Réécriture et problème du mot

Yves Lafont
Institut de Mathématiques de Luminy (UMR 6206 du CNRS)
Université de la Méditerranée (Aix-Marseille 2)

25 mars 2009

Exercice classique : Supposons que $ab = 1 = bc$ dans un monoïde (non commutatif). Peut-on en déduire que $ba = 1$? Même question si on suppose seulement que $ab = 1$.

Plus généralement, peut-on déduire une identité $u = v$ à partir d'une liste d'axiomes $u_1 = v_1, \ldots, u_n = v_n$? C'est ce qu'on appelle le *problème du mot* pour les monoïdes.

En codant le problème de l'arrêt pour les machines de Turing, on démontre facilement que ce problème est indécidable. Autrement dit, il n'existe aucun algorithme qui puisse répondre oui ou non à cette question, étant donnés les mots u, v et $u_1, v_1, \ldots, u_n, v_n$.

Ce problème est aussi indécidable dans le cas des groupes. La première démonstration de ce théorème non trivial a été publiée par P. S. Novikov en 1955. Elle a été ensuite simplifiée par W. W. Boone en 1958, puis par divers auteurs.

La démonstration que nous présentons ici est inspirée par un article de S. Anderaa et E. Cohen [1]. Nous utilisons la *réécriture* à la place du *lemme de Britton*, et les *machines affines* à la place des *machines modulaires* introduites par ces auteurs.

La réécriture apparaît dans un contexte un peu inhabituel, car elle a été plutôt inventée pour résoudre le problème des mots, au moins dans les bons cas. À la fin de cet article, nous évoquerons d'autres applications de la réécriture.

Enfin, il faut savoir que la variante commutative de ce problème du mot est décidable. Pour cela, on utilise un analogue commutatif de la réécriture : les *bases de Gröbner*. Ceci illustre le fait que l'algèbre est généralement plus simple dans le cas commutatif.

Cet article commence par trois sections introductives, respectivement à la *réécriture*, aux *preuves d'indécidabilité*, et à la *théorie combinatoire des groupes*.

1 Groupes libres et réécriture

Definition 1 *(présentation de monoïde)*

Soit Σ un ensemble de symboles. Le monoïde libre Σ^* *est l'ensemble des mots formés avec ces symboles, c'est-à-dire les suites finies $a_1 \dots a_n$ avec $a_1, \dots, a_n \in \Sigma$, muni de la* concaténation $u, v \mapsto uv$. *L'unité de Σ^* est le* mot vide, *noté* 1.

Une présentation *du monoïde M (ou d'un monoïde M) est la donnée de deux ensembles Σ et $\mathcal{R} \subset \Sigma^* \times \Sigma^*$, tels que M soit isomorphe au quotient de Σ^* par la* congruence $\leftrightarrow^*_{\mathcal{R}}$ engendrée par $\mathcal{R}$, *c'est-à-dire la plus petite relation d'équivalence $\sim$ contenant $\mathcal{R}$ et compatible avec la multiplication.*

Si les deux ensembles Σ et $\mathcal{R}$ sont finis, on dit que le monoïde M est finiment présenté.

Si un groupe est finiment présenté, il l'est en tant que monoïde, et réciproquement.

Un cas simple est le groupe $\langle a \rangle \cong \Sigma^*/\leftrightarrow^*_{\mathcal{R}}$ où $\Sigma = \{a, \overline{a}\}$ et $\mathcal{R} = \{(a\overline{a}, 1), (\overline{a}a, 1)\}$. C'est le *groupe libre à un générateur* $\mathbf{F}_1$. On dit que ce dernier, en tant que monoïde, est présenté par le symbole a et son *inverse formel* $\overline{a}$, avec les relations suivantes :

$$a\overline{a} = 1, \qquad \overline{a}a = 1.$$

Pour calculer dans $\mathbf{F}_1$, on considère ces relations comme des *règles de réduction* :

$$a\overline{a} \to 1, \qquad \overline{a}a \to 1.$$

Definition 2 *(réductions)*

Si $u, v \in \Sigma^*$ et $(r, s) \in \mathcal{R}$, on écrit $urv \to_{\mathcal{R}} usv$ (réduction élémentaire).

Si $u_0 \to_{\mathcal{R}} u_1 \to_{\mathcal{R}} \cdots \to_{\mathcal{R}} u_n$, on écrit $u_0 \to^*_{\mathcal{R}} u_n$ (réduction composée).

On dit que le mot u est réduit *s'il n'existe aucune réduction élémentaire $u \to_{\mathcal{R}} v$.*

Dans notre exemple, un mot est réduit lorsqu'il est de la forme a^n ou $\overline{a}^n$ (avec $n \in \mathbb{N}$). De plus, pour tout mot $u \in \Sigma^*$, il existe un unique mot réduit $v \in \Sigma^*$ tel que $u \to^*_{\mathcal{R}} v$. C'est la *forme réduite de u*, notée $\widehat{u}$. Par exemple, la forme réduite de $a\overline{a}aaa\overline{a}$ est aa.

De ce fait, les mots réduits sont des représentants canoniques pour la congruence $\leftrightarrow^*_{\mathcal{R}}$. On peut donc identifier $\mathbf{F}_1$ avec l'ensemble de ces mots, muni du produit $u, v \mapsto \widehat{uv}$. On en déduit que le groupe multiplicatif $\mathbf{F}_1$ est isomorphe au groupe additif $\mathbb{Z}$.

