Devoir à rendre avant le 23 octobre 2014

On s'intéresse à la décision d'une question de sécurité dans un monde idéal: f est un chiffrement par une clef secrète, qui n'est jamais envoyée (ni en clair ni chiffrée). Le chiffrement est supposé incassable: un adversaire ne peut jamais obtenir une information sur le message en clair à partir du chiffré.

Les messages sont constuits à partir de nombres engendrés aléatoirement (et supposés indevinables), de constantes, de chiffrements et de l'appariement. Plus précisément, $\mathcal{N}$ est un ensemble dénombrable de *noms*, qui représentent les nombres aléatoires et $\mathcal{M}$ est le plus petit ensemble contenant $\mathcal{N}$, l'ensemble (supposé fini et disjoint de $\mathcal{N}$) de constantes $\mathcal{C}$ et tel que, si $u, v \in \mathcal{M}$, alors $f(u) \in \mathcal{M}$ et $\langle\ u\ ,\ v\ \rangle \in \mathcal{M}$.

Les messages échangés sont supposés obéir à des règles de protocole. Un protocole est un ensemble fini de règles

$$r \ \rightarrow\ \nu n.\ e$$

où $n \in \mathcal{N}$ et r, e sont des motifs (à réception de r, on émet e). Plus précisément l'ensemble des motifs $\mathcal{P}$ est le plus petit ensemble contenant un ensemble dénombrable $\mathcal{X}$ de variables, les noms $\mathcal{N}$, les constantes $\mathcal{C}$ et tel que, si $u, v \in \mathcal{P}$, alors $f(u) \in \mathcal{P}$ et $\langle\ u\ ,\ v\ \rangle \in \mathcal{P}$.

Les règles du protocole supposent que r ne contient pas de symboles de nom, que le seul nom qui peut apparaitre dans e est le nom créé n et que les variables de e sont contenues dans les variables de r.

Les variables seront par la suite notées par des chaines commençant par x, y, z et les noms par des chaines commençant par n, m.

Exemple de règles de protocole valides ($0 \in \mathcal{C}$).

$$\begin{array}{rcl}
\langle\ f(x)\ ,\ \langle\ f(x)\ ,\ f(y)\ \rangle\ \rangle & \rightarrow & \nu n.x \\
\langle\ x\ ,\ f(x)\ \rangle & \rightarrow & \nu n.0 \\
f(\langle\ x\ ,\ y\ \rangle) & \rightarrow & \nu n.f(\langle\ \langle\ x\ ,\ n\ \rangle\ ,\ \langle\ y\ ,\ n\ \rangle\ \rangle) \\
f(0) & \rightarrow & \nu n.f(n)
\end{array}$$

Les règles suivantes ne sont en revanche pas des règles de protocole:

$$\begin{array}{rcl}
x & \rightarrow & \nu n.\langle\ x\ ,\ y\ \rangle \\
f(\langle\ x\ ,\ n\ \rangle) & \rightarrow & \nu n.n \\
f(x) & \rightarrow & \nu n.f(\langle\ x\ ,\ n'\ \rangle)
\end{array}$$

Une *substitution* σ est une application des variables dans les messages. Elle est étendue aux motifs par morphisme: $x\sigma = \sigma(x)$ si x est une variable et $f(u)\sigma = f(u\sigma)$, $n\sigma = n$ si n est un nom ou une constante, $\langle\ u\ ,\ v\ \rangle\sigma = \langle\ u\sigma\ ,\ v\sigma\ \rangle$.

Le modèle d'exécution des protocoles est décrit par une relation entre configurations. Une *configuration* est une expression $\nu\overline{n}.L$ où $\overline{n}$ est une séquence finie de noms et L est une liste non-ordonnée de messages (pas nécéssairement distincts). Intuitivement L est une séquence de messages que l'attaquant possède en mémoire.

La *relation de transition* définie par un protocole est la plus petite relation $\rightarrow$ sur les configurations telle que,

1. Application d'une règle: si $r \rightarrow \nu n.e$ est une règle, et σ est une substitution alors,

$$\nu\overline{m}.L \cdot r\sigma \ \rightarrow\ \nu\overline{m} \cup \{n'\}.L \cdot e'\sigma$$

où $n' \in \mathcal{N} \setminus \overline{m}$, et e' est l'expression e dans laquelle n est remplacée par n' (α-conversion de e).

Intuitivement, l'attaquant contrôle le réseau et peut décider de transmettre un message qu'il possède en mémoire pour jouer une règle de protocole: il récupère alors le message émis correspondant.

2. Formation d'une paire:
$$\nu\overline{n}.L \cdot u \cdot v \ \rightarrow \ \nu\overline{n}.L \cdot \langle\ u\ ,\ v\ \rangle$$

3. Décomposition d'une paire:
$$\nu\overline{n}.L \cdot \langle\ u\ ,\ v\ \rangle \ \rightarrow \ \nu\overline{n}.L \cdot u \cdot v$$

4. Duplication:
$$\nu\overline{n}.L \cdot u \ \rightarrow \ L \cdot u \cdot u$$

5. Suppression:
$$\nu\overline{n}.L \cdot u \ \rightarrow \ \nu\overline{n}.L$$

6. Ajout d'une constante:
$$\nu\overline{n}.L \ \rightarrow \ \nu\overline{n}.L \cdot c$$

où $c \in \mathcal{C}$.

