

MCAL/MT - Indécidabilité du PCP (1.5 TD)

Un PCP (Problème de Correspondance de Post) est un casse-tête à base de dominos.

Définition 1 (PCP) Étant donné un ensemble fini D de dominos de la forme $d_i = \begin{pmatrix} u_i \\ v_i \end{pmatrix}$ où u_i et v_i sont des mots sur un alphabet Σ , le **problème de correspondance de Post** sur $D = \{d_0, d_1, d_2, \dots, d_n\}$ est le suivant :

Existe-il une séquence finie de dominos $d_{i_1}.d_{i_2} \dots d_{i_k}$ telle que le mot $u_{i_1}.u_{i_2} \dots u_{i_k}$ formé par la partie haute des dominos soit identique au mot $v_{i_1}.v_{i_2} \dots v_{i_k}$ formé par la partie basse des dominos ?

La séquence peut comporter autant d'exemplaires qu'on veut de chaque dominos de D mais elle doit être finie.

Exercice 1 : Familiarisation avec le PCP

Exemple : On considère l'alphabet $\{0, 1\}$ et l'ensemble de dominos

$$D = \left\{ \begin{pmatrix} 0 \\ 01 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 00 \\ 0 \end{pmatrix}, \begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 101 \\ 0110 \end{pmatrix} \right\}$$

Q1. Une solution au PCP(D) Donnez une séquence de 5 dominos de D commençant par d_0 qui soit une solution au PCP(D)

La question précédente est une variante du PCP, appelée PCP **contraint** qui consiste à imposer le premier domino de la séquence.

Définition 2 (PCPC = PCP contraint) Étant donné un ensemble fini $D = \{d_0, d_1, \dots, d_n\}$ de dominos, existe-il une solution au PCP sur D commençant par d_0 ?

Notation

— $\text{Dominos} = \left\{ \begin{pmatrix} u \\ v \end{pmatrix} \mid u, v \in \Sigma^* \right\}$ est l'ensemble des dominos construits sur l'alphabet Σ

— $D \in \mathcal{P}(\text{Dominos}) \Leftrightarrow D \subseteq \text{Dominos} \wedge |D| \in \mathbb{N}$,
cela signifie que D est un sous-ensemble fini des dominos possibles

On note PCPC-SAT l'ensemble des couples (d_0, D) formés d'un domino et d'une collection de dominos pour lesquels le PCPC a une solution :

$$\text{PCPC-SAT} = \{ (d_0, D) \mid \exists d_0.d_{i_1} \dots d_{i_k} \in D^k, u_0.u_{i_1} \dots u_{i_k} = v_0.v_{i_1} \dots v_{i_k} \}$$

où $D \in \mathcal{P}(\text{Dominos})$ désigne un ensemble fini de dominos

Q2. Décrire en français l'ensemble $\overline{\text{PCPC-SAT}} = (\text{Dominos} \times \mathcal{P}(\text{Dominos})) \setminus \text{PCPC-SAT}$

Q3. Complétez $\overline{\text{PCPC-SAT}}$ est reconnaissable par une MT si ...

Q4. Complétez PCPC-SAT est indécidable signifie ...

Exercice 2 : Réduction des exécutions finies de MT au PCPC

On va démontrer que l'appartenance à $\overline{\text{PCPC-SAT}}$ est indécidable en reliant la terminaison d'une MT sur un mot ω et l'existence d'une solution au PCPC pour un couple (d_0, D) de dominos. Pour cela, on va montrer qu'on peut créer un couple (d_0, D) de dominos tels que

PCPC(d_0, D) admet une solution **si et seulement si** l'exécution de M sur ω termine (\dagger)

Q5. Complétez ce rappel de cours

— \mathcal{M} est l'ensemble des codages binaires de MT opérant sur l'alphabet $\{0, 1, \square, \$\}$

$$\mathcal{M} = \{m \in \dots \mid m = [\dots]_2, M \in \text{MT}\}$$

— $L_{EF} = \{(m, \omega) \in \mathcal{M} \times \{0, 1\}^* \mid \dots(m, \omega) \not\rightarrow \dots\} =$ le langage des exécutions \dots

