6.7.1 Extension de la notion de décidabilité

La notion de réduction ne requiert pas a priori que l'ensemble S dans lequel varie la donnée du problème soit récursif. Cependant, pour que le probème de décision soit équivalent à la décision de $Q \cap S$, il faut que S soit récursif.

Definition 6.7.1 *Si $S, Q \subseteq \Sigma^*$, le problème*

Donnée : $D \in S$

Question : Q

est indécidable, s'il n'existe aucune machine de Turing M qui s'arrête sur toute donnée $d \in S$ et telle que $L(M) \cap S = Q \cap S$.

Lorsque S est récursif, un tel problème est décidable, si et seulement si $Q \cap S$ est récursif.

Les méthodes de réduction permettent de prouver l'indécidabilité dans ce sens plus général.

6.8 Théorème de Rice

Théorème 6.8.1 *Si $\mathcal{P}$ est une propriété non triviale des langages récursivement énumérables, alors $\mathcal{P}$ est indécidables.*

Nous donnons ci-dessus l'énoncé "classique", mais en voici une version plus précis :

Pour tout ensemble $\mathcal{P}$ de (codes de) machines de Turing tel que :

1. pour toutes machines M, M' si $< M > \in \mathcal{P}$ et $L(M) = L(M')$ alors $< M' > \in \mathcal{P}$
2. on peut exhiber des machines M_1, M_2 telles que $< M_1 > \in \mathcal{P}$ et $< M_2 > \notin \mathcal{P}$

alors le problème suivant est indécidable :

Donnée : $< M >$

Question : $< M > \in \mathcal{P}$?

Pour prouver ce résultat, nous utiliserons une réduction du problème de l'arrêt, un type de réduction qui sera très fréquemment utilisé par la suite.

Soit $\mathcal{P}$ un sous-ensemble non-trivial des langages récursivement énumérables. $\mathcal{P}$ est récursif ssi $\overline{\mathcal{P}}$ est récursif. On peut donc supposer sans perte de généralité que $\emptyset \notin \mathcal{P}$. Comme $\mathcal{P}$ est non vide, soit $L \in \mathcal{P}$ et M_L une machine qui accepte L.

On réduit le problème de l'arrêt

Donnée : $< M, x >$ où M est une machine de Turing sur Σ et $x \in \Sigma^*$

Question : M s'arrête-t-elle sur x ?

au problème de l'appartenance à $\mathcal{P}$ en construisant, à partir de la donnée $< M, x >$ du problème de l'arrêt, une donnée M_x du problème de l'appartenance à $\mathcal{P}$, de telle manière à ce que $M_x \in \mathcal{P}$ ssi M s'arrête sur x.

Soit M_{arret} une machine qui accepte L_{arret}. M_x est une machine qui, sur la donnée y, commence par simuler M sur x et, en cas d'arrêt, simule ensuite M_L sur y. On remarque que $L(M_x) \in \{L, \emptyset\}$ et donc $L(M_x) \in \mathcal{P}$ ssi M s'arrête sur x.

Exercice 162 (4)
Dire si les problèmes suivants sont décidables ou non (justifier) :

1. **Donnée :** le code $< M >$ d'une machine de Turing

   Question : M s'arrête-t-elle sur le mot vide ?
2. **Donnée :** le code $< M >$ d'une machine de Turing

   Question : M s'arrête-t-elle sur au moins une donnée ?
3. **Donnée :** les codes $< M >$ et $< M' >$ de deux machines de Turing

   Question : $L(M) = L(M')$?
4. **Donnée :** le code $< M >$ d'une machine de Turing et un mot w.

   Question : Est ce que la machine M boucle sur w ?

   On dit que M boucle sur w si, de la configuration initiale γ_0 on peut atteindre une configuration γ, de laquelle on peut à nouveau atteindre γ en au moins une étape : $\gamma_0 \vdash_M^* \gamma \vdash_M^+ \gamma$.
5. **Donnée :** le code $< M, w >$ d'une machine de Turing et d'un mot w et un entier n (en base 2)

   Question : M accepte-t-elle w après au plus n transitions ?
6. **Donnée :** le code $< M, w >$ d'une machine de Turing et d'un mot w et un entier n (en base 2)

   Question : M accepte-t-elle w après au moins n transitions ?
7. **Donnée :** le code $< M >$ d'une machine de Turing

   Question : Est ce que le complémentaire de $L(M)$ est récursivement énumérable ?
8. **Donnée :** Le code d'une machine de Turing M_1 et le code d'une machine de Turing M_2 qui s'arrête, pour tout mot d'entrée w après au plus $2 \times |w|$ transitions

   Question : Pour tout mot w, $M_1(w) = M_2(w)$
9. **Donnée :** Le code d'une machine de Turing M

   Question : il existe deux mots w_1, w_2 de même longueur tels que $w_1, w_2 \in L(M)$.
10. **Donnée :** Le code d'une machine de Turing M

    Question : M calcule-t-elle en temps polynomial ?