Noter que, comme la liste L n'est pas ordonnée, $L = L' \cdot u$ signifie seulement que u est dans la liste L: les règles s'appliquent n'importe où dans L.

Exemple

Considérons le protocole décrit par les deux règles ($a, c \in \mathcal{C}$):

$$\begin{array}{lrcl} 1 & c & \rightarrow & \nu n.\ \langle\ f(n)\ ,\ a\ \rangle \\ 2 & f(x) & \rightarrow & \nu n.\ f(\langle\ n\ ,\ x\ \rangle) \end{array}$$

On peut construire par exemple la séquence de configurations suivantes (l'indice fait référence à la règle de construction des configurations utilisée):

$$\begin{array}{lll} \emptyset & \rightarrow_6 & c \\ & \rightarrow_{1.1} & \nu n.\langle\ f(n)\ ,\ a\ \rangle \\ & \rightarrow_3 & \nu n.f(n) \cdot a \\ & \rightarrow_{1.2} & \nu n, n'.\ f(\langle\ n'\ ,\ n\ \rangle) \cdot a \\ & \rightarrow_5 & \nu n, n'.\ f(\langle\ n'\ ,\ n\ \rangle) \\ & \rightarrow_{1.2} & \nu n, n', n''\ f(\langle\ n''\ ,\ \langle\ n'\ ,\ n\ \rangle\ \rangle) \end{array}$$

Question 1

Dans cette question, $\mathcal{C} = \{a, b, c\}$

Le protocole suivant est la traduction dans notre formalisme d'un protocole célèbre dû à Dolev & Yao. Intuitivement, nous avons traduit le chiffrement de m avec la clef publique de x comme $f(\langle\!\langle\ x\ ,\ m\ \rangle\!\rangle)$. La deuxième règle exprime que le chiffrement est justement à clef publique et la dernière règle exprime que c est acquis à l'attaquant.

$$\begin{array}{rcl} f(\langle\!\langle\ y\ ,\ \langle\!\langle\ z\ ,\ f(\langle\!\langle\ y\ ,\ x\ \rangle\!\rangle)\ \rangle\!\rangle) & \rightarrow & f(\langle\!\langle\ z\ ,\ \langle\!\langle\ y\ ,\ f(\langle\!\langle\ z\ ,\ x\ \rangle\!\rangle)\ \rangle\!\rangle) \\ x & \rightarrow & f(x) \\ c & \rightarrow & \nu n.f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle) \\ f(\langle\!\langle\ c\ ,\ x\ \rangle\!\rangle) & \rightarrow & x \end{array}$$

1. Donner une séquence de transitions qui conduit de la configuration vide à la configuration $\nu n.f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)$. (**Ind**: la séquence a pour longueur 14).

2. Donner une séquence de transitions qui conduit de la configuration vide à la configuration $\nu n.n$. (**Ind**: la séquence a pour longueur 22).

Intuitivement, la réponse à la dernière question est une attaque sur le protocole: le nombre aléatoire n engendré par la troisième règle devrait rester inconnu de l'attaquant.

Question 2

Dans cette question, on ne considère que des protocoles tels que les membres droit de règle e ne contiennent pas de nom. Dans cette question, on omet donc les expressions $\nu\overline{n}$ qui sont ici inutiles.

On considère le problème (de confidentialité de $f(c)$) suivant:

Donnée: Un protocole et une constante $c \in \mathcal{C}$

Question: Partant de la configuration vide, existe-t-il une séquence de transitions conduisant à la configuration $f(c)$?

Montrer que ce problème est indécidable.

Ind: On pourra réduire le problème de l'arrêt; plusieurs codages des mots sont possibles et les configurations peuvent correspondre à des paires (ou des triplets) de mots, auxquels on applique f, de manière à ne permettre que les transitions de la machine de Turing.

Question 3

Dans cette question, T est un ensemble fini de tuiles, $V, H \subseteq T^2$ sont respectivement les relations de compatibilité verticale et horizontale. $t_0, t_1 \in T$ sont deux tuiles particulières.

Si $n, m \in \mathbb{N}$, un *pavage d'un rectangle* $n \times m$ est une application p de $[0..n] \times [0.., m]$ telle que

- $p(0, 0) = t_0$ et $p(m, n) = t_1$
- Pour tout $i < m$, pour tout $j \leq n$, $(p(i, j), p(i + 1, j)) \in V$

- Pour tout $j < n$, pour tout $i \leq m$, $(p(i,j), p(i,j+1)) \in H$

Montrer que le problème suivant est indécidable:

Donnée: Un ensemble fini T, deux relations $H, V \subseteq T^2$, deux éléments $t_0, t_1 \in T$

Question Existe-il deux entiers $n, m \in \mathbb{N}$ et un pavage du rectangle $n \times m$?

Question 4

Dans cette question, on autorise à nouveau les membres droits de règle à contenir des noms. En revanche on considère une restriction sur la taille des messages émis: si $k \in \mathbb{N}$, un protocole est k-borné si l'application d'une règle de protocole est restreinte aux substitutions σ telles que $r\sigma$ et $e\sigma$ sont de taille bornée par k. (La taille est le nombre de symboles utilisés pour former le message, à l'exclusion des parenthèses et séparateurs. Par exemple $\langle\ f(\langle\ n\ ,\ c\ \rangle)\ ,\ n\ \rangle$ est de taille 6.)