— L_{EF} est \dots par $M_{L_{EF}} = [\dots; \dots]$

— $\overline{L_{EF}} = (\mathcal{M} \times \{0, 1\}^*) \setminus \dots = \{(m, \omega) \mid \dots\}$

— $\overline{L_{EF}}$ n'est pas \dots

Q6. Complétez le diagramme de réduction permettant de montrer que l'appartenance à $\overline{\text{PCPC-SAT}}$ est indécidable

$$\begin{array}{ccc} (m, w) \in \mathcal{M} \times \{0, 1\}^* & \xrightarrow{M_f} & (d_0, D) \text{ où } D = \{d_1, \dots, d_n\} \\ \underbrace{(m, w) \in \overline{L_{EF}}}_{\text{indécidable}} & \dots\dots\dots & \underbrace{(d_0, D) \in \overline{\text{PCPC-SAT}}}_{\text{indécidable}} \quad (\dagger) \end{array}$$

car $\overline{L_{EF}}$ $\dots\dots\dots$

où M_f désigne la fonction qui construit le couple (d_0, D) dominos associé à l'exécution de (m, ω) et D est un ensemble de dominos dont les mots u et vu sont écrits avec l'alphabet $\Sigma = \mathcal{Q} \cup \{0, 1, \square, \$\}$.

Q7. Preuve à compléter

En supposant que M_f est définie et que l'équivalence (\dagger) entre $\overline{L_{EF}}$ et $\overline{\text{PCPC-SAT}}$ est démontrée, complétez la preuve d'indécidabilité de $\overline{\text{PCPC-SAT}}$ suggérée par le diagramme de réduction.

Que doit-on montrer ? que $\dots\dots\dots$ est indécidable.

Preuve par contradiction: S $\dots\dots\dots \overline{\text{PCPC-SAT}}$ $\dots\dots\dots$ par une MT $M_{\overline{\text{PCPC-SAT}}}$, ie.

$$M_{\overline{\text{PCPC-SAT}}}(d_0, D) = \mathbb{V} \iff \dots\dots\dots \quad (1)$$

et $\dots\dots\dots M_{\overline{\text{PCPC-SAT}}}$ pour **construire une** MT $M_{\overline{L_{EF}}}$ qui reconnaît $\overline{L_{EF}}$, ie. telle que

$\dots\dots\dots \xleftrightarrow{?} (m, w) \in \overline{L_{EF}}$: **on doit montrer cette** $\dots\dots\dots$

Cela $\dots\dots\dots$ le fait que $\overline{L_{EF}}$ est indécidable (cf. cours) : on aura donc la CONTRADICTION cherchée.

Construction et preuve : Étant donné une machine m et un mot ω on peut obtenir un couple (d_0, D) de dominos en appliquant $\dots\dots\dots$ à (m, w) . Si le couple (d_0, D) appartient à $\overline{\text{PCPC-SAT}}$ on peut le

$\dots\dots\dots$ en interrogeant $M_{\overline{\text{PCPC-SAT}}}$. On peut alors définir $M_{\overline{L_{EF}}} \stackrel{\text{def}}{=} \dots\dots\dots$; $\dots\dots\dots$ qui effectue les opérations suivantes :

$$\begin{array}{ccc}
(m, \omega) \xrightarrow{M_f} \dots\dots\dots \xrightarrow{M_{\overline{\text{PCPC-SAT}}}} \mathbb{V} & \stackrel{(1)}{\Longleftrightarrow} & (d_0, D) \in \overline{\text{PCPC-SAT}} \\
& \Updownarrow \text{d\'ef } M_{\overline{L_{EF}}} & \Updownarrow \text{d'apr\'es } (\ddagger) \\
M_{\overline{L_{EF}}}(m, \omega) = \mathbb{V} & & (m, w) \in \overline{L_{EF}}
\end{array}$$

d'où
 $M_{\overline{L_{EF}}}(m, \omega) = \mathbb{V} \stackrel{\text{OK}}{\Longleftrightarrow} \dots\dots\dots : \text{cqfd}$