De même, on a le *groupe libre à deux générateurs* $\mathbf{F}_2 = \langle a, b \rangle$. En tant que monoïde, ce dernier est présenté par les symboles a, $\overline{a}$, b, $\overline{b}$, avec les règles suivantes :

$$(1) \quad a\overline{a} \to 1, \qquad (2) \quad \overline{a}a \to 1, \qquad (3) \quad b\overline{b} \to 1, \qquad (4) \quad \overline{b}b \to 1.$$

Un mot réduit est alors un produit alterné de mots réduits non vides pour $\langle a \rangle$ et pour $\langle b \rangle$. Par exemple, le mot $aabab\overline{a}$ est réduit. Ainsi, $\mathbf{F}_2$ est isomorphe au *produit libre* $\mathbb{Z} * \mathbb{Z}$. On peut représenter les éléments de ce groupe comme les noeuds d'un arbre fractal (voir figure 1).

Pour obtenir une présentation du *groupe abelien libre à deux générateurs*, c'est-à-dire du produit cartésien $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, il suffit d'ajouter la relation de commutation $ba = ab$. Autrement dit, on a la *présentation de groupe* suivante :

$$\mathbb{Z}^2 \cong \langle a, b \mid ba = ab \rangle \cong \langle a, b \mid bab^{-1}a^{-1} \rangle.$$

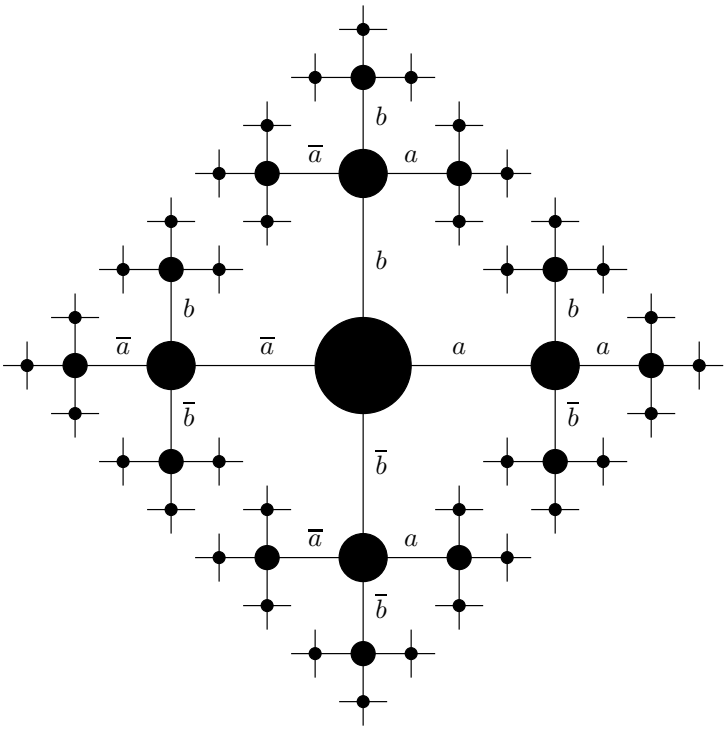


FIG. 1 – le groupe libre $\mathbf{F}_2 = \langle a, b\rangle$

Mais pour calculer la forme réduite d'un mot, il faut ajouter d'avantage de règles :

$$(5)\quad ba \to ab, \qquad (6)\quad b\overline{a} \to \overline{a}b, \qquad (7)\quad \overline{b}a \to a\overline{b}, \qquad (8)\quad \overline{b}\overline{a} \to \overline{a}\overline{b}.$$

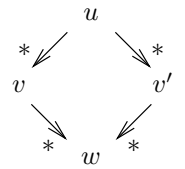
Un mot réduit est alors le produit d'un mot réduit pour $\langle a\rangle$ et d'un mot réduit pour $\langle b\rangle$. Notez que les règles (6) à (8), en tant que relations, se déduisent des règles (1) à (5). Par exemple, la règle (6) se déduit de la façon suivante : $b\overline{a} = \overline{a}ab\overline{a} = \overline{a}ba\overline{a} = \overline{a}b$. On dit que ce calcul est une *dérivation*, et non une réduction, car certaines règles sont utilisées en sens inverse.

Nous venons de voir trois exemples de *présentations convergentes* (pour $\mathbf{F}_1$, $\mathbf{F}_2$ et $\mathbb{Z}^2$).

Definition 3 *(présentation convergente)*

On dit qu'une présentation $\Sigma, \mathcal{R}$ *est* noetherienne *si on a la* propriété de terminaison : *Il n'existe aucune réduction infinie* $u_0 \to_{\mathcal{R}} u_1 \to_{\mathcal{R}} \cdots \to_{\mathcal{R}} u_n \to_{\mathcal{R}} \cdots$

On dit que la présentation est convergente *si, de plus, on a la* propriété de confluence : *Pour tous* u, v, v' *tels que* $u \to^*_{\mathcal{R}} v$ *et* $u \to^*_{\mathcal{R}} v'$*, il existe* w *tel que* $v \to^*_{\mathcal{R}} w$ *et* $v' \to^*_{\mathcal{R}} w$.