Montrer que dans ce cas le problème de confidentialité est encore indécidable: donner une constante $k \in \mathbb{N}$ telle que le problème

Donnée: Un protocole k-borné et une constante $c \in \mathcal{C}$

Question: Partant de la configuration vide, existe-t-il une séquence de transitions conduisant à une configuration $\nu\overline{n}.\ f(c)$?

est indécidable.

Ind: Avec cette restriction, on ne peut pas transmettre les configurations d'une machine de Turing. Mieux vaut donc réduire le problème de pavage de la question précédente. La création de nouveaux noms peut être utile pour coder les cases du rectangle, même si le codage n'est pas unique.

Solution

Question 1

Les transitions sont justifiées par l'une des règles 1 à 6 de définition des transitions. Pour la règle 1, on donne en plus le numéro de la règle de protocole utilisée.

1.

$$
\begin{array}{lll}
\emptyset & \to_6 & c \\
& \to_{1.3} & \nu n.f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_6 & \nu n.c \cdot f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_2 & \nu n.\langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_6 & \nu n.\, b \cdot \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_2 & \nu n.\ \langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_{1.2} & \nu n.\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.1} & \nu n.\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_3 & \nu n.\, b \cdot f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_5 & \nu n.\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle \\
& \to_3 & \nu n.\, a \cdot f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle) \\
& \to_5 & \nu n.\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)
\end{array}
$$

2. On répète une deuxième fois la séquence précdente ...

$$
\begin{array}{lll}
\emptyset & \to_6 & c \\
& \to_{1.3} & \nu n.f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_6 & \nu n.c \cdot f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_2 & \nu n.\langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_6 & \nu n.\, b \cdot \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_2 & \nu n.\ \langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_{1.2} & \nu n.\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.1} & \nu n.\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_3 & \nu n.\, b \cdot f(\langle\!\langle\ c\ ,\ \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.\, b \cdot \langle\!\langle\ a\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle \\
& \to_3 & \nu n.\, b \cdot a \cdot f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle) \\
& \to_5 & \nu n.\, b \cdot f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle) \\
& \to_6 & \nu n.\, c \cdot b \cdot f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle) \\
& \to_2 & \nu n.\, b \cdot a \cdot \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle \\
& \to_2 & \nu n.\ \langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle \\
& \to_{1.2} & \nu n.\ f(\langle\!\langle\ b\ ,\ \langle\!\langle\ c\ ,\ f(\langle\!\langle\ b\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_{1.1} & \nu n.\ f(\langle\!\langle\ c\ ,\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.\ \langle\!\langle\ b\ ,\ f(\langle\!\langle\ c\ ,\ n\ \rangle\!\rangle)\ \rangle\!\rangle \\
& \to_3 & \nu n.\, b \cdot f(\langle\!\langle\ c\ ,\ n\ \rangle\!\rangle) \\
& \to_5 & \nu n.f(\langle\!\langle\ c\ ,\ n\ \rangle\!\rangle) \\
& \to_{1.4} & \nu n.n
\end{array}
$$

Question 2

On code les mots comme des listes chainées à l'aide de la paire. Étant donnée une machine de Turing $M = (Q, q_0, \Sigma, \{B, \$\}, \delta)$ et un mot $w \in \Sigma^*$, on construit le protocole de la manière suivante:

- $\mathcal{C} = \Sigma \uplus Q \uplus \{c\}$.
- on définit par récurrence sur w le message $\overline{w}$ par:
  - $\overline{\epsilon} = c$
  - $\overline{a \cdot w} = \langle\ a\ ,\ \overline{w}\ \rangle$
- Si $\gamma = (q, w, w')$ est une configuration de M, on note $\overline{\gamma}$ le message $f(\langle\ \overline{\widetilde{w}}\ ,\ \overline{qw'}\ \rangle)$ où $\widetilde{w}$ est l'image miroir de w.

On construit ensuite les règles de protocole:

- La configuration initiale est donnée par la règle de protocole

$$(R1) \quad c \quad \to \quad \overline{\gamma_0}$$

- Pour chaque transition de δ de la forme $(q, a) \mapsto (q', b, \to)$ on construit la règle de protocole

$$(R2) \quad f(\langle\ x\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ y\ \rangle\ \rangle\ \rangle) \quad \to \quad f(\langle\ \langle\ b\ ,\ x\ \rangle\ ,\ \langle\ q'\ ,\ y\ \rangle\ \rangle)$$

  et, dans le cas où a est le symbole B on a aussi la règle:

$$(R2b) \quad f(\langle\ x\ ,\ \langle\ q\ ,\ c\ \rangle\ \rangle) \quad \to \quad f(\langle\ \langle\ b\ ,\ x\ \rangle\ ,\ \langle\ q'\ ,\ c\ \rangle\ \rangle)$$

- Pour chaque transition de δ de la forme $(q, a) \mapsto (q', b, \leftarrow)$ on construit la règle de protocole

$$(R3) \quad f(\langle\ \langle\ a'\ ,\ x\ \rangle\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ y\ \rangle\ \rangle\ \rangle) \quad \to \quad f(\langle\ x\ ,\ \langle\ q'\ ,\ \langle\ a'\ ,\ \langle\ b\ ,\ y\ \rangle\ \rangle\ \rangle\ \rangle)$$