Exercice 163 (5)
Dire, en le justifiant, si les problèmes suivants sont décidables :

1. **Donnée :** Le code d'une machine de Turing M qui s'arrête sur toutes ses entrées.

   Question : M calcule en temps polynômial

2. **Donnée :** Le code de deux machines de Turing M_1, M_2 qui calculent en temps polynomial.

   Question : $L(M_1) \cap L(M_2) = \emptyset$

Exercice 164 (5)
Un *automate linéairement borné* est une machine de Turing qui, lorsqu'elle lit un blanc, écrit un blanc et se déplace vers la gauche.

Montrer que l'arrêt universel des automates linéairement bornés est indécidable :

Donnée : $< M >$ où M est un automate linéairement borné

Question : est ce que M s'arrête sur toute donnée ?

Exercice 165 (5)
Donner une fonction calculable dont l'image est indécidable.

Exercice 166
Un *système de réécriture (de mots)* $\mathcal{R}$, sur l'alphabet Σ est un ensemble fini de paires de mots $(u_i, v_i) \in \Sigma^* \times \Sigma^*$. La *relation de réécriture* associée à un tel système de réécriture est la relation $\rightarrow_{\mathcal{R}} \subseteq \Sigma^* \times \Sigma^*$ définie par

$$u \rightarrow_{\mathcal{R}} v \quad \text{ssi} \quad \exists i, \exists w, x \in \Sigma^*,\ u = wu_ix \wedge v = wv_ix$$

La *relation de réduction* $\xrightarrow[\mathcal{R}]{*}$ associée à un système de réécriture $\mathcal{R}$ est la fermeture réflexive et transitive de la relation de réécriture :

$$\begin{array}{lcl} \xrightarrow[\mathcal{R}]{*} & = & \bigcup_{n=0}^{+\infty} \xrightarrow[\mathcal{R}]{n} \\ u \xrightarrow[\mathcal{R}]{0} v & \text{ssi} & u = v \\ u \xrightarrow[\mathcal{R}]{n} v & \text{ssi} & \exists w. u \rightarrow_{\mathcal{R}} w \wedge w \xrightarrow[\mathcal{R}]{n-1} v \end{array}$$

Par exemple, soit $\mathcal{R} = \{c \rightarrow abaca; c \rightarrow bcbabab; aca \rightarrow d;\ bcb \rightarrow d; ada \rightarrow d; bdb \rightarrow b\}$,sur l'alphabet $\Sigma = \{a, b, c, d\}$. $c \xrightarrow[\mathcal{R}]{*} d$, en effet :

$$c \rightarrow_{\mathcal{R}} abaca \rightarrow_{\mathcal{R}} ababcbababa \rightarrow_{\mathcal{R}} abababacabababa \rightarrow_{\mathcal{R}} ababadbababa \rightarrow_{\mathcal{R}} \\ ababadababa \rightarrow_{\mathcal{R}} ababdbaba \rightarrow_{\mathcal{R}} abadaba \rightarrow_{\mathcal{R}} abdba \rightarrow_{\mathcal{R}} ada \rightarrow_{\mathcal{R}} d$$

Montrer que le problème suivant, appelé *accessibilité* est indécidable :

Donnée : deux mots $u, v \in \Sigma^*$, un système de réécriture $\mathcal{R}$

Question : est-ce que $u \xrightarrow[\mathcal{R}]{*} v$?

Exercice 167

1. Si $n \in \mathbb{N}$, on note $\overline{n}$ le mot 0^n, de longueur n.

   Soit M une machine de Turing. Montrer qu'on peut construire une machine M_v telle que :

   (a) étant donné $w = \gamma_1 \# \overline{n} \#$, M_v vérifie que γ_1 est une configuration de M accessible en n étapes par M à partir de la configuration initiale $(\epsilon, q_0^M, \$_M)$ et s'arrête dans la configuration $(\$_v, q_1, \gamma_2 \# \overline{n+1} \#)$ si c'est le cas, où $\gamma_1 \vdash_M \gamma_2$

(b) quelle que soit la configuration γ de M_v (même une configuration inaccessible), il n'existe aucune suite infinie $\gamma_i, i \in \mathbb{N}$ telle que $\gamma_0 = \gamma$ et, pour tout i, $\gamma_i \vdash_{M_v} \gamma_{i+1}$.

