MCAL/MT - Indécidabilité du PCP (1 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 $d_i = \boxed{\frac{u_i}{v_i}}$ où u_i et v_i sont des mots sur un alphabet Σ, le* ***problème de correspondance de Post*** *sur $D = \{d_0, d_1, d_2, \ldots, d_n\}$ est le suivant :*

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

enseignants : Ce problème identifié par Emil POST en 1946 a des applications réelles en ordonnancement de tâches sur plusieurs machines parallèles (exemple à retrouver).

Exercice 1 : Familiarisation avec le PCP

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

$$D = \left\{ \underbrace{\boxed{\frac{0}{01}}}_{d_0}, \underbrace{\boxed{\frac{1}{1}}}_{d_1}, \underbrace{\boxed{\frac{00}{0}}}_{d_2}, \underbrace{\boxed{\frac{10}{00}}}_{d_3}, \underbrace{\boxed{\frac{101}{0110}}}_{d_4} \right\}$$

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)

SOLUTION

$d_0.d_4.d_3.d_2.d_2$ est une solution du PCP sur D. En effet, $\boxed{\frac{0}{01}}\boxed{\frac{101}{0110}}\boxed{\frac{10}{00}}\boxed{\frac{00}{0}}\boxed{\frac{00}{0}}$ *donne*

$$\begin{aligned} & u_0.u_4.u_3.u_2.u_2 \\ = \ & 0.101.10.00.00 \\ = \ & 0101100000 \\ = \ & 01.0110.00.0.0 \\ = \ & v_0.v_4.v_3.v_2.v_2 \end{aligned}$$

Autres solutions : $d_0.d_3.d_2.d_1.d_1$ et $d_0.d_1.d_3.d_2.d_1$.

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 $D = \{d_0, d_1, \ldots, d_n\}$ de dominos, existe-il une solution au PCP sur D commençant par d_0 ?*

Notation

- $Dominos = \left\{ \boxed{\frac{u}{v}} \mid u, v \in \Sigma^* \right\}$ est l'ensemble des dominos construits sur l'alphabet Σ
- $D \in \mathscr{P}(Dominos) \Leftrightarrow D \subseteq Dominos \ \wedge \ |D| \in \mathbb{N}$,
  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 :

$$\text{PCPC-SAT} = \{(d_0, D) \mid \exists d_0.d_{i_1}\ldots.d_{i_k} \in D^{k+1},\ u_0.u_{i_1}\ldots.u_{i_k} = v_0.v_{i_1}\ldots.v_{i_k}\}$$

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

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

SOLUTION

$\overline{\text{PCPC-SAT}}$ est l'ensemble des couples (d_0, D) formés d'un domino et d'une collection de dominos pour lesquelles PCPC n'a pas solution.

Q3. Complétez $\overline{\text{PCPC-SAT}}$ est reconnaissable ...

SOLUTION

s'il existe une MT M qui reconnaît $\overline{\text{PCPC-SAT}}$,
c'est-à-dire $M(d_0, D) = \mathbb{V} \iff (d_0, D) \in \overline{\text{PCPC-SAT}}$,
c'est-à-dire $M(d_0, D) = \mathbb{V}$ si et seulement si PCPC(d_0, D) n'a pas de solution.

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

SOLUTION

*Le langage PCPC-SAT **ou** son complémentaire $\overline{\text{PCPC-SAT}}$ n'est pas reconnaissable par une MT.*

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 $(\ddagger)$

Q5. Complétez ce rappel de cours

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

$$\mathscr{M} = \{ m \in \{0,1\}^* \mid m = [M]_2,\ M \in \text{MT} \}$$

— $L_{EF} = \{ (m, \omega) \in \mathcal{M} \times \{0,1\}^* \mid U(m, \omega) \not\to \infty \}$ = le langage des exécutions finies
— L_{EF} est reconnaissable par $M_{L_{EF}} = [\ U\ ; \to ◎\ ]$
— $\overline{L_{EF}} = (\mathcal{M} \times \{0,1\}^*) \setminus L_{EF} = \{ (m, \omega) \mid U(m, \omega) \to \infty \}$
— $\overline{L_{EF}}$ n'est pas reconnaissable

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

$$\begin{array}{rcl}
(m, w) \in \mathcal{M} \times \{0,1\}^* & \xrightarrow{M_R} & R(m, w) = (d_0, D) \text{ où } D = \{d_1, \ldots, d_n\} \\
\underbrace{(m, \omega) \in \overline{L_{EF}}} & \iff & R(m, w) = \underbrace{(d_0, D) \in \overline{\text{PCPC-SAT}}} \qquad (\ddagger) \\
\textit{indécidable} & \Longrightarrow & \textit{indécidable} \\
\textit{car } \overline{L_{EF}} \textit{ non-reconnaissable} & &
\end{array}$$

où M_R désigne la fonction de traduction 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 v sont écrits avec l'alphabet $\Sigma = \mathscr{Q} \cup \{0, 1, \Box, \$\}$.