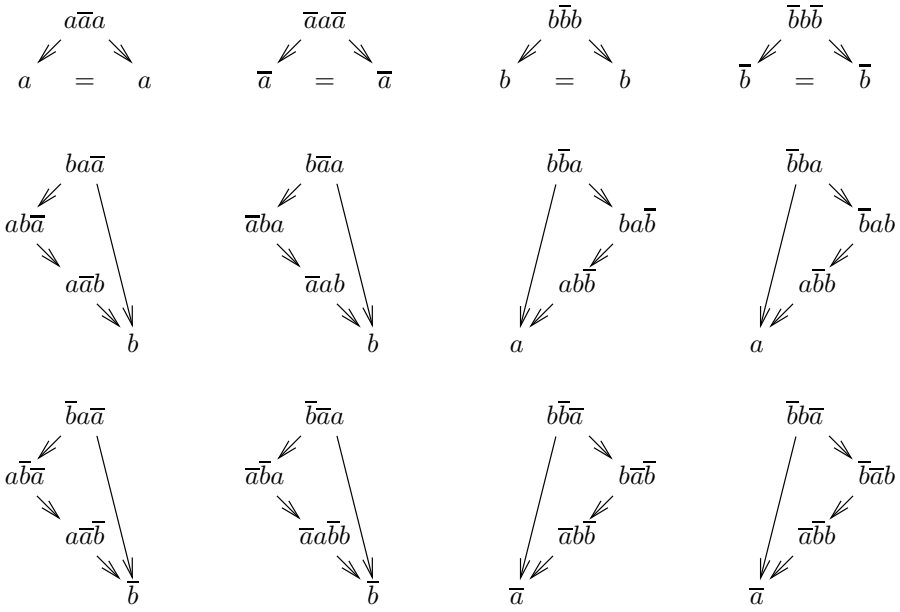


FIG. 2 – confluence des 12 pics critiques pour la présentation de $\mathbb{Z}^2$

Notez que dans ce dernier cas, on obtient l'existence de la forme réduite par la propriété de terminaison et son unicité par la propriété de confluence. Ainsi, pour savoir si les mots u et v représentent le même élément dans $M \cong \Sigma^*/\leftrightarrow^*_{\mathcal{R}}$, il suffit de comparer les formes réduites $\widehat{u}$ et $\widehat{v}$.

La propriété de terminaison est immédiate pour la présentation de $\mathbf{F}_1$ et celle de $\mathbf{F}_2$, puisque la longueur des mots décroît. Pour la présentation de $\mathbb{Z}^2$, il faut totaliser le nombre de fois où un b (ou bien un $\overline{b}$) apparaît avant un a (ou bien un $\overline{a}$), c'est-à-dire le nombre de décompositions du mot de la forme $u\beta v\alpha w$ avec $\beta \in \{b, \overline{b}\}$, $\alpha \in \{a, \overline{a}\}$, et $u, v, w \in \Sigma^*$.

Pour montrer qu'une présentation noetherienne est convergente, il suffit de vérifier la confluence de chaque *pic critique*, qui correspond au chevauchement de deux règles. Par exemple, il y a 12 pics critiques à considérer pour la présentation de $\mathbb{Z}^2$ (figure 2).

Proposition 1 *(famille libre infinie)*

La famille infinie $(b^n a b^{-n})_{n\in\mathbb{Z}}$ *est libre dans le groupe* $\mathbf{F}_2 = \langle a, b\rangle$.

Autrement dit, on a un plongement du *groupe libre à une infinité de générateurs* $\mathbf{F}_\omega$ dans le groupe libre à 2 générateurs $\mathbf{F}_2$.

Preuve : Pour montrer cela, on construit une présentation convergente infinie de $\mathbf{F}_2$.

On part de la présentation de $\mathbf{F}_2$ par les symboles a, $\overline{a}$, b, $\overline{b}$, avec les relations suivantes :

$$a\overline{a} = 1, \qquad \overline{a}a = 1, \qquad b\overline{b} = 1, \qquad \overline{b}b = 1.$$

Pour chaque $n > 0$, on introduit les 4 *générateurs superflus* suivants :

$$a_n = b^n a\overline{b}^n, \qquad \overline{a}_n = b^n\overline{a}\overline{b}^n, \qquad a_{-n} = \overline{b}^n a b^n, \qquad \overline{a}_{-n} = \overline{b}^n\overline{a}b^n.$$

Autrement dit, on ajoute à chaque fois le nouveau symbole et la relation qui le définit. On écrit aussi a_0 pour a, et $\overline{a}_0$ pour $\overline{a}$, puis on ajoute les *relations dérivables* suivantes :

$$a_n\overline{a}_n = 1 \text{ (pour } n > 0 \text{ ou } n < 0), \qquad \overline{a}_n a_n = 1 \text{ (idem)},$$
$$ba_n = a_{n+1}b, \qquad b\overline{a}_n = \overline{a}_{n+1}b, \qquad \overline{b}a_n = a_{n-1}\overline{b}, \qquad \overline{b}\overline{a}_n = \overline{a}_{n-1}\overline{b}.$$

Finalement, on supprime les relations définissant les a_n et les $\overline{a}_n$ (pour $n > 0$ ou $n < 0$), qui sont désormais dérivables. On obtient une nouvelle présentation de $\mathbf{F}_2$ par les symboles a_n (pour $n \in \mathbb{Z}$), b et $\overline{b}$, avec les relations suivantes, que nous écrivons comme des règles de réduction :

$$a_n\overline{a}_n \to 1, \qquad \overline{a}_n a_n \to 1, \qquad b\overline{b} \to 1, \qquad \overline{b}b \to 1,$$
$$ba_n \to a_{n+1}b, \qquad b\overline{a}_n \to \overline{a}_{n+1}b, \qquad \overline{b}a_n \to a_{n-1}\overline{b}, \qquad \overline{b}\overline{a}_n \to \overline{a}_{n-1}\overline{b}.$$

Notez que cette présentation ressemble beaucoup à la présentation convergente de $\mathbb{Z}^2$. En utilisant les mêmes arguments, on voit que cette présentation de $\mathbf{F}_2$ est convergente. De plus, elle contient une présentation du groupe libre $\mathbf{F}_\omega = \langle\Sigma\rangle$ où $\Sigma = \{a_n \mid n \in \mathbb{Z}\}$.

