# Chapitre 8

# Limites de la topologie algorithmique

On montre ici que certains problèmes topologiques fondamentaux sont indécidables. C'est en particulier le cas pour le problème de la contractibilité d'un lacet dans un complexe (simplicial ou autre) ou pour le problème de l'équivalence combinatoire de deux complexes. La preuve de telles indécidabilités s'obtient en deux étapes. Dans un premier temps on montre que le problème en question est équivalent à un problème de décisions dans les représentations combinatoires de groupes. Par exemple, une représentation du $\pi_1$ d'un complexe s'obtient aisément à partir de son 2-squelette. On obtient tout aussi aisément l'expression de la classe d'homotopie d'un lacet dans cette représentation. Il suit que le problème de la contractibilité se réduit au problème du mot dans les groupes. Inversement, toute représentation combinatoire est réalisable comme le $\pi_1$ d'un 2-complexe, constructible par une machine de Turing, dans lequel toute combinaison des générateurs se réalise comme un lacet. Le problème du mot est donc équivalent, au sens de la calculabilité, à celui de la contractibilité.

Dans un deuxième temps, on montre que les grands problèmes de décision dans les représentations combinatoires de groupes, comme le problème du mot, de la conjugaison et de l'isomorphisme, sont indécidables. La vraie difficulté réside dans cette seconde étape, au moins pour les problèmes du mot et de la conjugaison. L'indécidabilité du problème du mot a été prouvée par Novikov (1955) puis grandement simplifiée par Boone (1959), grâce à l'introduction des extensions HNN. Markov (1958) a déduit des résultats de Novikov et Boone l'indécidabilité du problème de l'homéomorphisme pour les complexes combinatoires.

L'objet de ce chapitre est de prouver l'indécidabilité du problème du mot. Je suis la présentation de Stillwell [Sti93, chap. 9].

## 8.1 Le problème de l'arrêt

### 8.1.1 Machine de Turing

Une machine de Turing est un modèle mathématique de la notion de calcul ou d'algorithme. Elle a été introduite par Alan Turing au milieu des années 1930. Selon la *thèse de*

*Church*, de telles machines modélisent toute automatisation imaginable du calcul. Elles sont d'ailleurs équivalentes aux autres approches de formalisation du calcul que sont les fonctions (semi-)récursives et le $\lambda$-calcul.

Formellement, une machine de Turing est un triplet $(\mathcal{A}, \mathcal{Q}, \mathcal{T})$ où $\mathcal{A}$ est un alphabet comportant un caractère spécial *blanc*, $\mathcal{Q}$ est un ensemble d'éléments appelés *états*, et $\mathcal{T} \subset \mathcal{A}\times\mathcal{Q}\times\mathcal{A}\times\mathcal{Q}\times\{R, L\}$ est une *table de transitions* spécifiant le fonctionnement de la machine. Celle-ci agit sur des *configurations*, c'est-à-dire des éléments de la forme $uqv \in \mathcal{A}^* \times \mathcal{Q} \times \mathcal{A}^*$. Une telle configuration modélise la machine dans un état $q$ et munie d'une bande linéaire marquée du mot $uv$, possédant une tête de lecture/écriture positionnée sur le premier caractère du mot $v$ (le mot vide est interprété comme le caractère *blanc*). Une transition $aqbpD \in \mathcal{T}$ s'applique sur toute configuration $uqv$ telle que $a$ est la première lettre de $v$. La transition transforme la configuration en remplaçant cette première lettre $a$ par $b$, l'état $q$ par l'état $p$ et déplace la tête de lecture d'une lettre à droite ou à gauche selon que $D$ vaut respectivement $R$ ou $L$.

On ne considère ici que des machines *déterministes*, c'est-à-dire telles que $aqbpD \in \mathcal{T}$ et $aqb'p'D' \in \mathcal{T}$ implique $a' = a$, $p' = p$ et $D' = D$ : en lisant une lettre dans un état donné on aboutit à une seule nouvelle configuration possible. Une machine est dite à l'arrêt si aucune transition ne s'applique à sa configuration courante.