Q7. Preuve à compléter En supposant que M_R est définie et que l'équivalence (‡) 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 $\overline{\text{PCPC-SAT}}$ est indécidable.

Preuve par contradiction SUPPOSONS $\overline{\text{PCPC-SAT}}$ reconnaissable par une MT $M_{\overline{\text{PCPC-SAT}}}$, *ie.*

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

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

$$M_{\overline{L_{EF}}}(m, \omega) = \mathbb{V} \overset{?}{\iff} (m, w) \in \overline{L_{EF}} \quad \textbf{: on doit montrer cette équivalence}$$

Cela contredira 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 M_R à (m, w). Si le couple (d_0, D) appartient à $\overline{\text{PCPC-SAT}}$ on peut le détecter en interrogeant $M_{\overline{\text{PCPC-SAT}}}$. On peut alors définir $M_{\overline{L_{EF}}} \overset{\text{def}}{=} [M_R\,; M_{\overline{\text{PCPC-SAT}}}]$ qui effectue les opérations suivantes :

$$\begin{array}{ccccc} (m,\omega) & \xrightarrow{M_f} & (d_0, D) & \xrightarrow{M_{\overline{\text{PCPC-SAT}}}} \mathbb{V} & \overset{(1)}{\iff} \quad (d_0, D) \in \overline{\text{PCPC-SAT}} \\ & & \Updownarrow \text{ déf } M_{\overline{L_{EF}}} & & \Updownarrow \text{ d'après (‡)} \\ & & M_{\overline{L_{EF}}}(m,\omega) = \mathbb{V} & & (m, w) \in \overline{L_{EF}} \end{array}$$

d'où $\quad M_{\overline{L_{EF}}}(m,\omega) = \mathbb{V} \quad \overset{\text{OK}}{\iff} \quad (m, w) \in \overline{L_{EF}}$: **cqfd**

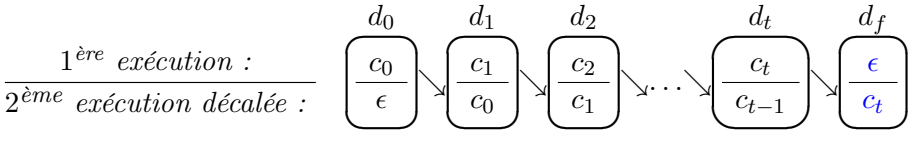
Conclusion : En supposant $\overline{\text{PCPC-SAT}}$ reconnaissable par une MT $M_{\overline{\text{PCPC-SAT}}}$, on a aboutit à une contradiction. Donc $\overline{\text{PCPC-SAT}}$ est indécidable. □

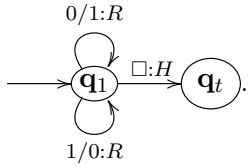
Exercice 3 : Construction des dominos associés à une exécution

Considérons un mot $\omega \in \{0,1\}^*$ et la MT $M = (\{0, 1, \square, \$\}, \mathscr{Q}, \mathbf{q}_0, \mathbf{q}_t, \delta)$ correspondant à m. L'éxécution de $M(\omega)$ est une suite de configurations $c_0 \xrightarrow{\tau} c_1 \xrightarrow{\tau} c_2 \to \dots$ reliée entre elles par des transitions τ de la MT M. La configuration de départ $c_0 \overset{\text{def}}{=} \mathbf{q}_0\,\omega$ correspond à la machine démarrant dans son état initial sur un ruban $\boxed{{}^{\infty}\square \mid \omega \mid \square^{\infty}}$ avec sa tête positionnée sur le premier sumbole du mot ω. Si l'exécution de la MT M termine avec un ruban $\boxed{{}^{\infty}\square \mid \omega_t \mid \omega'_t \mid \square^{\infty}}$, c'est que M a atteint un état $\mathbf{q}_t$ qui n'a pas de transition sortante. La configuration terminale est alors $c_t = \omega_t \mathbf{q}_t \omega'_t$

L'idée de la réduction Le domino d_0 est $\boxed{\frac{c_0}{\epsilon}}$. Les autres dominos $d_i = \boxed{\frac{c_{i+1}}{c_i}}$ 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 $M(\omega)$.

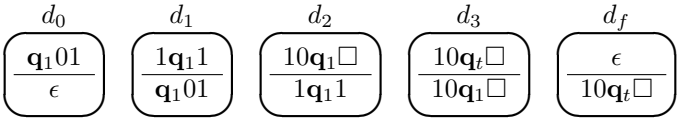
Q8. Complétez d_f pour obtenir une solution au PCPC



Q9. Donnez les dominos associés à l'exéction sur le mot $\omega = 01$ de la MT $M =$ 

. Ajoutez le domino d_f approprié pour que la séquence $d_0.d_1.\dots.d_f$ forme une solution au PCPC(d_0, D).