On a donc un morphisme $\varphi : \mathbf{F}_\omega \to \mathbf{F}_2$ tel que $\varphi(a_n) = b^n a b^{-n}$ pour tout $n \in \mathbb{Z}$. Comme tout mot réduit pour la présentation de $\mathbf{F}_\omega$ est aussi réduit pour celle de $\mathbf{F}_2$, on en déduit que φ est injectif. Autrement dit, la famille $(b^n a b^{-n})_{n\in\mathbb{Z}}$ est libre. ◀

Enfin, notons que tout monoïde M a une *présentation standard*, qui est convergente. Celle-ci est donnée par les symboles a_x (pour $x \in M$) et les règles suivantes :

$$a_x a_y \to a_{xy}, \qquad a_1 \to 1.$$

Les mots réduits pour cette présentation sont les a_x tels que $x \neq 1$ et le mot vide 1.

2 Problème du mot et machines affines

Definition 4 *(machine à registres déterministe)*

Une machine à 2 registres *est une suite de n instructions de l'une des deux formes suivantes :*

incrémenter x et aller à j, si $x = 0$ alors aller à j, sinon décrémenter x et aller à k,

où x est l'un des 2 registres et $j, k \in \{0, \ldots, n\}$.

Comme il n'y a pas d'instruction 0, on écrira *stop* à la place de *aller à 0*. Par exemple, la machine suivante calcule la multiplication de x par 2 (si on commence avec $y = 0$) :

1. si $x = 0$ alors stop, sinon décrémenter x et aller à 2,
2. incrémenter y et aller à 3,
3. incrémenter y et aller à 1.

Definition 5 *(configurations et transitions)*

Une configuration *pour une machine $\mathcal{M}$ à 2 registres et n instructions est donnée par un triplet (i, x, y) avec $i \in \{0, \ldots, n\}$ et $x, y \in \mathbb{N}$.*

Chaque instruction de $\mathcal{M}$ induit une ou deux transitions *de l'une des formes suivantes :*

$$(i,x,y) \to_{\mathcal{M}} (j,x{+}1,y), \quad (i,0,y) \to_{\mathcal{M}} (j,0,y), \quad (i,x{+}1,y) \to_{\mathcal{M}} (k,x,y),$$
$$(i,x,y) \to_{\mathcal{M}} (j,x,y{+}1), \quad (i,x,0) \to_{\mathcal{M}} (j,x,0), \quad (i,x,y{+}1) \to_{\mathcal{M}} (k,x,y).$$

On note alors $\to^*_{\mathcal{M}}$ et $\leftrightarrow^*_{\mathcal{M}}$ le préordre et l'équivalence engendrés par ces transitions.

Par exemple, la machine ci-dessus correspond aux transitions suivantes :

$$(1,0,y) \to_{\mathcal{M}} (0,0,y), \qquad (1,x{+}1,y) \to_{\mathcal{M}} (2,x,y),$$
$$(2,x,y) \to_{\mathcal{M}} (3,x,y{+}1), \qquad (3,x,y) \to_{\mathcal{M}} (1,x,y{+}1).$$

Théorème 1 *(indécidabilité du problème de l'arrêt pour les machines à 2 registres)*

Il existe une machine $\mathcal{M}$ à 2 registres telle que le problème suivant soit indécidable :

Etant donnée une configuration (i,x,y) pour $\mathcal{M}$, a-t-on $(i,x,y) \to^*_{\mathcal{M}} (0,0,0)$?

Pour montrer ce théorème, on code le problème de l'arrêt pour une machine de Turing : Si celle-ci utilise un alphabet à n symboles, on remplace le ruban par deux entiers dont les développements en base n correspondent aux parties gauche et droite du ruban.

Théorème 2 *(indécidabilité du problème du mot pour les monoïdes)*

Il existe une présentation finie $\Sigma, \mathcal{R}$ telle que le problème suivant soit indécidable :

Etant donnés deux mots $u, v \in \Sigma^*$, a-t-on $u \leftrightarrow^*_{\mathcal{R}} v$?

Preuve : Soit $\mathcal{M}$ une machine à 2 registres et n instructions. On introduit les symboles $a, b, c_0, \ldots, c_n, d, e$ et on code la configuration (i,x,y) par le mot $[i,x,y] = ab^x c_i d^y e$. Chaque transition de $\mathcal{M}$ correspond alors à une règle de l'une des formes suivantes :

$$c_i \to bc_j, \quad ac_i \to ac_j, \quad bc_i \to c_k, \quad c_i \to c_j d, \quad c_i e \to c_j e, \quad c_i d \to c_k d.$$

On obtient alors une présentation finie Σ, R sans pic critique telle que les trois énoncés suivants sont équivalents :

$$(i,x,y) \to^*_{\mathcal{M}} (0,0,0), \qquad [i,x,y] \to^*_{\mathcal{R}} [0,0,0], \qquad [i,x,y] \leftrightarrow^*_{\mathcal{R}} [0,0,0].$$

L'équivalence entre les deux derniers énoncés résulte de l'absence de pics critiques, qui implique la propriété de confluence même si on n'a pas la propriété de terminaison.

On a ainsi réduit le problème de l'arrêt pour $\mathcal{M}$ au problème du mot. Par le théorème 1, on obtient donc une présentation finie $\Sigma, \mathcal{R}$ pour laquelle ce dernier est indécidable. ◀

Il existe aussi une présentation finie Σ, R telle que le problème suivant soit indécidable :

Etant donné un mot $u \in \Sigma^*$, a-t-on $u \leftrightarrow^*_{\mathcal{R}} 1$?

Il suffit d'ajouter la règle $ac_0e \to 1$ à la présentation précédente, qui reste confluente.

Dans le cas des groupes, ce dernier problème est équivalent au problème initial, car on a $x = y$ si et seulement si $xy^{-1} = 1$. Pour montrer qu'un tel problème est indécidable, on voudrait plonger le monoïde précédent dans un groupe : Étant donné $M \cong \Sigma^*/\leftrightarrow^*_{\mathcal{R}}$, on peut évidemment construire un groupe G en ajoutant un inverse formel $\overline{\alpha}$ pour chaque symbole $\alpha \in \Sigma$, avec les relations $\alpha\overline{\alpha} = 1$ et $\overline{\alpha}\alpha = 1$. On obtient alors un morphisme $\varphi : M \to G$, mais celui-ci n'est pas forcément injectif.