### $\mathbb{Z}^2$-machine

On peut interpréter une machine de Turing $M$ comme un ensemble de transformations sur $\mathbb{Z}^2$. Pour cela, on pose $\beta = |\mathcal{A}| + |\mathcal{Q}|$ et on associe à chaque lettre et état de $M$ un chiffre distinct entre 0 et $\beta - 1$ en base $\beta$. On interprète ensuite une configuration $uqv$ comme le couple d'entiers $(\mathcal{B}(uq), \mathcal{B}(\bar{v}))$ en base $\beta$, où $\bar{v} = \overline{v_1 v_2 \dots v_k} = v_k \dots v_2 v_1$ et $\mathcal{B}(w)$ désigne le nombre dont les chiffres en base $\beta$ sont associés aux lettres et états de $w$, dans le même ordre. Toute transition de $M$ peut ainsi s'interpréter comme une transformation partielle sur $\mathbb{Z}^2$. Plus précisément, on associe à toute transition $aqbpL$ les $l$-transformations :

$$(\beta^2 U + \mathcal{B}(cq), \beta V + \mathcal{B}(a)) \xrightarrow{l} (\beta U + \mathcal{B}(p), \beta^2 V + \mathcal{B}(bc))$$

correspondant aux transitions $\mathcal{B}^{-1}(U)cqa\overline{\mathcal{B}^{-1}(V)} \mapsto \mathcal{B}^{-1}(U)pcb\overline{\mathcal{B}^{-1}(V)}$ sur les configurations. Ces transformations sont encore de la forme

$$(\beta^2 U + A_l, \beta V + B_l) \xrightarrow{l} (\beta U + C_l, \beta^2 V + D_l)$$

pour des nombres $A_l, B_l, C_l, D_l$ appropriés. Ces 4 nombres déterminent ainsi une $l$-transformation. Notons qu'une transition donne naissance à $|\mathcal{A}|$ transformations possibles, une pour chaque valeur de la lettre $c$. On associe de même à toute transition $aqbpR$ les $r$-transformations :

$$(\beta U + \mathcal{B}(q), \beta^2 V + \mathcal{B}(ca)) \xrightarrow{r} (\beta^2 U + \mathcal{B}(bp), \beta V + \mathcal{B}(c))$$

qui prennent la forme

$$(\beta U + A_r, \beta^2 V + B_r) \xrightarrow{r} (\beta^2 U + C_r, \beta V + D_r)$$

pour des nombres $A_r, B_r, C_r, D_r$ appropriés.

Pour des couples $(X,Y),(X',Y') \in \mathbb{Z}^2$, on écrit $(X,Y) \stackrel{s}{\to} (X',Y')$ si $(X',Y')$ se déduit de $(X,Y)$ par l'application d'une $s$-transformation, $s \in \{l,r\}$. Plus généralement on écrit $(X,Y) \stackrel{*}{\to} (X',Y')$ si $(X',Y')$ se déduit de $(X,Y)$ par l'application d'une succession de transformations. Ainsi, la machine $M$ passe d'une configuration données à une autre par une succession de transitions si et seulement $(X,Y) \stackrel{*}{\to} (X',Y')$ pour les couples correspondants.

On écrit finalement $(X,Y) \stackrel{*}{\leftrightarrow} (X',Y')$ s'il existe des couples
$(X,Y) = (X_0,Y_0),(X_1,Y_1),\ldots,(X_n,Y_n) = (X',Y')$ tels que $(X_i,Y_i) \stackrel{s_i}{\to} (X_{i+1},Y_{i+1})$ ou $(X_{i+1},Y_{i+1}) \stackrel{s_i}{\to} (X_i,Y_i)$ pour $0 \leq i < n$ et $s_i \in \{l,r\}$.

**Codage standard des machines de Turing**

On dit qu'une machine de Turing $M$ est sous *forme standard* si elle a pour alphabet un sous-ensemble fini de $\Sigma = \{blanc, 1, 1', 1'', 1''', \ldots\}$ et pour états un sous-ensemble fini de $\{q, q', q'', q''', \ldots\}$. On peut alors coder la table de transition de la machine sur l'alphabet à 6 lettres $\{blanc, 1, q,', R, L\}$ en concaténant les transitions (de la forme $1'q'1''q''D$) de $M$ où le symbole $'$ est considéré comme une lettre. Finalement en remplaçant les lettres $q,', R, L$ par les lettres respectives $1', 1'', 1''', 1''''$, on obtient un codage de la table de transition sur l'alphabet $\Sigma$. Une telle description de $M$ constitue son *code standard*, et est noté $\lceil M \rceil$.