- Pour chaque transition de δ de la forme $(q, a) \mapsto (q', b, \downarrow)$ on construit la règle de protocole

$$(R4) \quad f(\langle\ x\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ y\ \rangle\ \rangle\ \rangle) \quad \to \quad f(\langle\ x\ ,\ \langle\ q'\ ,\ \langle\ b\ ,\ y\ \rangle\ \rangle\ \rangle)$$

- Enfin, quand on atteint un état $q_f \in \{\mathbf{accept}, \mathbf{reject}\}$ on émet $f(c)$:

$$(R5) \quad f(\langle\ x\ ,\ \langle\ q_f\ ,\ y\ \rangle\ \rangle) \quad \to \quad f(c)$$

On note $\overline{L}$ la configuration obtenue à partir de L en "aplatissant" c'est à dire en décomposant les paires autant que possible et en supprimant les constantes:

- $\overline{\emptyset} = \emptyset$

- $\overline{a \cdot L} = \overline{L}$ si $a \in \mathcal{C}$
- $\overline{\langle\ u\ ,\ v\ \rangle \cdot L} = \overline{u \cdot v \cdot L}$
- $\overline{f(u) \cdot L} = f(u) \cdot \overline{L}$

On montre alors l'invariant suivant:

$\emptyset \rightarrow^* L$ avec $f(u) \in \overline{L}$ et $u \neq c$ ssi il existe une configuration γ telle que $\gamma_0 \vdash_M^* \gamma$ et $\overline{\gamma} = f(u)$

L'implication de gauche à droite est montrée par récurrence sur le nombre de transitions.

Cas de base: il n'y a aucune transition et donc la configuration du protocole est telle que $f(u) \notin \overline{L}$ pour tout u: il n'y a rien à prouver.

Récurrence: supposons maintenant que $\emptyset \rightarrow^* L \rightarrow L'$ et $f(u) \in \overline{L'}$. Si $f(u) \in \overline{L}$, il suffit s'appliquer l'hypothèse de récurrence. Sinon, L' est obtenu à partir de L en utilisant une des règles de protocole car pour toutes les autres règles $\overline{L'} \subseteq \overline{L}$.

Donc, ou bien $f(u)$ est obtenue par la règle $R1$ et on a bien $\gamma_0 \vdash_M^* \gamma_0$ avec $f(u) = \overline{\gamma_0}$, ou bien il existe $f(v) \in \overline{L}$ tel que $f(v) \rightarrow f(u)$ est une instance de l'une des règles. Par hypothèse de récurrence, il existe une configuration γ telle que $\gamma_0 \vdash_M^* \gamma$ et $\overline{\gamma} = f(v)$. Comme, par hypothèse, $f(u) \neq f(c)$, 4 cas doivent être envisagés, qui correspondent aux 4 types de règle $R2, R2b, R3, R4$:

R2: $v = \langle\ v_1\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ v_1'\ \rangle\ \rangle\ \rangle$ et $u = \langle\ \langle\ b\ ,\ v_1\ \rangle\ ,\ \langle\ q'\ ,\ v_1'\ \rangle\ \rangle$ et $\delta(q,a) = (q', b, \rightarrow)$. Par hypothèse de récurrence, il existe une configuration γ de M telle que $\gamma_0 \vdash_M^* \gamma$ et $\overline{\gamma} = f(v)$. Par définition du codage des configurations, $\gamma = (q, w_1, aw_1')$ et $\widetilde{\overline{w_1}} = v_1$ et $v_1' = \overline{w_1'}$. Dans ce cas $\gamma \vdash_M \gamma' = (q', w_1 b, q' w_1')$ et

$$\overline{\gamma'} = f(\Big\langle\ \widetilde{\overline{w_1 b}}\ ,\ \overline{q' w_1'}\ \Big\rangle) = f(\langle\ \overline{b \cdot \widetilde{\overline{w_1}}}\ ,\ \langle\ q'\ ,\ \overline{w_1'}\ \rangle\ \rangle) = f(\langle\ \langle\ b\ ,\ \widetilde{\overline{w_1}}\ \rangle\ ,\ \langle\ q'\ ,\ \overline{w_1'}\ \rangle\ \rangle) = f(u)$$

R2b : Ce cas, comme les suivants, sont semblables au premier. Nous abrégeons donc: $v = \langle\ v_1\ ,\ \langle\ q\ ,\ c\ \rangle\ \rangle = \overline{(q, w_1, \epsilon)} = \overline{\gamma}$, $u = \langle\ \langle\ b\ ,\ v_1\ \rangle\ ,\ \langle\ q'\ ,\ c\ \rangle\ \rangle = \overline{(q', w_1 b, \epsilon)} = \overline{\gamma'}$ et $\gamma \vdash_M \gamma'$.

R3 : $v = \langle\ \langle\ a'\ ,\ v_1\ \rangle\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ v_1'\ \rangle\ \rangle\ \rangle = \overline{(q, w_1 a', a w_1')} = \overline{\gamma}$,

$$u = \langle\ v_1\ ,\ \langle\ q'\ ,\ \langle\ a'\ ,\ \langle\ b\ ,\ v_1'\ \rangle\ \rangle\ \rangle\ \rangle = \overline{(q', w_1, a' b w_1')} = \overline{\gamma'}$$

et $\gamma \vdash_M \gamma'$.

R4 : $v = \langle\ v_1\ ,\ \langle\ q\ ,\ \langle\ a\ ,\ v_1'\ \rangle\ \rangle\ \rangle = \overline{(q, w_1, a w_1')} = \overline{\gamma}$, $u = \langle\ v_1\ ,\ \langle\ q\ ,\ \langle\ b\ ,\ v_1'\ \rangle\ \rangle\ \rangle = \overline{(q', w_1, b w_1')} = \overline{\gamma'}$ et $\gamma \vdash_M \gamma'$.