2. Montrer que le problème suivant est indécidable :

   Donnée : Une machine de Turing M

   Question : Existe-t-il une suite infinie de configurations (w_i, q_i, x_i) telle que, pour tout i, $(w_i, q_i, x_i) \vdash_M (w_{i+1}, q_{i+1}, x_{i+1})$?

Exercice 168 (5)

Un *Système de Post* P est donné par un ensemble fini de paires de mots $(\alpha, \beta) \in (\Sigma^*)^2$ et un *mot de départ* γ. Une *configuration* d'un tel système est un mot $w \in \Sigma^*$. On peut effectuer un mouvement de w vers w' s'il existe une paire (α, β) dans le système et un mot δ tels que $w = \alpha\delta$ et $w' = \delta\beta$.

Montrer que le problème

Donnée : un système de post P et un mot w

Question : peut-on atteindre une configuration w de P (après un nombre quelconque de mouvements)

est indécidable.

Exercice 169 (7)

Soit $\mathcal{P}$ une propriété des langages récursivement énumérables. ($\mathcal{P}$ est un ensemble de codes de machines de Turing $< M >$ tel que, si $L(M) = L(M')$ et $< M > \in \mathcal{P}$, alors $< M' > \in \mathcal{P}$. Par abus de langage on dira alors que $L \in \mathcal{P}$ s'il existe une machine de Turing M telle que $L(M) = L$ et $< M > \in \mathcal{P}$)

1. Montrer que, s'il existe deux langages récursivement énumérables $L_1 \subseteq L_2$ tels que $L_1 \in \mathcal{P}$ et $L_2 \notin \mathcal{P}$, alors $\mathcal{P}$ n'est pas récursivement énumérable.
2. Montrer que s'il existe $L \in \mathcal{P}$ tel que, pour tout $L' \subseteq L$, ou bien L' est infini, ou bien $L' \notin \mathcal{P}$, alors $\mathcal{P}$ n'est pas récursivement énérable.
3. On considère une application c (calculable) injective qui associe à chaque sous-ensemble fini de Σ^* un mot de Σ^*. Montrer que, si $\mathcal{P}$ est récursivement énumérable, $\mathsf{Fin}(\mathcal{P}) = \{c(L)(M) | < M > \in \mathcal{P}, L(M) \text{ fini }\}$ est récursivement énumérable.
4. En déduire que $\mathcal{P}$ est récursivement énumérable si et seulement si les trois propriétés suivantes sont satisfaites :
   (a) $\mathsf{Fin}(\mathcal{P})$ est récursivement énumérable
   (b) Tout langage de $\mathcal{P}$ contient un langage fini dans $\mathcal{P}$
   (c) Pour tous langages $L \subseteq L'$ récursivement énumérables, si $L \in \mathcal{P}$, alors $L' \in \mathcal{P}$.
5. Montrer que les propriétés suivantes des langages récursivement énumérables ne sont pas récursivement énumérables :
   (a) $\mathcal{P} = \{\emptyset\}$
   (b) $\mathcal{P} = \Sigma^*$
   (c) $\mathcal{P}$ est l'ensemble des langages finis

(d) $\mathcal{P}$ est l'ensemble des langages reconnaissables.

(e) $\mathcal{P}$ est l'ensemble des langages récursifs.

(f) $\mathcal{P}$ est l'ensemble des langages récursivement énumérables, mais pas récursifs

Exercice 170 (5)
Une *machine à registres* est donnée par un ensemble fini d'états (contenant les états **accept** et **reject**), un état initial, N *registres* $r_1, \ldots, r_N$ et une fonction de transition de $Q \times \{0,1\}^N$ dans $Q \times \{+1, 0, -1\}^N$: $\delta(q, \alpha_1, \ldots, \alpha_N) = (q', d_1, \ldots, d_N)$ telle que si $\alpha_i = 0$, alors $d_i \neq -1$.

Une *configuration* de la machine est donnée par N entiers en base 1 (les contenus de registres) et un état.

Un mouvement de la machine est une relation entre configurations : $q, k_1, \ldots, k_N \vdash_M q', k'_1, \ldots, k'_N$ ssi il existe une transition de la machine $q, \alpha_1, \ldots, \alpha_N \mapsto q', d_1, \ldots, d_N$ telle que $\alpha_i = 0$ si $k_i = 0$ et $\alpha_i = 1$ sinon et, pour tout i, $k'_i = k_i + d_i$.

Un *calcul* de la machine sur la donnée n_0 est une suite de configurations, la première étant la configuration initiale $(q_0, n_0, 0 \ldots, 0)$ et telle que la $i$ème configuration est obtenue par un mouvement de la machine sur la $i-1$ème configuration.