## 8.1.2 Indécidabilité du problème de l'arrêt

Un ensemble de mots $W \subset \mathcal{A}^*$ est dit *décidable* (ou récursif) par une machine de Turing $M = (\mathcal{A}, \mathcal{Q}, \mathcal{T})$ si on peut distinguer trois états $q_i, q_a, q_r \in \mathcal{Q}$, respectivement appelés initial, acceptant et rejetant, tels que pour tout mot $w \in \mathcal{A}^*$, partant de la configuration $q_i w$, la machine $M$ atteint une configuration d'arrêt dans l'état $q_a$ si $w \in W$ et dans l'état $q_r$ sinon. On exige en particulier que $M$ atteint une configuration d'arrêt pour tous les mots $w$.

Un *problème de décision* est un ensemble de questions à réponses binaires (oui ou non). Par extension, on dira qu'un problème de décision est décidable par une machine de Turing, s'il est possible de coder ses questions par des mots d'un alphabet et si l'ensemble des mots codant les questions à réponse positive est décidable.

Soit $M$ une machine de Turing sous forme standard et $\lceil M \rceil$ son code standard. On considère le problème de décision suivant :
*la machine $M$ atteint-elle, à partir de la configuration $q\lceil M \rceil$, une configuration d'arrêt dans l'état $q''$ ?*

**Théorème 8.1.1** *Le problème de décision précédent est indécidable.*

**Preuve :** Supposons le problème décidable et soit $S$ une machine de Turing sous forme standard le décidant. Quitte à renommer les états de $S$, on peut supposer que ses états

initiaux, acceptant et rejetant sont respectivement $q, q'$ et $q''$. Partant de la configuration $q\lceil S\rceil$, la machine $S$ ne peut aboutir à l'état acceptant $q'$ car cela signifierait de manière contradictoire que $S$, partant de $q\lceil S\rceil$ aboutit à $q''$. De même, $S$ ne peut aboutir à l'état $q''$, car cela signifierait de manière contradictoire que $S$ n'aboutit pas à $q''$. □

Plus généralement,

**Corollaire 8.1.2** *Le problème qui demande pour toute machine $M$ et toute configuration initiale $C$, si $M$ atteint une configuration d'arrêt à partir de $C$ est indécidable.*

En effet, le problème précédent se réduit aisément [1] à ce problème général de l'arrêt. Il est en fait possible de construire une machine $M$ explicite pour laquelle le problème de l'arrêt à partir d'une configuration initiale quelconque est indécidable. Le paragraphe suivant indique une construction relativement simple.

### Machine de Turing universelle

On peut construire une machine de Turing $T$, dite *universelle*, telle que pour toute machine $M$ sous forme standard et toute configuration initiale $C$, la machine $T$, partant de la configuration $q\lceil M\rceil C$, simule le calcul de $M$ à partir de $C$ et s'arrête dans l'état $q'$ si et seulement si le calcul de $M$ à partir de $C$ finit par s'arrêter. Une telle machine serait fastidieuse à décrire dans les détails mais on peut aisément concevoir un programme dans un langage de haut niveau, tel que le langage C++, qui réalise cette simulation. Ceci indique à fortiori l'existence d'une machine de Turing universelle. Le principe est de parcourir la configuration initiale $q\lceil M\rceil C$ pour "lire" l'état et le symbole courants de $C$. Il faut ensuite parcourir $\lceil M\rceil$ pour déterminer quelle transition de $M$ s'applique. Cette transition transforme $C$ en une configuration $C'$, et on aboutit finalement à une configuration $q\lceil M\rceil C'$ de $T$. On peut ainsi recommencer jusqu'à éventuellement atteindre une configuration $q\lceil M\rceil C''$ telle que $C''$ est une configuration d'arrêt pour $M$ et passer ensuite dans l'état d'arrêt $q'$ pour $M$.