SOLUTION



Q10. Démontrez l'équivalence (‡)

— *« L'exécution de M sur ω termine* ***implique que*** PCPC(d_0, D) *admet une solution»*

SOLUTION

Par construction, le mot du haut de la séquence de dominos $d_0.d_1.\ldots.d_t.d_f$ correspond à l'exécution de $M(\omega)$ et le mot du bas correspond aussi à l'exécution $M(\omega)$. Le décalage ϵ du domino d_0 est comblé par le domino d_f. On a donc le même mot en haut et en bas qui correspond à l'exécution $c_0.c_1.\ldots.c_t$ de $M(\omega)$.

— *« PCPC(d_0, D) admet une solution* ***implique que*** *l'exécution de M sur ω termine »*

SOLUTION

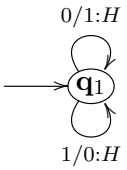
— *Si PCPC(d_0, D) admet une solution elle commence forcément par d_0 avec c_0 en haut et ϵ en bas ; donc le domino suivant doit avoir c_0, la configuration initiale, en bas.*
Or, les dominos de D correspondent à des transitions de M. Le domino suivant sera donc une transition de M depuis la configuration précédente c_i vers la configuration suivante c_{i+1} de l'exécution de M.
Ainsi il est clair qu'une solution au $PCPC(d0, D)$ pour $(d_0, D) = R(m, w)$ est le préfixe d'une exécution de m sur w. Mais ...

— ***Cette exécution est-elle complète ? le dernier domino de la séquence correspond t'il à un état terminal ?*** *Considérons une suite de domino $d_0.d_1.\ldots.d_k$ qui n'utilise pas le domino d_f. Le mot du haut $u = u_0.u_1.\ldots.u_{k_1}.u_k$ correspond à la séquence de configuration $c_0.c_1.\ldots.c_{k-1}.c_k$ et chaque configuration contient l'état courant de M donc le mot u contient k états. Par construction des dominos de D, le mot du bas contient les mêmes configurations jusqu'à c_{k-1} mais pas c_k donc le mot $v = v_0.v_1.\ldots.v_{k_1}$ contient seulement $k-1$ états. Donc, sans utiliser d_f il est donc impossible que les mots u et v soient identiques.*

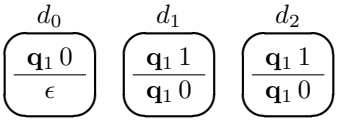
— *Donc la seule manière d'obtenir le même mot en haut et en bas dans la séquence de domino est de compenser le décalage initial de d_0 en ajoutant le domino final d_f. Or, ce domino correspond à un état terminal $\mathbf{q}_t$ de M, ce qui indique que la machine de Turing M a atteint un état terminal, ie. sans transition sortante, et donc M s'arrête : il s'agit donc bien d'une exécution finie.*

Le nombre de dominos ainsi généré est-il fini ? Dans un PCP(D) ou 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 ?

Q11. 1ercas : exécution infinie, nombre fini de dominos

Donnez les dominos associés à l'exécution sur $\omega = 0$ de la MT $M =$ 

SOLUTION



Remarque : On obtient bien un PCPC puisque le nombre de domino est fini. Remarquez qu'on a bien l'équivalence « pas de solution au $PCPC(d_0, D)$ » $\iff$ « exécution infinie de $M(w)$ ». L'exécution de M peut-être décrite pour la séquence de dominos $d_0.(d_1.d_2)^\infty$. Ce n'est pas une solution au PCPC puique la séquence est infinie.

Q12. $2^{ème}$cas : exécution infinie, nombre infini de dominos

Donnez les 4 premiers dominos associés à l'exécution sur $\omega = \epsilon$ de la MT $M =$ 

SOLUTION

d_0 d_1 d_2 d_3 $\dots$

$$\boxed{\frac{\mathbf{q}_1\square}{\epsilon}} \quad \boxed{\frac{1\mathbf{q}_1\square}{\mathbf{q}_1\square}} \quad \boxed{\frac{11\mathbf{q}_1\square}{1\mathbf{q}_1\square}} \quad \boxed{\frac{111\mathbf{q}_1\square}{11\mathbf{q}_1\square}} \quad \dots$$

Q13. Reconsidérez les dominos de la question précédente et scindez les en plusieurs dominos afin de pouvoir générer l'exécution infinie de $M(\omega)$ avec un nombre fini de dominos.

Indication : Certains dominos ne représentent plus une configuration complète.

SOLUTION

L'exécution peut se construire grâce à l'ensemble fini de dominos : d_0, d_1 et $d' =$ $\boxed{\frac{1}{1}}$.

Erratum

La construction des dominos présentée dans cet exercice ne conduit pas à des PCP (voir **Q12**). Néanmoins, elle comporte les raisonnements et les ingrédients qui permettraient de faire la preuve de la réduction de L_{EF} à $PCPC$, 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.