Dans tous les cas, $f(u) = \overline{\gamma'}$ et $\gamma \vdash_M \gamma'$.

L'implication de droite à gauche est montrée par récurrence sur le nombre d'étapes de calcul de la machine de Turing.

Cas de base Il suffit de remarquer que $\emptyset \rightarrow_6 c \rightarrow_1 \overline{\gamma_0}$.

Récurrence si $\gamma_0 \vdash_M^n \gamma_n \vdash_M \gamma_{n+1}$, par hypothèse de récurrence, $\emptyset \to^* L$ avec $\overline{\gamma_n} = f(u) \in \overline{L}$ et $u \neq c$. Par construction, si $\gamma_n = (q, w, w')$, $u = \langle\, \overline{\widetilde{w}} \,,\, \overline{qw'} \,\rangle$. Par exemple, si la machine effectue un mouvement gauche, $w' = aw'_1, w = w_1 c$ et $\delta(q, a) = (q', b, \leftarrow)$, alors $u = \langle\, \langle\, c \,,\, \overline{\widetilde{w_1}} \,\rangle \,,\, \langle\, q \,,\, \langle\, a \,,\, \overline{w'_1} \,\rangle \,\rangle \,\rangle$ et $\gamma_{n+1} = (q', w_1, cbw'_1)$, $\overline{\gamma_{n+1}} = f(\langle\, \overline{\widetilde{w_1}} \,,\, \overline{q'cbw'_1} \,\rangle)$. En utilisant l'instance $\sigma = \{x \mapsto \overline{\widetilde{w_1}}, y \mapsto \overline{w'_1}\}$ de la règle de protocole, on obtient $\overline{\gamma_{n+1}}$ à partir de $f(u)$: $L \to^* \overline{L} = L_1 \cdot f(u) \to L_1 \cdot \overline{\gamma_{n+1}}$.

Si maintenant $\gamma = (q_f, w_1, w_2)$ est une configuration d'arrêt de M, par l'invariant que nous venons de prouver, $\emptyset \to^* \overline{\gamma} \cdot L$ et $\overline{\gamma} = f(\langle\, \overline{\widetilde{w_1}} \,,\, \overline{w_2} \,\rangle)$. Par application de la dernière règle de protocole, $\overline{\gamma} \cdot L \to f(c) \cdot L$. Par application répétée de la règle de suppression, $f(c) \cdot L \to^* f(c)$. Ainsi $\emptyset \to^* f(c)$.

Réciproquement, si $\emptyset \to^* f(c)$, soit L la première configuration telle que $f(c) \in \overline{L}$: $\emptyset \to^* L_1 \to L \to^* f(c)$. La règle appliquée à L_1 ne peut être que la dernière règle de protocole (aucune autre règle ne peut faire apparaitre $f(c)$ dans $\overline{L}$). Par conséquent, $\overline{\gamma_f} \in \overline{L_1}$ pour une configuration finale γ_f de la machine M. Par l'invariant, $\gamma_0 \vdash_M^* \gamma_f$ et donc M s'arrête sur w.

Question 3

Il faut reprendre la preuve d'indécidabilité du pavage, mais cette fois en réduisant l'arrêt des MT et pas le non-arrêt. C'est très compliqué de réduire le non-pavage car il ne suffit pas de considérer une situation de blocage, mais toutes les situations de blocage.

On se donne donc une machine de Turing M et on réduit le problème de l'arrêt sur le mot vide. On suppose sans perte de généralité que, quand la machine de Turing s'arrête, c'est dans un (unique) état q_f. On suppose de plus que la machine n'écrit jamais de blanc (on a vu en cours que ce n'était pas une limitation).

On reprend donc les constructions du cours, avec les modifications suivantes:

- la tuile t_1 est BBq_f.
- On ajoute les compatibilités verticales (aq_fb, abq_f), (abq_f, abc), (q_fab, aq_fb), (abc, q_fbc) pour $a, b, c \in \Sigma$

Tout d'abord, supposons que M s'arrête sur w en n étapes. Notons $\gamma_i = w_i q_i w'_i$ la ième configuration de M ($i \leq n$), les mots w_i, w'_i ne contenant pas B. On peut remarquer que $|\gamma_i| \leq n$. Soit $\alpha_{j,i}$ la $j$ème lettre de γ_i si $j \leq |\gamma_i|$ et B si $|\gamma_i| < j \leq n+2$. On pose $p(j, i) = \alpha_{j,i}\alpha_{j+1,i}\alpha_{j+2,i}$. D'après le cours, il s'agit bien d'un pavage du rectangle $(n+2) \times n$ (excepté pour ce qui concerne la contrainte de la tuile $p(n+2, n)$). Comme la machine s'arrête, il existe un indice j tel que $\alpha_{j,n} = q_f$. Pour $n+1 \leq k \leq 2n+2-j$ on ajoute les nouvelles tuiles $p(i, k)$ $(0 \leq i \leq n+2)$: $p(i, k) = p(i, k-1)$ si $p(i, k-1) \in \Sigma^3$, $p(i, k) = aq_fb$ si $p(i, k-1) = q_fab$, $p(i, k) = abq_f$ si $p(i, k-1) = aq_fb$ et $p(i, k) = abc$ si $p(i, k-1) = abq_f$ et $p(i+1, k-1) = bq_fc$. (Dans ce dernier cas, on suppose $i < n+2$).