**Théorème 8.1.3** *Le problème de l'arrêt pour la machine universelle $T$ est indécidable.*

Autrement dit, il n'existe pas de machine de Turing qui décide pour toute configuration $C$ si la machine $T$, partant de $C$, aboutit à l'arrêt. En effet, l'existence d'une telle machine de Turing permettrait de décider le problème général de l'arrêt, en contradiction avec le corollaire 8.1.2.

## 8.2 Indécidabilité du problème du mot

Soit $G$ un groupe de représentation combinatoire $\langle E \mid R\rangle$ et soit $w$ une expression sur les générateurs $E$ de $G$. Le *problème du mot* consiste à déterminer si $w =_G 1$, i.e. si $w$ est une

1. par une petite modification calculable par une machine de Turing.

conséquence des relations $R$ de $G$. Par extension, le *problème du mot généralisé* consiste à déterminer si une certaine expression $w$ appartient à un certain sous-groupe de $G$ spécifié par des générateurs dans $G$. Pour montrer que de tels problèmes sont indécidables on va montrer que le problème de l'arrêt pour les machines de Turing se réduit, au sens de Turing, au problème du mot généralisé, puis au problème du mot. Pour cela on considère le problème de l'arrêt pour une machine de Turing quelconque, ou plus précisément pour la $\mathbb{Z}^2$-machine $Z$ équivalente (cf. section 8.1.1). On construit ensuite un groupe $K_Z$ et une injection $p : \mathbb{Z}^2 \to K_Z$, de sorte que l'arrêt de $Z$ – partant d'un élément quelconque $(u, v) \in \mathbb{Z}^2$ – corresponde à l'appartenance de $p(u, v)$ à un certain sous-groupe de $K_Z$. On commence par rappeler une construction fondamentale de théorie combinatoire des groupes.

### 8.2.1 Extension HNN et lemme de Britton

Partant du groupe $G = \langle S \mid R\rangle$ et d'un isomorphisme $\varphi : A \to B$ entre deux sous-groupes $A$ et $B$ de $G$, Graham Higman, Bernhard Neumann et Hanna Neumann ont établi en 1949 l'existence d'un groupe $G*_\varphi$ contenant $G$ et dans lequel $A$ et $B$ sont conjugués. Plus précisément,

**Définition 8.2.1** *L'extension HNN de $G$ relativement à $\varphi$ est le groupe*

$$G*_\varphi := \langle S, t \mid R, \{t^{-1}at = \varphi(a)\}_{a\in A}\rangle$$

*où $t$ est un nouveau générateur qualifié de* stable.

Une propriété essentielle des extensions HNN est un théorème de forme normale issu du

**Lemme 8.2.2 (de Britton)** *Si un produit $g_0t^{\epsilon_1}g_1t^{\epsilon_2}\dots t^{\epsilon_n}g_n$ vaut l'élément neutre dans $G*_\varphi$, où $g_i \in G$ et $\epsilon_i \in \{-1, 1\}$, $\forall i \in [0, n]$, alors ou bien $n = 0$ et $g_0 =_G 1$, ou bien pour un certain $i \in [1, n-1]$ on a*
– *soit $\epsilon_i = -1, \epsilon_{i+1} = 1$ et $g_i \in A$*
– *soit $\epsilon_i = 1, \epsilon_{i+1} = -1$ et $g_i \in B$.*

### 8.2.2 Indécidabilité du problème du mot généralisé

On pose

$$K = \langle x, y, z \mid [x, y]\rangle \cong \mathbb{Z}^2 * \mathbb{Z}$$

et on considère l'application $p : \mathbb{Z}^2 \to K, (u, v) \mapsto (x^uy^v)^{-1}zx^uy^v$

**Lemme 8.2.3** *L'image de l'application $p$ forme une base d'un sous-groupe libre de $K$. En particulier, $p$ est injective.*