Conclusion : En supposant $\dots\dots\dots$ reconnaissable par une MT $M_{\overline{\text{PCPC-SAT}}}$, on a aboutit à une $\dots\dots\dots$. Donc $\overline{\text{PCPC-SAT}}$ est $\dots\dots\dots$. □

Q8. Reformulez l'équivalence (\ddagger) entre $(m, w) \in \overline{L_{EF}} \iff M_f(m, w) = (d_0, D) \in \overline{\text{PCPC-SAT}}$

Pour terminer la preuve d'indécidabilité de $\overline{\text{PCPC-SAT}}$ il nous reste à définir la fonction M_f qui associe un couple (d_0, D) de dominos à l'exécution (m, ω) et qui vérifie l'équivalence (\ddagger) , c'est-à-dire

$\text{PCPC}(d_0, D) \dots\dots\dots \text{ si et seulement si l'exécution de } m \text{ sur } \omega$
 $\dots\dots\dots (\ddagger)$

Q9. Reformulez en notation logique, la phrase

« $\text{PCPC}(d_0, D)$ admet une solution **si** l'exécution de M sur ω termine »

$$\begin{array}{ccc}
M(w) \not\vdash \dots\dots\dots \text{PCPC}(d_0, D) = \dots\dots\dots & & \\
\equiv & & \\
(m, \omega) \in L_{EF} \dots\dots\dots (d_0, D) \in \text{PCPC-SAT} & & \\
\equiv & \text{(par contraposé)} & \\
(m, \omega) \in \overline{L_{EF}} \dots\dots\dots (d_0, D) \in \overline{\text{PCPC-SAT}} & &
\end{array}$$

Q10. Reformulez en notation logique, la phrase

« L'exécution de M sur ω termine **si** $\text{PCPC}(d_0, D)$ admet une solution »

$$\begin{array}{ccc}
M(w) \not\vdash \dots\dots\dots \text{PCPC}(d_0, D) = \dots\dots\dots & & \\
\equiv & & \\
(m, \omega) \in L_{EF} \dots\dots\dots (d_0, D) \in \text{PCPC-SAT} & & \\
\equiv & \text{(par contraposé)} & \\
(m, \omega) \in \overline{L_{EF}} \dots\dots\dots (d_0, D) \in \overline{\text{PCPC-SAT}} & &
\end{array}$$

Exercice 3 : Construction des dominos associés à une exécution

Considérons un mot $\omega \in \{0, 1\}^*$ et la MT $M = (\{0, 1, \square, \$\}, \mathcal{Q}, \mathbf{q}_0, \mathbf{q}_t, \delta)$ correspondant à m .

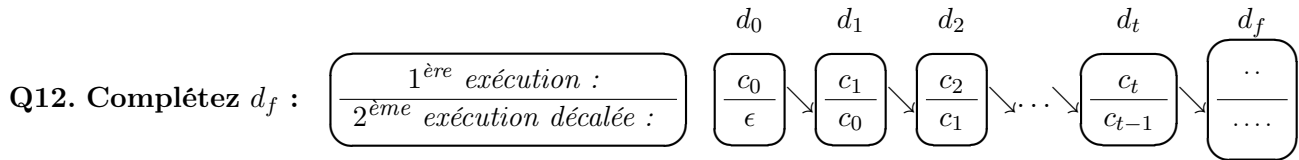
Q11. Complétez ce rappel de cours

- L'exécution de $M(\omega)$ est une suite de configurations $c_0 \xrightarrow{\tau} c_1 \xrightarrow{\tau} c_2 \rightarrow \dots$ reliée entre elles par des transitions τ de la MT M .
- La configuration c_0 de départ correspond au ruban $\overline{\infty \square \mid \$ \mid \omega \mid \square \infty}$
c'est-à-dire $c_0 = \dots\dots\dots$

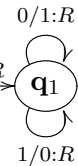
\uparrow
 \mathbf{q}_0
- Si l'exécution de la MT M termine,
c'est que M a atteint l'état $\dots\dots\dots$ avec un ruban $\overline{\infty \square \mid \omega_t \mid \omega'_t \mid \square \infty}$. La configuration terminale est alors $c_t = \dots\dots\dots$