Considérons par exemple le monoïde M construit à partir de la machine $\mathcal{M}$ suivante :

1. si $x = 0$ alors stop, sinon décrémenter x et aller à 2,
2. incrémenter x et aller à 3,
3. si $y = 0$ alors stop, sinon décrémenter y et aller à 3.

Dans ce cas, on obtient une présentation confluente de M avec les règles suivantes :

$$ac_1 \to ac_0, \quad bc_1 \to c_2, \quad c_2 \to bc_3, \quad c_3e \to c_0e, \quad c_3d \to c_3.$$

Comme c_1 et c_3 sont réduits pour cette présentation, on a $c_1 \neq c_3$ dans le monoïde M. Mais dans le groupe G, on a $c_1 = b^{-1}bc_1 = b^{-1}c_2 = b^{-1}bc_3 = c_3$, ce qui nous donne $ac_1de = ac_3de = ac_3e = ac_0e$. Pourtant, on n'a pas $(1,0,1) \to^*_{\mathcal{M}} (0,0,0)$.

Ainsi, l'existence d'inverses crée des « interférences » dans le codage de nos machines. En fait, cette méthode est vouée à l'échec, et il faut changer complètement de codage.

Definition 6 *(machine affine)*

Une machine affine *est un ensemble fini $\mathcal{A} \subset \mathbb{Z} \times \mathbb{Z}^\bullet \times \mathbb{Z} \times \mathbb{Z}^\bullet$, où $\mathbb{Z}^\bullet = \mathbb{Z} \setminus \{0\}$.*

Chaque $(p,q,p',q') \in \mathcal{A}$ définit une transition affine $p+qz \to_{\mathcal{A}} p'+q'z$ *(pour $z \in \mathbb{Z}$).*

On note $\leftrightarrow^*_{\mathcal{A}}$ la relation d'équivalence engendrée par $\to_{\mathcal{A}}$.

Théorème 3 *(indécidabilité du problème de l'équivalence pour une machine affine)*

Il existe une machine affine $\mathcal{A}$ et $m \in \mathbb{Z}$ tels que le problème suivant soit indécidable :

Étant donné $z \in \mathbb{Z}$, a-t-on $z \leftrightarrow^*_{\mathcal{A}} m$?

Preuve : Soit $\mathcal{M}$ une machine à 2 registres et n instructions. On pose $m = n+1$ et on code la configuration (i,x,y) par l'entier $[i,x,y] = i + m2^x3^y$. Chaque transition de $\mathcal{M}$ correspond alors à une ou deux transitions affines de l'une des formes suivantes :

$$\begin{array}{lll} i+mz \to j+2mz, & i+m(2z+1) \to j+m(2z+1), & i+2mz \to k+mz, \\ i+mz \to j+3mz, & i+m(3z+1) \to j+m(3z+1), & i+3mz \to k+mz, \\ & i+m(3z+2) \to j+m(3z+2). & \end{array}$$

On obtient ainsi une machine affine $\mathcal{A}$ qui satisfait les deux propriétés suivantes :

si $z \to_{\mathcal{A}} z'$, alors z est le code d'une configuration si et seulement si z' l'est ;

$(i,x,y) \to_{\mathcal{M}} (i',x',y')$ si et seulement si $[i,x,y] \to_{\mathcal{A}} [i',x',y']$.

Comme $\mathcal{M}$ est déterministe, les trois énoncés suivants sont équivalents :

$$(i,x,y) \to^*_{\mathcal{M}} (0,0,0), \qquad (i,x,y) \leftrightarrow^*_{\mathcal{M}} (0,0,0), \qquad [i,x,y] \leftrightarrow^*_{\mathcal{A}} [0,0,0].$$

Comme $[0,0,0] = m$, on a réduit le problème de l'arrêt pour $\mathcal{M}$ au problème ci-dessus. Il suffit alors d'appliquer le théorème 1. ◀

3 Extensions de Higman-Neuman-Neuman

On va démontrer ici quelques résultats classiques de théorie combinatoire des groupes en utilisant des techniques de réécriture.

On écrit $H \sqsubset G$ si H est un sous-groupe de G et $F \sqsupset G$ si F est une extension de G, c'est-à-dire si G est un sous-groupe de F.

On note $\langle x_1, \ldots, x_n \rangle$ le sous-groupe de G engendré par les éléments $x_1, \ldots, x_n \in G$, et on dit qu'un tel sous-groupe est *finiment engendré*.

Proposition 2 *(extension HNN associée à un sous-groupe)*

Pour tout $H \sqsubset G$, il existe $F \sqsupset G$ et $t \in F$ tels que $H = \{x \in G \mid tx = xt\}$.

De plus, F est finiment présenté si G l'est et si H est finiment engendré.

Preuve : Soit $F = \hat{G}/{\leftrightarrow_{\mathcal{C}}^*}$ où $\hat{G} = G * \langle b \rangle$ et $\mathcal{C} = \{(bu, ub) \mid u \in H\}$.

En partant de la présentation standard de G (voir la fin de la section 1), on obtient une présentation de F (en tant que monoïde) par les symboles a_x (pour $x \in G$), b et $\overline{b}$, avec les relations suivantes :

$$a_x a_y = a_{xy}, \qquad a_1 = 1, \qquad b\overline{b} = 1, \qquad \overline{b}b = 1, \qquad ba_u = a_u b \text{ (pour } u \in H).$$

On choisit alors un ensemble $H^\perp$ de représentants pour les *classes à droite modulo* H. Autrement dit, tout $x \in G$ a une unique décomposition $x = uv$ où $u \in H$ et $v \in H^\perp$. De plus, on peut supposer que $1 \in H^\perp$.