**Preuve :** Soit $w = p(u_1, v_1)^{j_1} \cdot p(u_2, v_2)^{j_2} \dots p(u_n, v_n)^{j_n}$ un produit réduit sur les $p(u, v)$, i.e. avec $(u_i, v_i) \neq (u_{i+1}, v_{i+1})$ et avec $j_i \neq 0$. En développant et en utilisant la commutation de $x$ et $y$ on obtient

$$w =_K x^{-u_1} y^{-v_1} z^{j_1} x^{u_1-u_2} y^{v_1-v_2} z^{j_2} \dots x^{u_{n-1}-u_n} y^{v_{n-1}-v_n} z^{j_n} x^{u_n} y^{v_n}$$

D'après le théorème de forme normale pour les produits libres de groupes, si ce produit vaut 1 dans $K \cong \langle x, y \mid [x, y] \rangle * \langle z \mid - \rangle$ alors il contient un facteur $x^{u_i-u_{i+1}} y^{v_i-v_{i+1}}$ valant 1 dans $\langle x, y \mid [x, y] \rangle$ pour un certain entier $i \in [1, n-1]$. Mais ceci contredit l'hypothèse $(u_i, v_i) \neq (u_{i+1}, v_{i+1})$. □

On associe à toute $l$-transformation le morphisme
$\phi_l :< x^{\beta^2}, y^\beta, p(A_l, B_l) > \to < x^\beta, y^{\beta^2}, p(C_l, D_l) >$, entre deux sous-groupes de $K$, défini par $x^{\beta^2} \mapsto x^\beta, y^\beta \mapsto y^{\beta^2}, p(A_l, B_l) \mapsto p(C_l, D_l)$. Notons que l'existence d'un tel morphisme n'est a priori pas évidente. On associe de même à toute $r$-transformation le morphisme $\phi_l :< x^\beta, y^{\beta^2}, p(A_r, B_r) > \to < x^{\beta^2}, y^\beta, p(C_r, D_r) >$ défini par
$x^\beta \mapsto x^{\beta^2}, y^{\beta^2} \mapsto y^\beta, p(A_r, B_r) \mapsto p(C_r, D_r)$.

**Lemme 8.2.4** *Les morphismes $\phi_l$ et $\phi_r$ existent et sont des isomorphismes.*

**Preuve :** Soit $\rho_l$ le morphisme intérieur de $K$ qui conjugue par $x^{-A_l} y^{-B_l}$. Ce morphisme envoie $< x^{\beta^2}, y^\beta, p(A_l, B_l) >$ isomorphiquement sur $< x^{\beta^2}, y^\beta, z >$. On envoie de même $< x^\beta, y^{\beta^2}, p(C_l, D_l) >$ sur $< x^\beta, y^{\beta^2}, z >$ par un morphisme intérieur $\theta_l$. Il suffit de montrer que $\theta_l \circ \phi_l \circ \rho_l^{-1}$ existe et est un isomorphisme. Mais ceci résulte du fait que $< x^{\beta^2}, y^\beta, z >$ est égal à $< x^{\beta^2}, y^\beta > * < z >$ dans $K$ (montrer l'inclusion dans les deux sens) et que $< x^\beta, y^{\beta^2}, z >$ est égal à $< x^\beta, y^{\beta^2} > * < z >$ dans $K$. En effet, l'application $x^{\beta^2} \mapsto x^\beta, y^\beta \mapsto y^{\beta^2}$ induit clairement un isomorphisme $< x^{\beta^2}, y^\beta > \to < x^\beta, y^{\beta^2} >$ entre deux sous-groupes eux-mêmes isomorphes à $\mathbb{Z}^2$. Le "produit libre" de cet isomorphisme avec l'identité sur $< z >$ fournit un isomorphisme qui vaut précisément $\theta_l \circ \phi_l \circ \rho_l^{-1}$. □

On peut donc considérer l'extension HNN $K*_{\phi_l}$ de $K$ par $\phi_l$. Soit $t_l$ le générateur stable de cette extension.

