolas Ollinger (LIFO, Université d'Orléans)

M1 info, Université d'Orléans — S2 2025/2026

Problème de l'arrêt

entrée :	*une machine de Turing* $\mathcal{M}$ *et un mot* u
question :	*est-ce que* $\mathcal{M}$ *s'arrête sur l'entrée* u *?*

1. Dans l'épisode précédent. . .

Un problème indécidable

Théorème Le **problème de l'arrêt** est **indécidable**.

Problème de l'arrêt

entrée : *une machine de Turing $\mathcal{M}$ et un mot u*
question : *est-ce que $\mathcal{M}$ s'arrête sur l'entrée u ?*

Le langage associé est $K = \{\langle \mathcal{M}, u\rangle | \mathcal{M} \text{ s'arrête sur } u\}$.

Proposition K est **récursivement énumérable** mais **non récursif**.

Des problèmes indécidables

Définition Soient $A \subseteq \Sigma^*$ et $B \subseteq \Gamma^*$ deux langages. Une **réduction** (many-one) de A à B est une fonction **totale calculable** $f : \Sigma^* \to \Gamma^*$ telle que

$$u \in A \Leftrightarrow f(u) \in B \qquad \forall u \in \Sigma^* \quad .$$

Le langage A **se réduit** au langage B, noté $A \leqslant_m B$ s'il existe une réduction de A à B.

Proposition La relation $\leqslant_m$ est une relation de **pré-ordre**.

Proposition Si $\mathcal{P}$ est **indécidable** et si $L_{\mathcal{P}} \leqslant_m L_{\mathcal{P}'}$ alors $\mathcal{P}'$ est **indécidable**.

Théorème de Rice

Définition Une propriété $\mathfrak{P}$ des langages est **non triviale** s'il existe deux machines de Turing $\mathcal{M}$ et $\mathcal{M}'$ telles que $L(\mathcal{M})$ vérifie $\mathfrak{P}$ et $L(\mathcal{M}')$ ne vérifie pas $\mathfrak{P}$.

Théorème Soit $\mathfrak{P}$ une propriété des langages **non triviale**. Le problème d'appartenance à $\mathfrak{P}$ est **indécidable**.

Problème d'appartenance à $\mathfrak{P}$

entrée : *une machine de Turing $\mathcal{M}$*
question : *est-ce que $L(\mathcal{M})$ vérifie $\mathfrak{P}$?*

Le langage associé est $L_{\mathfrak{P}} = \{\langle\mathcal{M}\rangle \mid L(\mathcal{M}) \text{ vérifie } \mathfrak{P}\}$.

Des tas de problèmes indécidables

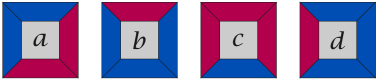
Mortalité de matrices

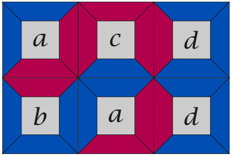
entrée : *une famille de matrices* 3×3 *à coefficients entiers*
question : *Cette famille engendre-t-elle la matrice nulle ?*

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 0 & 4 & 5 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 4 & 0 \end{pmatrix}$$

Problème du domino

entrée : *un jeu de tuiles de Wang*
question : *Ce jeu de tuile peut-il paver le plan ?*





Des tas de problèmes indécidables

Typage d'ordre supérieur

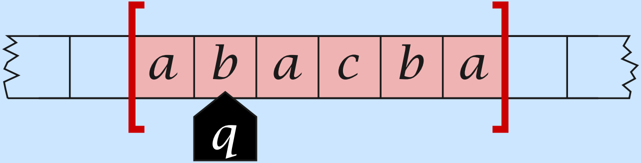
entrée : *un lambda-terme*
question : *ce terme est-il typable dans Système F?*

$$\Lambda y.\lambda x, y : \Lambda.x$$

Dixième problème de Hilbert

entrée : *une équation dipohantienne*
question : *cette équation admet-elle une solution?*

$$4x^2y + 12zx - 8y^3z^2 = 0$$



2. MT linéairement bornées

MT linéairement bornées

Définition Une **MTLB** est une MT qui ne **modifie pas le symbole blanc**. Formellement, pour tout état $q \in Q$:

$$\delta(q, B) = (q', b, \Delta) \quad \Longrightarrow \quad b = B$$

Proposition L'arrêt des MTLB est **décidable**.

Idée Pour toute entrée, les configurations atteignables qui ne quittent pas définitivement la zone de calcul sont en nombre fini.

Un problème indécidable

∃MTLB

entrée :	*une MTLB* $\mathcal{M}$
question :	*existe-t-il une entrée* $u \in \Sigma^*$ *acceptée par* $\mathcal{M}$ *?*

Proposition ∃MTLB est **indécidable**.