Pour chaque $v \in H^\perp \setminus \{1\}$, on introduit les générateurs superflus $b_v = ba_v$ et $b'_v = \overline{b}a_v$. On écrit aussi b_1 pour b et b'_1 pour $\overline{b}$, puis on ajoute les relations dérivables suivantes :

$$b_1 b'_v = a_v \text{ (pour } v \in H^\perp), \qquad b'_1 b_v = a_v \text{ (pour } v \in H^\perp),$$
$$b_v a_x = a_u b_w \text{ (si } u \in H, v, w \in H^\perp \text{ et } vx = uw), \qquad b'_v a_x = a_u b'_w \text{ (idem).}$$

Notez que dans le cas où $x = u$ et $v = w = 1$, on retrouve la relation $ba_u = a_u b$.

On supprime les relations $b\overline{b} = 1$ et $\overline{b}b = 1$, ainsi que celles définissant les b_v et les b'_v, qui sont désormais dérivables. On obtient une présentation convergente du groupe F par les symboles a_x (pour $x \in G$), b_v et b'_v (pour $v \in H^\perp$), avec les règles suivantes :

$$a_x a_y \to a_{xy}, \qquad a_1 \to 1, \qquad b_1 b'_v \to a_v, \qquad b'_1 b_v \to a_v,$$
$$b_v a_x \to a_u b_w \text{ (si } u \in H, v, w \in H^\perp \text{ et } vx = uw), \qquad b'_v a_x \to a_u b'_w \text{ (idem).}$$

Cette présentation de F contient la présentation standard de G, et tout mot réduit pour celle de G est aussi réduit pour celle de F. On en déduit que F est une extension de G. On vérifie de même que F est une extension de $\langle b \rangle$. En particulier, on a $b \in F$.

Si $x = uv$ où $u \in H$ et $v \in H^\perp$, la forme réduite de $b_1 a_x$ est $a_u b_v$ (ou b_v si $u = 1$), et le mot $a_x b_1$ est réduit (ou sa forme réduite est b_1 si $x = 1$). Ces formes réduites coïncident lorsque $v = 1$, c'est-à-dire $x \in H$. Autrement dit, $H = \{x \in G \mid bx = xb\}$.

Enfin, remarquons que si $\Sigma, \mathcal{R}$ est une présentation finie de G (en tant que monoïde), et si $u_1, \ldots, u_n \in \Sigma^*$ sont des mots dont les classes modulo $\mathcal{R}$ engendrent le sous-groupe H, alors on obtient une présentation finie $\Sigma', \mathcal{R}'$ de F (en tant que monoïde) en posant $\Sigma' = \Sigma \cup \{b, \overline{b}\}$ et $\mathcal{R}' = \mathcal{R} \cup \{(b\overline{b}, 1), (\overline{b}b, 1), (bu_1, ub_1), \ldots, (bu_n, ub_n)\}$. ◀

Corollaire 1 *(réduction du problème de Magnus au problème du mot)*

Si G a une présentation finie $\Sigma, \mathcal{R}$ (en tant que monoïde) et le sous-groupe $H \sqsubset G$ est finiment engendré, alors on peut réduire le problème suivant au problème du mot pour une extension finiment présentée $F \sqsupset G$:

Etant donné un mot $u \in \Sigma^*$, la classe de u modulo $\mathcal{R}$ est-elle dans H ?

Notez que dans le cas particulier où $H = \{1\}$, on retrouve le problème du mot.

Definition 7 *(isomorphisme local)*

Un isomorphisme local de G *est un isomorphisme* $\varphi : H \to H'$ *avec* $H, H' \sqsubset G$.

On dit que $t \in G$ représente φ *si on a* $txt^{-1} = \varphi(x)$ *pour tout* $x \in H$.

On dit que le sous-groupe $K \sqsubset G$ *est* invariant par φ *si on a* $\varphi(H \cap K) = H' \cap K$.

Proposition 3 *(extension HNN associée à un isomorphisme local)*

Pour tout isomorphisme local $\varphi : H \to H'$ *de* G*, il existe* $F \sqsupset G$ *et* $t \in F$ *tels que :*

1. t *représente* φ *;*
2. $\langle K, t\rangle \cap G = K$ *pour tout* $K \sqsubset G$ *invariant par* φ *;*
3. F *est finiment présenté si* G *l'est et si* H *est finiment engendré.*

Ici, $\langle K, t\rangle$ désigne le sous-groupe de F engendré par l'ensemble $K \cup \{t\}$.

Preuve : Soit $F = \hat{G}/\leftrightarrow^*_{\mathcal{C}}$ où $\hat{G} = G * \langle b\rangle$ et $\mathcal{C} = \{(bu, \varphi(u)b) \mid u \in H\}$.

On introduit les deux ensembles $H^\perp$ et $H'^\perp$ comme dans la preuve de la proposition 2. On obtient ainsi une présentation convergente de F par les symboles a_x (pour $x \in G$), b_v (pour $v \in H^\perp$) et b'_v (pour $v \in H'^\perp$), avec les règles suivantes :

$$a_x a_y \to a_{xy}, \qquad a_1 \to 1, \qquad b_1 b'_v \to a_v, \qquad b'_1 b_v \to a_v,$$
$$b_v a_x \to a_{\varphi(u)} b_w \text{ (si } u \in H, v, w \in H^\perp \text{ et } vx = uw),$$
$$b'_v a_x \to a_{\varphi^{-1}(u)} b'_w \text{ (si } u \in H', v, w \in H'^\perp \text{ et } vx = uw).$$

On en déduit que F est une extension de G et de $\langle b\rangle$. En particulier, on a $b \in F$.