Une machine à registres M *accepte* l'entier n_0, si le calcul de M sur n s'arrête en **accept**.

1. Soit $k > 1$. Montrer qu'on peut construire une machine à registresM_k telle que, sur la donnée $n \in \mathbb{N}$, M_k s'arrête dans une configuration où le premier registre contient q et le deuxième registre contient r où q, r sont respectivement le quotient et le reste de la division euclidienne de n par k.
2. Soit $\Sigma \setminus \{\$, B\} = \{a_1, \ldots, a_k\}$. Pour $w \in (\Sigma \setminus \{\$, B\})^*$, on note $c_k(w)$ l'entier dont l'écriture en base $k+1$ est w.

   Montrer que, si L est récursivement énumérable, il existe une machine à 4 registres qui accepte $\{c_k(w) \mid w \in L\}$.
3. Montrer le même résultat que celui de la question précédente, mais avec une machine à 2 registres (au lieu de 4). Ind : on pourra considérer le codage de 4 entiers en un seul par $\overline{(n_1, n_2, n_3, n_4)} = 2^{n_1} \times 3^{n_2} \times 5^{n_3} \times 7^{n_4}$.
4. Montrer que le problème de savoir si une machine à 2 registres accepte au moins un entier est indécidable.

6.9 Problèmes de pavages

Le problème de pavage de $\mathbb{N}\times\mathbb{N}$ (les définitions sont semblables pour d'autres sous-ensembles de $\mathbb{Z} \times \mathbb{Z}$) est défini par :

Donnée : un ensemble fini $T = \{t_0, \ldots, t_k\}$ de *tuiles* et deux sous-ensembles H, V de $T \times T$. (Les relations de compatibilité horizontale et verticale).

Question : existe-t-il une fonction de pavage $f : \mathbb{N} \times \mathbb{N} \mapsto T$ telle que $f(0,0) = t_0$ et, pour tout $i, j \in \mathbb{N}$, $(f(i,j), f(i,j+1)) \in H$, $(f(i,j), f(i+1,j)) \in V$.

Théorème 6.9.1 *Le problème de savoir, étant donnés T, V, H si $\mathbb{N} \times \mathbb{N}$ est pavable, est indécidable.*

Pour simplifier, notons d'abord que le problème $\mathcal{P}$:

Donnée : une machine de Turing M, qui ne revient jamais en début de ruban, ne revient jamais dans l'état initial, n'écrit jamais de blancs.

Question : Est ce que M ne s'arrête pas sur le mot vide ?

est indécidable.

Tout d'abord, le problème du non-arrêt sur le mot vide est indécidable. Il suffit en effet de réduire le problème du non-arrêt en construisant à partir de $< M, w >$ une machine M_w qui commence par écrire w sur le ruban, puis simule M.

Étant donnée une machine de Turing M_1, on construit ensuite une machine M, qui ne revient jamais en début de ruban, ne revient jamais dans létat initial, nécrit jamais B et s'arrête sur le mot vide ssi M_1 s'arrête sur le mot vide.

On ajoute pour cela deux états q_0, q_1 à Q_{M_1}, un symbole \$ et un symbole B ; M commence par avancer (en passant de q_0 à q_1) puis écrit $\$_{M_1}$, passe dans l'état initial de M_1 et simule M ; chaque transition $\delta_{M_1}(q, B_{M_1}) = (q', a, m)$ est doublée d'une transition $\delta_{M'}(q, B) = (q', a, m)$.

On réduit ensuite $\mathcal{P}$ au problème de pavage. On choisit pour $T = (\Sigma \cup Q)^3 \cap \Sigma^*(Q + \epsilon)\Sigma^*$ (autrement dit, les mots de longueur 3 contenant au plus un symbole de Q).

$$H = \{(atc, tcb) \mid atc, tcb \in T, a, c, b \in \Sigma \cup Q, c = B \Rightarrow b = B\}$$