Idée Par réduction, montrer que K_0 se réduit à ∃MTLB.

$$\left[\frac{a}{aa}\right], \left[\frac{aaaa}{abab}\right], \left[\frac{aaab}{ba}\right], \left[\frac{bab}{b}\right]$$

3. Problème de Correspondance de Post

Problème de Correspondance de Post

PCP

entrée : n *dominos* $\left[\frac{u_1}{v_1}\right], \ldots, \left[\frac{u_n}{v_n}\right] \in (\Sigma^* \times \Sigma^*)^n$

question : *existe-t-il une suite finie* (i_k) *d'indices telle que*

$$u_{i_1} u_{i_2} \cdots u_{i_m} = v_{i_1} v_{i_2} \cdots v_{i_m} \qquad ?$$

Quelques exemples d'instances positives :

- $\left[\frac{b}{ca}\right], \left[\frac{a}{ab}\right], \left[\frac{ca}{a}\right], \left[\frac{abc}{c}\right]$
- $\left[\frac{a}{b}\right], \left[\frac{ab}{a}\right], \left[\frac{b}{bab}\right]$
- $\left[\frac{a}{aa}\right], \left[\frac{aaaa}{abab}\right], \left[\frac{aaab}{ba}\right], \left[\frac{bab}{b}\right]$

Problème de Correspondance de Post

PCP

entrée : n *dominos* $\left[\frac{u_1}{v_1}\right], \ldots, \left[\frac{u_n}{v_n}\right] \in (\Sigma^* \times \Sigma^*)^n$

question : *existe-t-il une suite finie* (i_k) *d'indices telle que*

$$u_{i_1} u_{i_2} \cdots u_{i_m} = v_{i_1} v_{i_2} \cdots v_{i_m} \qquad ?$$

Quelques exemples d'instances positives :

- $\left[\frac{b}{ca}\right], \left[\frac{a}{ab}\right], \left[\frac{ca}{a}\right], \left[\frac{abc}{c}\right]$ $(2, 1, 3, 2, 4)$
- $\left[\frac{a}{b}\right], \left[\frac{ab}{a}\right], \left[\frac{b}{bab}\right]$ *44 indices*
- $\left[\frac{a}{aa}\right], \left[\frac{aaaa}{abab}\right], \left[\frac{aaab}{ba}\right], \left[\frac{bab}{b}\right]$ *781 indices*

Un problème indécidable

Théorème PCP est **indécidable**.

Définition **PCP Marqué** (**MPCP**) est la variante de PCP qui impose qu'une solution débute toujours par le domino $\left[\frac{u_1}{v_1}\right]$.

Idée Pour montrer que PCP est indécidable, on va d'abord montrer que $K_0 \leqslant_m \mathrm{MPCP}$ puis que $\mathrm{MPCP} \leqslant_m \mathrm{PCP}$.

$K_0 \leqslant_m$ MPCP

Construisons une **fonction de réduction** g qui transforme une MT $\mathcal{M}$ en une instance de MPCP dont les solutions codent des traces valides d'un calcul de $\mathcal{M}$ sur ε.

(i) $\left[\dfrac{\#}{\#q_0B\#}\right]$

(ii) $\left[\dfrac{qa}{b'q'}\right]$ si $\delta(q,a) = (q',b',\blacktriangleright)$

(iii) $\left[\dfrac{a'qa}{q'a'b'}\right]$ si $\delta(q,a) = (q',b',\blacktriangleleft)$

(iv) $\left[\dfrac{qa}{q'b'}\right]$ si $\delta(q,a) = (q',b',\blacktriangledown)$

(v) $\left[\dfrac{a}{a}\right]$ pour tout $a \in \Gamma$

(vi) $\left[\dfrac{\#}{\#}\right]$ et $\left[\dfrac{\#}{B\#}\right]$

(vii) $\left[\dfrac{aq_F}{q_F}\right]$ et $\left[\dfrac{q_Fa}{q_F}\right]$

(viii) $\left[\dfrac{q_F\#\#}{\#}\right]$

MPCP $\leqslant_m$ PCP

Recodons toute instance de MPCP en une instance de PCP de sorte à forcer l'utilisation de la tuile $\left[\frac{u_1}{v_1}\right]$ au début d'une solution.

Soit $\star \notin \Sigma$, on pose pour $u \in \Sigma^*$, $\begin{cases} \bullet u = & \star u_1 \star u_2 \cdots \star u_n \\ u\bullet = & u_1 \star u_2 \star \cdots u_n \star \\ \bullet u \bullet = & \bullet u \star = \star u \bullet \end{cases}$

Soit $\dagger \notin \Sigma \cup \{\star\}$, la fonction de réduction est définie par

$$h\left(\left[\frac{u_1}{v_1}\right], \cdots, \left[\frac{u_n}{v_n}\right]\right) = \left\{\left[\frac{\bullet u_1}{\bullet v_1 \bullet}\right], \left[\frac{\bullet u_1}{v_1 \bullet}\right], \left[\frac{\bullet u_2}{v_2 \bullet}\right], \ldots, \left[\frac{\bullet u_n}{v_n \bullet}\right], \left[\frac{\star \dagger}{\dagger}\right]\right\}$$