Si $u \in H$, la forme réduite de $b_1 a_u b'_1$ est $a_{\varphi(u)}$ (ou 1 si $u = 1$). Ainsi, b représente φ.

Si $K \sqsubset G$, on choisit des ensembles de représentants $H^\perp$ et $H'^\perp$ compatibles avec K. Autrement dit, on peut supposer que tout $x \in K$ a une unique décomposition $x = uv$ où $u \in H \cap K$ et $v \in H^\perp \cap K$ (respectivement $u \in H' \cap K$ et $v \in H'^\perp \cap K$).

Supposons maintenant que K soit invariant par φ. D'après ce qui précède, si tous les symboles d'un mot ont leurs indices dans K, il en va de même pour sa forme réduite. On en déduit aisément que $\langle K, b\rangle \cap G \subset K$, et l'inclusion réciproque est immédiate.

Pour le reste, on procède exactement comme dans la preuve de la proposition 2. ◄

On peut facilement généraliser cette construction :

Proposition 4 *(extension HNN associée à plusieurs isomorphismes locaux)*

Pour toute suite $\varphi_1 : H_1 \to H'_1, \ldots, \varphi_n : H_n \to H'_n$ *d'isomorphismes locaux de* G*, il existe* $F \sqsupset G$ *et* $t_1, \ldots t_n \in F$ *tels que :*

1. t_i *représente* φ_i *pour chaque* i *;*
2. $\langle K, t_1, \ldots, t_n\rangle \cap G = K$ *pour tout* $K \sqsubset G$ *invariant par chaque* φ_i *;*
3. F *est finiment présenté si* G *l'est et si les* H_i *sont finiment engendrés.*

Ici, $\langle K, t_1, \ldots, t_n\rangle$ désigne le sous-groupe de F engendré par $K \cup \{t_1, \ldots, t_n\}$.

Preuve : Par récurrence sur n, en utilisant la proposition 3. ◄

4 Théorème de Novikov-Boone

Si $n \in \mathbb{Z}$, on pose $a_n = b^n a b^{-n} \in \mathbf{F}_2 = \langle a, b\rangle$. Notez que $a_{p+qn} \in \langle a_p, b^q\rangle$.

Lemme 1 *Si $p, q \in \mathbb{Z}$ avec $q \neq 0$, alors le couple (a_p, b^q) est libre dans le groupe $\mathbf{F}_2$.*

Preuve : Comme a et b^q sont d'ordre infini, le couple (a, b^q) est libre dans le groupe $\mathbf{F}_2 \cong \langle a\rangle * \langle b\rangle$. Il suffit alors d'appliquer l'*isomorphisme intérieur* $x \mapsto b^p x b^{-p}$. ◄

Lemme 2 *Si $p, q, p', q' \in \mathbb{Z}$ avec $q, q' \neq 0$, alors on peut construire un isomorphisme $\varphi : \langle a_p, b^q\rangle \to \langle a_{p'}, b^{q'}\rangle$ tel que $\varphi(a_{p+qz}) = a_{p'+q'z}$ pour tout $z \in \mathbb{Z}$.*

Preuve : Par le lemme 1, on a $\langle a_p, b^q\rangle \cong \mathbf{F}_2 \cong \langle a_{p'}, b^{q'}\rangle$. Ainsi, on a un isomorphisme $\varphi : \langle a_p, b^q\rangle \to \langle a_{p'}, b^{q'}\rangle$ tel que $\varphi(a_p) = a_{p'}$ et $\varphi(b^q) = b^{q'}$, d'où le résultat. ◄

Si $P \subset \mathbb{Z}$, on note $[P]$ le sous-groupe de $\mathbf{F}_2$ engendré par l'ensemble $\{a_z \mid z \in P\}$.

Lemme 3 *Si $p, q \in \mathbb{Z}$, alors on a $\langle a_p, b^q\rangle \cap [\mathbb{Z}] = [p + q\mathbb{Z}]$.*

Preuve : Comme $K = [p+q\mathbb{Z}]$ est invariant par l'isomorphisme intérieur $x \mapsto b^q x b^{-q}$ et $a_p \in K$, il apparaît que tout $x \in \langle a_p, b^q\rangle$ est de la forme uv avec $u \in K$ et $v \in \langle b^q\rangle$.

De plus, on a $K \sqsubset [\mathbb{Z}] \sqsubset \ker \pi$ où $\pi : \mathbf{F}_2 \to \langle b\rangle$ est défini par $\pi(a) = 1$ et $\pi(b) = b$. Dans le cas où $x \in [\mathbb{Z}]$, on obtient donc $1 = \pi(x) = \pi(u)\pi(v) = v$, d'où $x = u \in K$. Ainsi, on a $\langle a^p, b_q\rangle \cap [\mathbb{Z}] \sqsubset K$, et l'inclusion réciproque est immédiate. ◄

Les deux lemmes suivants sont des conséquences immédiates de la proposition 1 :

Lemme 4 *Si $P, Q \subset \mathbb{Z}$, alors on a $[P] \cap [Q] = [P \cap Q]$.*

Lemme 5 *Si $z \in \mathbb{Z}$ et $P \subset \mathbb{Z}$, alors on a $z \in P$ si et seulement si $a_z \in [P]$.*

Nous pouvons maintenant démontrer le théorème de Novikov-Boone :

Théorème 4 *(indécidabilité du problème du mot pour les groupes)*

Il existe un groupe finiment présenté pour lequel le problème du mot est indécidable.

Preuve : Soit $\mathcal{A}$ une machine affine et soit $m \in \mathbb{Z}$.