**Lemme 8.2.5** *$(u, v) \xrightarrow{l} (u', v')$ si et seulement si $t_l^{-1} p(u, v) t_l = p(u', v')$ dans $K*_{\phi_l}$. De même, $(u, v) \xrightarrow{r} (u', v')$ si et seulement si $t_r^{-1} p(u, v) t_r = p(u', v')$ dans $K*_{\phi_r}$.*

**Preuve :** Si $(u, v) \xrightarrow{l} (u', v')$ alors on a pour certains $U, V$ : $u = \beta^2 U + A_l, v = \beta V + B_l, u' = \beta U + C_l, v' = \beta^2 V + D_l$. On en déduit aisément que $t_l^{-1} p(u, v) t_l = p(u', v')$ en utilisant les relations de $K*_{\phi_l}$. Réciproquement, supposons $t_l^{-1} p(u, v) t_l p(u', v')^{-1} = 1$. Par le lemme de Britton appliqué à $K*_{\phi_l}$, on a $p(u, v) \in < x^{\beta^2}, y^\beta, p(A_l, B_l) >$. Soit encore

$$p(u, v) = x^{\beta^2 j_1} y^{\beta j_2} p(A_l, B_l)^{j_3} x^{\beta^2 j_4} \dots p(A_l, B_l)^{j_n}$$

pour des entiers $j_1, j_2, \dots, j_n$. Par des transformations triviales le membre de droite peut s'écrire sous la forme

$$p(\beta^2 U_1 + A_l, \beta V_1 + B_l)^{j_3} \cdot p(\beta^2 U_2 + A_l, \beta V_2 + B_l)^{j_6} \dots p(\beta^2 U_k + A_l, \beta V_k + B_l)^{j_n} x^{\beta^2 p} y^{\beta q}$$

pour certains entiers $U_1, V_1, U_2, V_2, \dots U_k, V_k, p, q$. En abélianisant $K*_{\phi_l}$ (ou plus simplement $K$, puisque $t_l$ n'intervient pas), l'égalité ci-dessus impose $p = q = 0$. Le lemme 8.2.3 permet de conclure que le membre de droite se réduit à un seul terme $p(\beta^2 U + A_l, \beta V + B_l)$ pour lequel $u = \beta^2 U + A_l$ et $v = \beta V + B_l$. On peut donc appliquer la $l$-transformation à $(u, v)$, d'où $p(u', v') = t_l^{-1} p(u, v) t_l = p(\beta U + C_l, \beta^2 V + D_l)$ et finalement $u' = \beta U + C_l$ et $v' = \beta^2 V + C_l$ par le lemme 8.2.3, soit encore $(u, v) \xrightarrow{l} (u', v')$.

Le cas d'une transformation droite se traite de la même manière. □

On note $K_Z$ le groupe obtenu par extensions HNN successives par tous les morphismes $\phi_l$ et $\phi_r$ associés aux $l$ et $r$-transformations de $Z$. Clairement, ce groupe ne dépend pas de l'ordre des extensions effectuées. Puisqu'un groupe se plonge dans chacune de ses extensions HNN, le lemme précédent reste vrai dans $K_Z$.

**Corollaire 8.2.6** *$p(u', v') \overset{*}{\leftrightarrow} p(u, v)$ si et seulement si $p(u', v') \in < p(u, v), \{t_r\}, \{t_l\} > \subset K_Z$, où $\{t_l\}$ et $\{t_r\}$ désignent les ensembles de générateurs stables associés aux extensions HNN relatives respectivement aux $\varphi_l$ et $\varphi_r$.*

**Preuve :** D'après le lemme précédent, si $p(u', v') \overset{*}{\leftrightarrow} p(u, v)$ alors il existe un élément $w \in < \{t_l\}, \{t_r\} > \subset K_Z$ tel que $p(u', v') = w^{-1} p(u, v) w$. En particulier $p(u', v') \in < p(u, v), \{t_r\}, \{t_l\} >$. Réciproquement, supposons $p(u', v') \in < p(u, v), \{t_r\}, \{t_l\} >$. Donc $p(u', v')$ s'écrit

$$T_0 p(u, v)^{j_1} T_1 p(u, v)^{j_2} \dots p(u, v)^{j_k} T_k$$

pour des entiers $j_1, j_2, \dots, j_k$ et des mots $T_0, T_1, \dots, T_k$ de $< \{t_r\}, \{t_l\} >$. Puisqu'une telle expression vaut un élément dans $K$, il est facile de voir par récurrence sur le nombre d'extensions HNN pour passer de $K$ à $K_Z$ et en utilisant le lemme de Britton, que cette expression contient un sous-mot de la forme $t_s^{\pm 1} w t_s^{\mp 1}$ où $w$ est une expression dans le domaine ou codomaine de $\phi_s$. Mais un tel $w$ étant nécessairement de la forme $p(u, v)^j$, on a