Par construction, on obtient un pavage du rectangle $(n+2) \times (2n+2-j)$ dans lequel la tuile du coin en haut à droite est t_1.

Supposons réciproquement que p est un pavage d'un rectangle $m \times n$ D'après le cours, si p est un pavage d'un rectangle $m \times \mathbb{N}$, qui n'utilise pas les nouvelles tuiles, alors, pour tout $i \leq m$, la $i$ème ligne code la $i$ème configuration de la machine de Turing. Comme la $i$ème configuration de la machine a une longueur (nombre de cases du ruban différentes de

B) bornée par $i + |w|$, ce résultat s'applique aussi si p est un pavage d'un rectangle $m \times k$ avec $k \geq m$.

Si on note $\alpha_{i,j}$ la première lettre de $p(i,j)$, pour tout $i \leq m$, il existe m_i et k_i tels que:

- $\alpha_{i,m_i} \in Q$ et pour tout $j \neq m_i$, $\alpha_{i,j} \notin Q$
- $\forall j > k_i$, $\alpha_{i,j} = B$ et $\forall j \leq k_i, \alpha_{i,j} \neq B$
- Si, pour tout $i \leq k$, $w_i = \alpha_{i,0} \cdots \alpha_{i,m_i-1}$, $q_i = \alpha_{i,m_i}$, $w'_i = \alpha_{i,m_{i+1}} \cdots \alpha_{i,k_i}$, alors, pour tout $i < k$, $(q_i, w_i, w'_i) \vdash_M (q_{i+1}, w_{i+1}, w'_{i+1})$
- (q_0, w_0, w'_0) est la configuration initiale de M.

S'il existe un pavage d'un rectangle tel que la tuile $p(n,m) = t_1$, comme la machine n'écrit pas de blanc et n'a aucune transition depuis son état final, toutes les configurations ont une longueur inférieure ou égale à n. Si j est le plus petit indice tel qu'il existe un k_j tel que $\alpha_{k_j,j} = q_f$, $(q_0, w_0, w'_0) \vdash_M \cdots \vdash_M (q_f, w_j, w'_j)$ et la machine s'arrête.

Question 4

L'idée est de coder les entiers à l'aide d'un chainage de noms.

$$f(\langle\ x\ ,\ c\ \rangle) \quad \to \quad \nu n.\ \langle\ f(\langle\ x\ ,\ n\ \rangle)\ ,\ f(\langle\ n\ ,\ c\ \rangle)\ \rangle$$

Par simplicité, on omet les paires à gauche et à droite des règles de protocole, lorsqu'elles sont au sommet.

Ensuite, ou bien on est sur un des bords gauche ou bas, et, dans ce cas, pour paver, on n'a besoin que d'une compatibilit'e, ou bien on est à l'intérieur du rectangle et deux compatibilités sont nécessaires pour continuer à paver. (Si on omet ce détail, on pourrait avoir une séquence de transitions du protocole qui conduit à t_1 mais ne remplit pas tout un rectangle).

Bootstrap: on démarre en associant la tuile t_0 à une case (n,n). On garde en mémoire que c'est une case du bas (constante b) et à gauche (constante g).

$$c \quad \to \quad \nu n.\ f(\langle\ \langle\ n\ ,\ n\ \rangle\ ,\ t_0\ \rangle),\ f(\langle\ n\ ,\ c\ \rangle),\ f(\langle\ b\ ,\ \langle\ n\ ,\ n\ \rangle\ \rangle),\ f(\langle\ g\ ,\ \langle\ n\ ,\ n\ \rangle\ \rangle)$$

Compat horizontale pour une tuile du bas: si $(t,t') \in H$,

$$f(\langle\ b\ ,\ \langle\ x\ ,\ z\ \rangle\ \rangle),\ f(\langle\ x\ ,\ y\ \rangle),\ f(\langle\ \langle\ x\ ,\ z\ \rangle\ ,\ t\ \rangle)$$
$$\to$$
$$f(\langle\ \langle\ y\ ,\ z\ \rangle\ ,\ t'\ \rangle),\ f(\langle\ b\ ,\ \langle\ y\ ,\ z\ \rangle\ \rangle)$$

Compat verticale pour une tuile de gauche: si $(t,t') \in V$,

$$f(\langle\ g\ ,\ \langle\ x\ ,\ z\ \rangle\ \rangle),\ f(\langle\ z\ ,\ y\ \rangle),\ f(\langle\ \langle\ x\ ,\ z\ \rangle\ ,\ t\ \rangle)$$
$$\to$$
$$f(\langle\ \langle\ x\ ,\ y\ \rangle\ ,\ t'\ \rangle),\ f(\langle\ g\ ,\ \langle\ x\ ,\ y\ \rangle\ \rangle)$$

Placement d'une tuile dans le cas général: si $(t,t'') \in V$ et $(t',t'') \in H$,

$$f(\langle\ \langle\ x\ ,\ y\ \rangle\ ,\ t\ \rangle),\ f(\langle\ \langle\ x'\ ,\ y'\ \rangle\ ,\ t'\ \rangle),\ f(\langle\ y\ ,\ y'\ \rangle),\ f(\langle\ x'\ ,\ x\ \rangle) \quad \to \quad f(\langle\ \langle\ x\ ,\ y'\ \rangle\ ,\ t''\ \rangle)$$