Le lemme 2 associe des isomorphismes locaux $\varphi_1, \ldots, \varphi_n$ de $\mathbf{F}_2$ aux transitions de $\mathcal{A}$. Par la proposition 4, on a une extension finiment présentée $F \sqsupset \mathbf{F}_2$ et $t_1, \ldots, t_n \in F$ tels que chaque t_i représente φ_i.

On pose $H = \langle a_m, t_1, \ldots, t_n\rangle$ et $K = [P]$ où $P = \{z \in \mathbb{Z} \mid z \leftrightarrow^*_{\mathcal{A}} m\}$.

En utilisant le lemme 2, on obtient les deux propriétés suivantes :

$$\text{si } z \to_{\mathcal{A}} z', \text{ on a } a_{z'} = \varphi_i(a_z) = t_i a_z t_i^{-1} \text{ pour un certain } i \in \{1, \ldots, n\},$$
$$\text{si } z \leftrightarrow^*_{\mathcal{A}} m, \text{ on a } a_z = u a_m u^{-1} \text{ pour un certain } u \in \langle t_1, \ldots, t_n\rangle.$$

On a donc $K \sqsubset H$, et comme $a_m \in K$, on en déduit que $H = \langle K, t_1, \ldots, t_n\rangle$.

Comme $K \sqsubset [\mathbb{Z}]$, on a $K = [\mathbb{Z}] \cap K$. Par les lemmes 3 et 4, on obtient :

$$\langle a_p, b^q\rangle \cap K = \langle a_p, b^q\rangle \cap [\mathbb{Z}] \cap K = [p + q\mathbb{Z}] \cap [P] = [(p + q\mathbb{Z}) \cap P].$$

On en déduit que K est invariant par chaque φ_i, d'où $K = H \cap \mathbf{F}_2$ par la proposition 4.

D'après le lemme 5 et la proposition 2, on a une extension finiment présentée $E \sqsupset F$ et $t \in E$ tels que les quatre énoncés suivants sont équivalents :

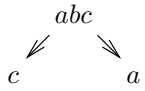
$$z \leftrightarrow_{\mathcal{A}}^{*} m, \qquad a_z \in K, \qquad a_z \in H, \qquad a_z t = t a_z.$$

Comme une égalité dans E revient à une équivalence modulo une certaine congruence engendrée $\leftrightarrow_{\mathcal{R}}^{*}$, on a ainsi réduit le problème de l'équivalence pour $\mathcal{A}$ et m au problème du mot pour E. Il suffit alors d'appliquer le théorème 3. ◀

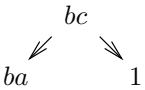
Épilogue

Revenons maintenant à l'exercice du début. La réponse à la première question est oui, car on a $ba = babc = bc = 1$. Mais comment trouver cette réponse sans tâtonner ?

Il suffit de considérer la présentation définie par les générateurs a, b, c avec les règles $ab \to 1$ et $bc \to 1$. Cette présentation satisfait évidemment la propriété de terminaison, mais pas la confluence, à cause du pic critique suivant :



Pour y remédier, on ajoute la règle $c \to a$, qui est bien sûr dérivable en tant que relation, et qui produit un nouveau pic critique :



De même, on ajoute la règle $ba \to 1$, qui donne cette fois une présentation convergente et qui permet de répondre à la question posée.

Par contre, la réponse à la deuxième question est non, car la règle $ab \to 1$ définit une présentation convergente (sans pic critique) pour laquelle les mots ba et 1 sont réduits.

On a utilisé l'*algorithme de Knuth-Bendix* qui construit une présentation convergente $\Sigma, \mathcal{R}$ à partir d'une présentation finie et d'un *ordre de terminaison* sur Σ^* : voir [3]. Mais cet algorithme ne permet pas de résoudre le problème du mot dans tous les cas.

Un contre-exemple classique à la méthode de Knuth-Bendix que l'on vient d'illustrer est la présentation du monoïde $\mathbf{B}_3^+$ des *tresses positives* par les symboles a, b et la relation $bab = aba$. Dans ce cas, l'algorithme ne termine pas. En fait, il est impossible de construire une présentation convergente finie de $\mathbf{B}_3^+$ sans ajouter de nouveau générateur. On y arrive si on introduit le générateur superflu $c = ab$.

En 1987, C. C. Squier construit un exemple de monoïde finiment présenté pour lequel le problème du mot est décidable, mais qui n'a aucune présentation convergente finie. Il utilise le critère suivant : si un monoïde M admet une présentation convergente finie, alors son groupe d'homologie $\mathrm{H}_3(M)$ est de type fini. Voir [4].

Ces travaux sont à l'origine d'une *théorie homotopique du calcul* qui relie la réécriture à l'algèbre homotopique en passant par la notion de *catégorie de dimension supérieure*. Cette théorie fournit de nouveaux outils pour calculer les invariants homologiques de groupes ou de structures algébriques plus générales. Voir [5] et [6] pour en savoir plus.

Références

[1] S. Anderaa & E. Cohen, Modular machines, the word problem for finitely presented groups, Collins' theorem. *Word Problems II. The Oxford book*, Adjan, Boone, Higman, North-Holland, 1980, p. 1–16.

[2] J. Stillwell, The word problem and the isomorphism problem for groups. *Bulletin AMS* 6, 1982, p. 33–56.

[3] D. Kapur & P. Narendran. The Knuth-Bendix completion procedure and Thue systems. *SIAM journal on computing* 14 (4), 1985, p. 1052–1072.

[4] C. Squier. Word problems and a homological finiteness condition for monoids. *Journal of Pure and Applied Algebra* 49, 1987, p. 201–217.

[5] Y. Lafont, Algebra and Geometry of Rewriting. *Applied Categorical Structures* 15, 2007, p. 415–437.

[6] Y. Lafont, F. Métayer, Polygraphic resolutions and homology of monoids. *Journal of Pure and Applied Algebra* 213 (6), 2009, p. 947–968.