$$
\begin{array}{rllll}
V = & \{ & (bcq, bca') & \mid b, c \in \Sigma, \delta(q,a) = (q', a', \rightarrow) & \} \\
\cup & \{ & (cqa, ca'q') & \mid c \in \Sigma, \delta(q,a) = (q', a', \rightarrow) & \} \\
\cup & \{ & (qad, a'q'd) & \mid d \in \Sigma, \delta(q,a) = (q', a', \rightarrow) & \} \\
\cup & \{ & (ade, q'de) & \mid d, e \in \Sigma, \delta(q,a) = (q', a', \rightarrow), a \neq \$ & \} \\
\cup & \{ & (bcd, bcq') & \mid b, c, d \in \Sigma, \delta(q,a) = (q', a', \leftarrow) & \} \\
\cup & \{ & (cdq, cq'd) & \mid c, d \in \Sigma, \delta(q,a) = (q', a', \leftarrow) & \} \\
\cup & \{ & (dqa, q'da') & \mid d \in \Sigma, \delta(q,a) = (q', a', \leftarrow) & \} \\
\cup & \{ & (qae, da'e) & \mid d, e \in \Sigma, \delta(q,a) = (q', a', \leftarrow) & \} \\
\cup & \{ & (aef, a'e, f) & \mid e, f \in \Sigma, \delta(q,a) = (q', a', \leftarrow) & \} \\
\cup & \{ & (bcq, bcq') & \mid b, c \in \Sigma, \delta(q,a) = (q', a', \downarrow) & \} \\
\cup & \{ & (cqa, cq'a') & \mid c \in \Sigma, \delta(q,a) = (q', a', \downarrow) & \} \\
\cup & \{ & (qad, q'a'd) & \mid d \in \Sigma, \delta(q,a) = (q', a', \downarrow) & \} \\
\cup & \{ & (ade, a'de) & \mid d, e \in \Sigma, \delta(q,a) = (q', a', \downarrow) & \} \\
\cup & \{ & (\$BB, q_1BB) & \mid \delta(q_0, \$) = (q_1, \$, \rightarrow) & \} \\
\cup & \{ & (\alpha, \alpha) & \mid \alpha \in \Sigma^3 & \}
\end{array}
$$

Les premières pièces verticales correspondent à des fenêtres glissantes sur les séquences

Mouvement droit :

$$
\begin{array}{cccccc}
b & c & a' & q' & d & e \\
b & c & q & a & d & e
\end{array}
$$

Mouvement gauche :

$$
\begin{array}{ccccccc}
b & c & q' & d & a' & e & f \\
b & c & d & q & a & e & f
\end{array}
$$

Mouvement sur place :

$$
\begin{array}{cccccc}
b & c & q' & a' & d & e \\
b & c & q & a & d & e
\end{array}
$$

Enfin, on demande que le pavage satisfasse $f(0,0) = q_0\$B$.

Si M ne s'arrête pas sur le mot vide. Pour $n \in \mathbb{N}$, on note γ_n le codage de la $n$ième configuration atteinte par M : $\gamma_n = w_n q w'_n$ et $\alpha_{i,n}$ est la ième lettre de γ_n si i est inférieur ou égal à la longueur de γ_n et B sinon.

On considère alors $f(i,j) = \alpha_{i,j}\alpha_{i+1,j}\alpha_{i+2,j}$. Pour tous i, j, $\alpha_{i,j} \in T$ et $f(0,0) = q_0\$B$.

Montrons que f est un pavage :

— pour tous i, j, $(f(i,j), f(i+1,j)) \in H$, par construction

— Pour tout n, il existe un unique entier m_n tel que $\alpha_{m_n,n} \in Q$. Par hypothèse sur M, $m_n = 0$ ssi $n = 0$. Comme γ_{n+1} est la configuration obtenue par un mouvement de M à partir de γ_n, $\forall n, \forall i < m_n - 1. \alpha_{i,n} = \alpha_{i,n+1}$ et $\forall n, \forall i > m_n + 1, \alpha_{i,n} = \alpha_{i,n+1}$. En particulier, pour tout $i \notin \{m_n - 3, m_n - 2, m_n - 1, m_n, m_n + 1\}$, $f(i,n) = f(i,n+1) \in \Sigma^3$. Donc $(f(i,n,i), f(i,n+1)) \in V$ dans ces cas.

Soit

$$\alpha_{m_n-3,n}\alpha_{m_n-2,n}\alpha_{m_n-1,n}\alpha_{m_n,n}\alpha_{m_n+1,n}\alpha_{m_n+2,n}\alpha_{m_n+3,n}\} = a_1a_2a_3qa_4a_5a_6$$

Si $\delta(q, a_4) = q', b \rightarrow$, alors

$$\alpha_{m_n-3,n+1}\alpha_{m_n-2,n+1}\alpha_{m_n-1,n+1}\alpha_{m_n,n+1}\alpha_{m_n+1,n+1}\alpha_{m_n+2,n+1}\alpha_{m_n+3,n+1} = a_1a_2a_3bq'a_5a_6$$