$$t_s^{\pm 1} w t_s^{\mp 1} = t_s^{\pm 1} p(u, v)^j t_s^{\mp 1} = (t_s^{\pm 1} p(u, v) t_s^{\mp 1})^j = p(u'', v'')^j$$

où l'on a soit $(u, v) \xrightarrow{s} (u'', v'')$ soit $(u, v) \xleftarrow{s} (u'', v'')$ suivant les signes des puissances de $t_s$. En particulier, le fait que $p(u, v)^j$ soit dans le (co)domaine de $\phi_s$ implique que la $s$-transformation correspondant à $t_s$ s'applique à $(u, v)$. En substituant $p(u'', v'')^j$ à $t_s^{\pm 1} p(u, v)^j t_s^{\mp 1}$ dans l'expression de $p(u', v')$ ci-dessus, on obtient une nouvelle expression en les $T_i, p(u, v)$ et $p(u'', v'')$. En itérant ce procédé, on obtient finalement

$$p(u', v') = p(u_1, v_1)^{j_1} p(u_2, v_2)^{j_2} \dots p(u_k, v_k)^{j_k}$$

où pour chaque $i$, on a $(u_i, v_i) \overset{*}{\leftrightarrow} (u, v)$. Le lemme 8.2.3 implique finalement que le membre de droite de l'égalité se réduit à $p(u', v')$. En particulier $(u', v') \overset{*}{\leftrightarrow} (u, v)$. □

**Lemme 8.2.7** *Soit $(u_0, v_0) \in \mathbb{Z}^2$ correspondant à une configuration d'arrêt de $Z$. Alors $(u, v) \overset{*}{\leftrightarrow} (u_0, v_0)$ si et seulement si $(u, v) \xrightarrow{*} (u_0, v_0)$*

**Preuve :** On ne peut avoir $(u,v) \overset{s}{\leftarrow} (u_0,v_0)$ par hypothèse sur $(u_0,v_0)$. Par ailleurs si $(u,v) \overset{s}{\leftarrow} (u',v') \overset{s'}{\rightarrow} (u'',v'')$ alors $(u,v) = (u'',v'')$ car $Z$ correspond à une machine déterministe. On peut donc supposer qu'un tel motif n'existe pas dans la séquence $(u,v) \overset{*}{\leftrightarrow} (u_0,v_0)$. La conjonction de ces deux propriétés implique que cette séquence est de la forme $(u,v) \overset{*}{\rightarrow} (u_0,v_0)$. □

**Théorème 8.2.8** *Le problème du mot généralisé est indécidable.*

**Preuve :** Soit $Z$ la $\mathbb{Z}^2$-machine correspondant à une machine de Turing universelle $T$. Quitte à ajouter quelques transitions à $T$, on peut supposer que cette machine universelle possède une unique configuration d'arrêt interprétée comme un certain $(u_0,v_0)$ par $Z$. Le lemme et corrolaire précédents montrent alors que $T$ atteint sa configuration d'arrêt partant d'une configuration initiale donnée de code $(u,v)$ si et seulement si $p(u,v)$ appartient au sous-groupe $< p(u_0,v_0), \{t_r\}, \{t_l\} >$ de $K_Z$. Le théorème 8.1.3 permet de conclure. □

**Corollaire 8.2.9 (Boone)** *Le problème du mot est indécidable.*

**Preuve :** On note $H$ le sous-groupe $< p(u_0,v_0), \{t_r\}, \{t_l\} >$ de $K_Z$. On considère l'extension $L = K_Z *_{Id_H}$ et soit $k$ le générateur stable de cette extension. Alors $p(u,v) \in H$ si et seulement si $[p(u,v),k] =_L 1$. En effet, par le lemme de Britton $p(u,v)kp(u,v)^{-1}k^{-1} =_L 1$ si et seulement si $p(u,v) \in H$. □