\uparrow

L'idée de la réduction Le domino d_0 est $\frac{c_0}{\epsilon}$. Les autres dominos $d_i = \frac{c_{i+1}}{c_i}$ correspondent à une transition de l'exécution de $M(\omega)$. On ajoutera un domino d_f à déterminer. On s'intéresse au PCPC qui impose comme d_0 en début de séquence. Ainsi construit, la séquence de dominos $d_0.d_1.d_2.\dots.d_t.d_f$ correspond à une double exécution de $M(\omega)$.



Q13. Construire les 6 dominos associés au mot $\omega = 01$ et à la MT $M = \xrightarrow{\quad} \textcircled{q_0} \xrightarrow{\$: R} \textcircled{q_1} \xrightarrow{\square : H} \textcircled{q_t}$. Et vérifier qu'ils forment une solution au $\text{PCPC}(d_0, D)$.



Q14. Démontrez l'équivalence (\dagger)

- « L'exécution de M sur ω termine **implique que** $\text{PCPC}(d_0, D)$ admet une solution »
- « $\text{PCPC}(d_0, D)$ admet une solution **implique que** l'exécution de M sur ω termine »

Le nombre de dominos ainsi généré est-il fini ? Dans un $\text{PCP}(D)$ ou $\text{PCPC}(d_0, D)$, l'ensemble D de dominos doit être fini. Le procédé de construction précédent génère-t'il un nombre de dominos fini ? C'est évidemment le cas lorsque l'exécution de $M(\omega)$ est finie, mais que se passe-t'il lorsque l'exécution est infinie ?

Q15. 1^{er} cas : nombre fini de dominos Donnez une MT M (très simple) dont l'exécution est infinie sur $\omega = 0$ mais qui donne un nombre fini de dominos. Puis construisez les dominos.

Indication : On peut construire l'exécution infinie en répétant un cycle de domino, par exemple $d_0.(d_1.d_2)^*$

Q16. 2^{ème} cas : nombre infini de dominos Donnez une MT M (très simple) dont l'exécution est infinie sur $\omega = \epsilon$ et qui donne un nombre infini de dominos. Puis construisez les 5 premiers dominos.

Indication : Pour avoir un infinité de domino il suffit que la configuration du haut soit différente dans chaque domino.

Erratum


Cette construction des dominos est incorrecte (voir dernière question). Néanmoins, elle comporte tous les raisonnements et les ingrédients qui permettraient de faire la vraie preuve de l'exercice 4, tout en essayant de rester à un niveau de technicité raisonnable et de préserver l'intuition de la preuve. Les enseignants ont fait ce choix en pensant qu'il vaut mieux une bonne compréhension d'une solution partielle et de ses limites plutôt qu'une solution complète à laquelle on ne comprend rien.

Exercice 4 : Construction de dominos associés à un machine de Turing

Q17. Reconsidérez chaque domino d_0, \dots, d_4 de la question précédente et scindez le en plusieurs dominos d' afin de pouvoir générer l'exécution infinie de $M(\omega)$ avec un nombre fini de dominos.

Indication : Un domino d'_i ne représente plus une configuration complète.

Q18. Généralisez le procédé de la question précédente afin de générer les dominos non plus à partir de l'exécution de $M(\omega)$ mais à partir des symboles de Σ et des transitions de M .

 **Indication :** Il faut bien choisir les dominos de sorte que toute solution de $\text{PCPC}(d_0, D)$ correspondent à une exécution finie de $M(\omega)$.

Q19. Justifiez que ce procédé de génération est calculable (*ie.* peut être réalisé) par une MT.

Q20. Démontrez l'implication $M(\omega) \not\rightarrow \infty \implies \text{PCPC}(D) = \mathbb{V}$ laissée en suspens à l'Exercice 2:

Remarque : La preuve de la réciproque (\Leftarrow) est plus technique et ne sera pas traitée en TD, vous pouvez la trouver dans [CLSH⁺09, Wol06].