On vérifie alors que $(f(m_n-3, n), f(m_n-3, n+1)) = (a_1a_2a_3, a_1a_2a_3) \in V$, $(f(m_n - 2, n), f(m_n - 2, n + 1)) = (a_2a_3q, a_2a_3b) \in V$, $(f(m_n - 1, n), f(m_n - 1, n + 1)) = (a_3qa_4, a_3bq') \in V$, $(f(m_n, n), f(m_n, n + 1)) = (qa_4a_5, bq'a_5) \in V$, $(f(m_n+1, n), f(m_n+1, n+1)) = (a_4a_5a_6, q'a_5a_6) \in V$. Dans ce dernier cas, a_4 est en effet différent de \$, sauf si $q = q_0, q' = q_1, a_5 = a_6 = B$, par hypothèse sur M. Et dans ce cas particulier, on a aussi $(\$BB, q_1BB) \in V$.
Si $\delta(q, a_4) = q', b \leftarrow$ ou bien $\delta(q, a_4) = q', b, \downarrow$, on vérifie de même que les relations de compatibilité verticale sont satisfaites.

Si f est un pavage du quart de plan. On note $\alpha_{i,j}$ la première lettre de $f(i, j)$. On montre alors, par récurrence sur n que la $n$ème ligne est un codage de la configuration atteinte par M après n mouvements : pour tout n, il existe m_n et k_n tels que

— $\alpha_{m_n,n} \in Q$ et $\forall i \neq m_n$, $\alpha_{i,n} \in \Sigma$

— $\forall i > k_n, \alpha_{i,} = B$ et $\forall i \leq k_n, \alpha_{i,n} \neq B$.

— Si $w_n = \alpha_{0,n} \cdots \alpha_{m_n-1,n}$, $q_n = \alpha_{m_n,n}$, $w'_n = \alpha_{m_n+1,n} \cdots \alpha_{k_n,n}$, alors $(w_n, q_n, w'_n) \vdash_M (w_{n+1}, q_{n+1}, w'_{n+1})$

— (w_0, q_0, w'_0) est la configuration initiale de M

— pour $n = 0$, la première ligne contient la configuration initiale ; $f(0, 0) = q_0\$B$ et donc $f(1, 0) = \$BB$ et $f(2, 0) = BBB$. Par récurrence sur $m \geq 0$, $f(m + 2, 0) = B^3$, par compatibilité horizontale.

— pour $n = 1$, par compatibilité verticale, $f(0, 1) = \$q_1B$ et, de même que ci-dessus, $f(1, 1) = q_1BB$ et pour $i \geq 2, f(i, 1) = B^3$.

— Supposons la propriété vraie pour $n \geq 1$ et soit $\gamma_n = w_nq_nw'_n$. $m_n > 0$, par hypothèse sur M.

Lemme. Remarquons d'abord que, si $f(i, n), f(i + 1, n), f(i + 2, n) \in \Sigma^3$, alors $f(i + 1, n + 1) = f(i + 1, n)$, par compatibilités horizontales et verticales : lorsque $f(i + 1, n) \in \Sigma^3$, $f(i + 1, n + 1) \neq f(i + 1, n)$ n'est possible que dans l'un des cas suivants, par compatibilité verticale :

1. $f(i + 1, n) = ade$, $d, e \in \Sigma$, $\delta(q, a) = (q', a', \rightarrow)$. Dans ce cas, $f(i + 1, n + 1) = q'de$
2. $f(i + 1, n) = bcd$, $b, c, d \in \Sigma$, $\delta(q, a) = (q', a', \leftarrow)$. Dans ce cas, $f(i + 1, n + 1) = bcq'$
3. $f(i + 1, n) = aef$, $e, f \in \Sigma$, $\delta(q, a) = (q', a', \leftarrow)$. Dans ce cas, $f(i + 1, n + 1) = a'ef$
4. $f(i + 1, n) = ade$, $d, e \in \Sigma$, $\delta(q, a) = (q', a', \downarrow)$. Dans ce cas $f(i + 1, n + 1) = a'de$

— Dans le premier cas, par compatibilité horizontale, $f(i, n+1) = cq'd$ et par compatibilité verticale, on ne peut pas avoir $f(i, n) \in \Sigma^3$.
— Dans le deuxième cas, par compatibilité horizontale, $f(i+2, n+1) = cq'd$ et, par compatibilité verticale, on ne peut pas avoir $f(i+2, n) \in \Sigma^3$.
— Dans le toisième cas, par compatibilités horizontales, $f(i, n) = \alpha a e$ et $f(i, n+1) = \beta a' \gamma$. Par compatibilité verticale, ceci n'est possible que quand $\alpha \in Q$
— Le dernier cas est semblable au précédent.