Si on arrive à t_1, on émet le secret (dès l'instant qu'une tuile est posée, on peut paver un rectangle dont le coin supérieur est cette tuile):

$$f(\langle\!\langle\ \langle\!\langle\ x\ ,\ y\ \rangle\!\rangle\ ,\ t_1\ \rangle\!\rangle) \quad \rightarrow \quad f(c)$$

Il existe une constante k (22 dans le codage ci-dessus, sauf erreur) qui borne la longueur des messages émis si on suppose que les variables ne sont instanciées que par des noms ou des constantes. On complète les membres droits (en rajoutant des constantes bidon) pour que tous les membres droits aient pour longueur k: les protocoles k-bornés ne peuvent s'exécuter qu'en remplaçant les variables par des noms ou des constantes.

On peut, sans perte de généralité, se ramener à des configurations qui sont des séquences non-ordonnées de messages qui sont des instances des membres gauche ou droit de règles de protocole par des noms ou des constantes, ou leurs sous-termes.

Montrons d'abord que, s'il existe un rectangle pavable par p et tel que $p(0,0) = t_0$ et $p(k,m) = t_1$, alors $\emptyset \rightarrow^* \nu\overline{n}.f(c)$. On suppose sans perte de généralité que $k \geq m$. On suppose aussi que chaque application de règle (sauf la suppression) est précédée d'une duplication, qui évite toute "perte de mémoire": les messages des configurations antérieures peuvent être réutilisés

On commence par engendrer les chainages:

$$\begin{aligned}\emptyset \rightarrow^* \nu n_1, \ldots, n_k.\ f(\langle\!\langle\ n_1\ ,\ n_2\ \rangle\!\rangle) \cdots f(\langle\!\langle\ n_{k-1}\ ,\ n_k\ \rangle\!\rangle) \cdot f(\langle\!\langle\ n_k\ ,\ c\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ ,\ t_0\ \rangle\!\rangle) \\ \cdot f(\langle\!\langle\ b\ ,\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ g\ ,\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle)\end{aligned}$$

en utilisant la règle de bootstrap et la règle de chainage de noms.

En utilisant la règle de duplication, les chainages sont dupliqués k fois: on ne répètera plus ces chainages dans les règles/configurations.

En utilisant la règle de compabitibilité horizontale en bas:

$$\begin{aligned}f(\langle\!\langle\ b\ ,\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ ,\ t_0\ \rangle\!\rangle) &\rightarrow f(\langle\!\langle\ b\ ,\ \langle\!\langle\ n_2\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_2\ ,\ n_1\ \rangle\!\rangle\ ,\ p(0,1)\ \rangle\!\rangle) \\ &\rightarrow \cdots \\ &\rightarrow f(\langle\!\langle\ b\ ,\ \langle\!\langle\ n_k\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_k\ ,\ n_1\ \rangle\!\rangle\ ,\ p(0,k)\ \rangle\!\rangle)\end{aligned}$$

En utilisant la rège de compatibilité verticale à gauche:

$$\begin{aligned}f(\langle\!\langle\ g\ ,\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_1\ ,\ n_1\ \rangle\!\rangle\ ,\ t_0\ \rangle\!\rangle) &\rightarrow f(\langle\!\langle\ g\ ,\ \langle\!\langle\ n_1\ ,\ n_2\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_1\ ,\ n_2\ \rangle\!\rangle\ ,\ p(1,0)\ \rangle\!\rangle) \\ &\rightarrow \cdots \\ &\rightarrow f(\langle\!\langle\ g\ ,\ \langle\!\langle\ n_1\ ,\ n_k\ \rangle\!\rangle\ \rangle\!\rangle) \cdot f(\langle\!\langle\ \langle\!\langle\ n_1\ ,\ n_k\ \rangle\!\rangle\ ,\ p(k,0)\ \rangle\!\rangle)\end{aligned}$$

Par récurrence sur (i,j), on produit aussi à l'aide de la règle générale de placement d'une tuile:

$$f(\langle\!\langle\ \langle\!\langle\ n_{i-1}\ ,\ n_j\ \rangle\!\rangle\ ,\ p(i-1,j)\ \rangle\!\rangle), f(\langle\!\langle\ \langle\!\langle\ n_i\ ,\ n_{j-1}\ \rangle\!\rangle\ ,\ p(i,j-1)\ \rangle\!\rangle) \ \rightarrow\ f(\langle\!\langle\ \langle\!\langle\ n_i\ ,\ n_j\ \rangle\!\rangle\ ,\ p(i,j)\ \rangle\!\rangle)$$

En particulier, on atteint une configuration contenant $f(\langle\!\langle\ \langle\!\langle\ n_k\ ,\ n_m\ \rangle\!\rangle\ ,\ t_1\ \rangle\!\rangle)$, à partir de laquelle on émet le secret, puis on efface tout ce qui n'est pas pertinent

Réciproquement, supposons que $\emptyset \to^* \nu\overline{n}.\ f(c)$. On peut supposer sans perte de généralité que les règles de suppression ne sont appliquées quà la fin : $\emptyset \to^* \nu\overline{n}.\ f(c) \cdot L_1 \to_5^* \nu\overline{n}.\ f(c)$

On a les invariants suivants (par définition des règles de protocole), si $\emptyset \to^* \nu\overline{n'}.\ L_0 \to \nu\overline{n}\ L$ et $f(u) \in L$:

1. si u est une paire $\langle\ v\ ,\ n\ \rangle$ où v est un nom, alors u est un nom.
2. si $u = \langle\ v\ ,\ c\ \rangle$, alors v est un nom
3. si $u = \langle\ v\ ,\ t\ \rangle$ où t est une tuile, alors v est une paire de noms
4. si $u = \langle\ b\ ,\ v\ \rangle$ ou $u = \langle\ g\ ,\ v\ \rangle$, alors v est une paire de noms.
5. si $u = \langle\ \langle\ n\ ,\ n'\ \rangle\ ,\ t\ \rangle$, alors ou bien $f(\langle\ b\ ,\ \langle\ n\ ,\ n'\ \rangle\ \rangle) \in L_0$ ou bien il existe un $n_0 \in \mathcal{N}$ et $t' \in T$ tels que $f(\langle\ n_0\ ,\ n'\ \rangle) \in L_0$ et $f(\langle\ \langle\ n\ ,\ n_0\ \rangle\ ,\ t'\ \rangle) \in L_0$ et $(t', t) \in V$
6. si $u = \langle\ \langle\ n\ ,\ n'\ \rangle\ ,\ t\ \rangle$, alors ou bien $f(\langle\ g\ ,\ \langle\ n\ ,\ n'\ \rangle\ \rangle) \in L_0$ ou bien il existe un $n_0 \in \mathcal{N}$ et $t' \in T$ tels que $f(\langle\ n_0\ ,\ n\ \rangle) \in L_0$ et $f(\langle\ \langle\ n_0\ ,\ n'\ \rangle\ ,\ t'\ \rangle) \in L_0$ et $(t', t) \in H$
7. si $f(\langle\ n_1\ ,\ n_2\ \rangle), \ldots, f(\langle\ n_{k-1}\ ,\ n_k\ \rangle) \in L_0$, alors $n_k \neq n_1$ (La règle de chainage ajoute toujours un nom frais).
8. si $f(\langle\ g\ ,\ \langle\ n\ ,\ n'\ \rangle\ \rangle) \in L_0$, alors, pour tout n'', $f(\langle\ n''\ ,\ n\ \rangle) \notin L_0$
9. si $f(\langle\ b\ ,\ \langle\ n\ ,\ n'\ \rangle\ \rangle) \in L_0$, alors pour tout n'', $f(\langle\ n''\ ,\ n'\ \rangle) \notin L_0$

Si L_0 est tel que $\emptyset \to^* \nu\overline{n}.L_0 \to \nu\overline{n'}.f(c) \cdot L_0'$ et $f(c) \notin L_0$ (autrement dit L_0 est la première séquence dans laquelle apparait $f(c)$, on reconstruit le pavage en numérotant les noms utilisés dans le chainage conduisant à cette solution (NB: il peut y avoir plusieurs chainages, dont certains ne conduisent à rien, mais il suffit d'en extraire un).

Soit $f(\langle\ \langle\ x\ ,\ y\ \rangle\ ,\ t_1\ \rangle) \in L_0$ (qui doit exister, sans quoi, on ne peut pas obtenir $f(c)$). D'après la propriété 3. ci-dessus, x et y sont des noms que nous notons α_0, β_0.

On définit ensuite par récurrence les suites $\alpha_i, \beta_j, t_{i,j}$ $(i \leq k_1, j \leq k_2)$ avec les propriétés suivantes:

- $f(\langle\ g\ ,\ \langle\ \alpha_{k_1}\ ,\ \beta_j\ \rangle\ \rangle) \in L_0$ pour tout $j \in [0..k_2]$
- $f(\langle\ b\ ,\ \langle\ \alpha_i\ ,\ \beta_{k_2}\ \rangle\ \rangle) \in L_0$ pourtout $i \in [0..k_1]$
- $f(\langle\ \alpha_i\ ,\ \alpha_{i-1}\ \rangle) \in L_0$ pour tout $k_1 \geq i \geq 1$
- $f(\langle\ \beta_j\ ,\ \beta_{j-1}\ \rangle) \in L_0$ pour tout $k_2 \geq j \geq 1$
- $f(\langle\ \langle\ \alpha_i\ ,\ \beta_j\ \rangle\ ,\ t_{i,j}\ \rangle) \in L_0$ pour tous $i, j \in [0..k_1] \times [0..k_2]$
- $(t_{i,j}, t_{i-1,j}) \in H$ pour tous $i, j \in [1..k_1] \times [0..k_2]$
- $(t_{i,j}, t_{i,j-1}) \in V$ pour tous $i, j \in [0..k_1] \times [1..k_2]$

Pour l'étape de récurrence, il suffit d'appliquer les invariants 5 et 6. Enfin, on a aussi $f(\langle\ g\ ,\ \langle\ \alpha_{k_1}\ ,\ \beta_{k_2}\ \rangle\ \rangle), f(\langle\ b\ ,\ \langle\ \alpha_{k_1}\ ,\ \beta_{k_2}\ \rangle\ \rangle) \in L_0$ et, par les invariants 7,8,9, ceci implique que $\alpha_{k_1} = \beta_{k_2}$.

On construit alors le pavage du rectangle $k_1 \times k_2$ comme suit: $p(i, j) = t_{k_1-j,k_2-j}$. Les énoncés ci-dessus montrent que c'est bien un pavage.