Revenons à la preuve de la récurrence. Comme

$$(\alpha_{n,m_n-1} q_n \alpha_{n,m_n+1}, \alpha_{n+1,m_n-1} \alpha_{n+1,m_n} \alpha_{n+1,m_n+1}) \in V$$

par définition de V seuls trois cas se présentent :

1. $\delta(q_n, \alpha_{n,m_n+1}) = (q, a', \rightarrow)$ **et** $\alpha_{m_n-1,n} = \alpha_{m_n-1,n+1}$ **et** $\alpha_{m_n,n+1} = a'$ **et** $\alpha_{m_n+1,n+1} = q$**.**

1.1. Montrons d'abord dans ce cas, par récurrence sur i**, que** $\alpha_{m_n-i-1,n+1} = \alpha_{m_n-i-1,n}$**.** C'est le cas par hypothèse quand $i = 0$. Supposons $m_n > 1$ (sinon, il n'y a plus rien à démontrer). Pour $i = 1$, $f(m_n - 2, n) = \alpha_{m_n-2,n} \alpha_{.m_n-1,n} q_n$ et $f(m_n - 2, n+1) = \alpha_{m_n-2,n+1}, \alpha_{m_n-1,n} a'$. Par définition de V, $(f(m_n - 2, n), f(m_n - 2, n+1)) \in V$ entraine $\alpha_{m_n-2,n+1} = \alpha_{m_n-2,n}$. Si $i > 1$, alors $f(m_n - i - 1, n) \in \Sigma^3$ (puisque, par hypothèse de récurrence, γ_n est une configuration de M). Par définition de V, trois cas sont alors a priori possibles pour $f(m_n - i - 1, n+1)$:

— ou bien $f(m_n - i - 1, n+1) = \alpha_{m_n-i-1,n} \alpha_{m_n-i,n} q$ pour un certain $q \in Q$.
— ou bien $f(m_n - i - 1, n+1) = q \alpha_{m_n-i,n} \alpha_{m_n-i+1,n}$, pour un certain $q \in Q$.
— ou bien $f(m_n - i - 1, n+1) = c \alpha_{m_n-i,n} \alpha_{m_n-i+1,n}$ avec $c \in \Sigma$ et $\delta(q, \alpha_{m_n-i-1,n}) = (q', c, \downarrow)$

Le premier cas est impossible puisqu'on devrait avoir $f(m_n - i, n+1) \in \Sigma \cdot Q \cdot \Sigma$ par compatibilité horizontale, ce qui contredit l'hypothèse de récurrence.

Dans le deuxième cas, par construction de V, $\alpha_{m_n-i-1,n} \neq \$$ et donc (puisque γ_n est une configuration de M), $m_n > i+1$. Alors $f(m_n - i - 2, n), f(m_n - i - 1, n), f(m_n - i, n) \in \Sigma^3$ ce qui entraine, comme nous l'avons vu plus haut dans le lemme, $f(m_n - i, n+1) = f(m_n - i, n)$.

Dans le dernier cas, $\alpha_{m_n-i-1,n} \neq \$$ (puisqu'il n'y a pas de mouvement à droite), et donc, comme dans le cas précédent, $f(m_n - i, n+1) = f(m_n - i, n)$.

Ceci termine la récurrence : pour tout $k < m_n$, $\alpha_{k,n+1} = \alpha_{k,n}$.

1.2 Notons ensuite que $\alpha_{m_n+2,n+1} = \alpha_{m_n+2,n}$ **et** $\alpha_{m_n+3,n} = \alpha_{m_n+3,n+1}$**.** :
$(q_n \alpha_{m_n+1,n} \alpha_{m_n+2,n}, a' q \alpha_{m_n+2,n+1}) \in V$. Par définition de V, ceci

n'est possible (avec $q_n, q \in Q$) que quand les deux dernières lettres sont identiques. De même, $(abc, qbc') \in V$ seulement si $c = c'$ et donc $\alpha_{n,m_n+3} = \alpha_{n+1,m_n+3}$.

1.3. Pour $i > 1$**,** $f(m_n + i, n + 1) = f(m_n + i, n)$
car $f(m_n + i - 1, n), f(m_n + i, n), f(m_n + i + 1, n) \in \Sigma^3$ et d'après le lemme prouvé plus haut.

2. $\delta(q_n, \alpha_{m_n+1,n}) = (q, b, \leftarrow)$ **et** $\alpha_{m_n-1,n+1} = q$ **et** $\alpha_{m_n,n+1} = \alpha_{m_n-1,n}$ **et** $\alpha_{m_n+1,n+1} = b$**.** On procède de la même manière que ci-dessus.

3. $\delta(q_n, \alpha_{m_n+1,n}) = (q.b, \downarrow)$ **et** $\alpha_{m_n-1,n+1} = \alpha_{m_n-1,n}$ **et** $\alpha_{m_n,n+1} = q$ **et** $\alpha_{m_n+1,n+1} = b$**.** On procède de la même manière que ci-dessus.

On conclut donc que l'on peut paver le quart de plan si et seulement si, pour tout n, il existe une séquence de configurations $\gamma_0 \vdash_M \cdots \vdash \gamma_{n-1} \vdash_M \gamma_n$. Autrement dit, on peut paver le quart de plan si et seulement si M ne s'arrête pas sur le mot vide.

Exercice 171
Dans cette partie, on se donne un ensemble fini $C = \{W, P, R, G, B ...\}$ de *couleurs*. Un *domino* est un quadruplet de couleurs $(c_L, c_H, c_R, C_B) \in C^4$, que l'on peut représenter graphiquement comme sur la figure 6.2. Étant donné un ensemble fini D de dominos et un domino distingué $d_0 \in D$, un *pavage* de $\mathbb{N} \times \mathbb{N}$ par D est une application p de $\mathbb{N} \times \mathbb{N}$ dans D telle que :

1. $p(0, 0) = d_0$
2. Si $(i, j) \in \mathbb{N} \times \mathbb{N}$ et $p(i, j) = (c_L^{i,j}, c_H^{i,j}, c_R^{i,j}, c_B^{i,j})$, $p(i, j+1) = (c_L^{i,j+1}, c_H^{i,j+1}, c_R^{i,j+1}, c_B^{i,j+1})$, alors $c_H^{i,j} = c_B^{i,j+1}$.
3. Si $(i, j) \in \mathbb{N} \times \mathbb{N}$ et $p(i, j) = (c_L^{i,j}, c_H^{i,j}, c_R^{i,j}, c_B^{i,j})$, $p(i+1, j) = (c_L^{i+1,j}, c_H^{i+1,j}, c_R^{i+1,j}, c_B^{i+1,j})$, alors $c_R^{i,j} = c_L^{i+1,j}$.

r est la rotation sur les dominos : $r(c_L, c_H, c_R, C_B) = (c_H, c_R, c_B, c_L)$. Un *pavage sans orientation* de S par D est un pavage de S par $D \cup r(D) \cup r^2(D) \cup r^3(D)$.

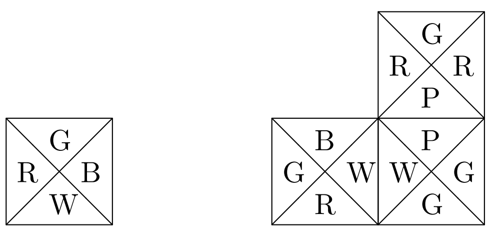

FIGURE 6.2 – Un exemple de tuile/d'un assemblage de tuiles

1. Montrer que les problèmes suivants sont indécidables :
   (a) **Donnée** un ensemble fini de couleurs C et un ensemble fini de dominos D sur C et un domino $d_0 \in D$

Question existe-t-il un pavage de $\mathbb{N}^2$ par D ?

(b) **Donnée** un ensemble fini de couleurs C et un ensemble fini de dominos D sur C et un domino $d_0 \in D$

Question existe-t-il un pavage sans orientation de $\mathbb{N}^2$ par D ?

2. Montrer que le problème suivant est indécidable :

   Donnée : un ensemble fini S de formules du premier ordre sur un ensemble $\{P_1, \ldots, P_n\}$ de symboles de prédicats binaires et l'ensemble $\mathcal{F} = \{0(0), s(1)\}$ de symboles de fonction.

   Question : S est il satisfaisable ?

Exercice 172 (6)

1. Le problème suivant est-il décidable ?

   Donnée : Un ensemble fini de tuiles T, deux relations de compatibilité $H, V \subseteq T \times T$ et une tuile de bordure $t_0 \in T$

   Question : Existe-t-il un rectangle (non vide) que l'on peut paver avec T ?

   Un rectangle $(n, m) \in \mathbb{N}^2$ est pavable (par T, V, H, t_0) s'il existe une application $f : [0, ..., n+1] \times [0, m+1] \to T$ telle que
   — pour tout i, $f(0, i) = f(i, m+1) = f(i, 0) = f(n+1, i) = t_0$
   — pour tout $i \leq n$, pour tout j, $(f(i, j), f(i+1, j)) \in H$
   — pour tout $j \leq m$, pour tout i, $(f(i, j), f(i, j+1)) \in V$
   — pour tout $1 \leq i \leq n$ et tout $1 \leq j \leq m$, $f(i, j) \neq t_0$
   Un rectangle est non vide quand $n, m \geq 1$.

2. Le problème suivant est il décidable ?

   Donnée : un ensemble fini de formules S de la logique du premier ordre

   Question : S a un modèle fini