ELSEVIER

Theoretical Computer Science 145 (1995) 229–240

Theoretical Computer Science

# Variétés et fonctions rationnelles

Christophe Reutenauer[a,*,1], Marcel Paul Schützenberger[b]

[a] *Université du Québec à Montréal, C.P. 8888, succursale Centre Ville, Montréal, Québec, Canada H3C 3P8*

[b] *97 rue du Ranelagh, 75016 Paris, France*

Reçu avril 1994

Communiqué par M. Nivat

**Abstract**

We say that a rational (resp. a subsequential) function $\alpha$ from a free monoid into another one is in the variety of monoids $V$ if it may realized by some unambiguous (resp. subsequential) transducer whose monoid of transitions is in $V$. We characterize these functions when $V$ is the variety of aperiodic monoids, and the variety of groups. In the first case, the period of $\alpha^{-1}(L)$ divides that of $L$, for each rational language $L$ on the outputs. In the second case, $\alpha^{-1}(L)$ is a group-language for each group language $L$; equivalently, $\alpha$ is continuous for the pro-finite topology. Examples of such functions are: the multiplication by a given number in a given basis, which is aperiodic; the division, which is a group-function.

## 1. Introduction

Dans la théorie des variétés de langages et de monoïdes, le théorème d'Eilenberg met en correspondance les (pseudo-) variétés de monoïdes finis et les variétés de langages rationnels. Ces dernières sont closes par image inverse des morphismes de monoïdes libres.

Dans le contexte des automates finis, les morphismes se généralisent en les fonctions rationnelles. Ceci suggère le problème de caractériser l'action par image inverse des fonctions rationnelles sur les variétés. À toute fonction rationnelle, on peut associer un monoïde. Notre résultat principal caractérise, en termes de leur action, les fonctions rationnelles pour lesquelles ce monoïde est apériodique ou un groupe: dans le premier cas la fonction divise les périodes des langages rationnels (en particulier, elle préserve les langages apériodiques). Dans le second cas, elle préserve les rationnels à groupe; de manière équivalente, elle est continue pour la topologie pro-finie; incidemment, nous montrons qu'elle est aussi pluri-sous-séquentielle. Un corollaire du résultat principal

*Auteur correspondant.

[1] Le premier auteur a bénéficié d'une subvention CRSNG (Canada) et d'une subvention Action Concerté FCAR-BNR-CRSNG.



*SSDI* 0304-3975(94)00180-4

est une caractérisation des morphismes: une fonction rationnelle est un morphisme dès qu'elle divise les périodes et préserve les rationnels à groupe par image inverse.

Deux exemples bien connus des écoliers illustrent les deux classes de fonctions rationnelles considérées dans cet article.

Il s'agit de la multiplication et de la division, qui sont respectivement des fonctions rationnelles apériodiques et à groupe. Classiquement, elles se font respectivement de droite à gauche, et de gauche à droite: ce sont des fonctions sous-séquentielles. Cette problématique sur les quatre opérations arithmétiques est évoquée dans une question de Placiard et dans les réponses données par Lagrange et Monge lors des cours à l'École normale de l'an III, [6, pp. 197–198) et l'incidente mentionnée ci-dessus y ajoute les remarques suivantes: la division peut *presque* se faire de droite à gauche, c'est-à-dire qu'elle est pluri-sous-séquentielle de droite à gauche; par contre, la multiplication n'est pas pluri-sous-séquentielle de gauche à droite.

## 2. Fonctions rationnelles dans une variété de monoïdes

Soit $V$ une variété de monoïdes, c'est-à-dire [8] une classe de monoïdes finis fermée pour les opérations "quotient", "sous-monoïde" et "produit direct fini". Nous ferons de plus l'hypothèse que $V$ est fermée pour le produit semi-direct. Soit $\alpha: A^* \to B^*$ une fonction (partielle) d'un monoïde libre (finiment engendré) dans un autre.

Si $\alpha$ est sous-séquentielle (de gauche à droite), nous dirons que $\alpha$ *est dans* $V$ si $\alpha$ est réalisée par un transducteur sous-séquentiel dont le monoïde des transitions (obtenu en oubliant les sorties du transducteur) appartient à $V$; de manière équivalente, le transducteur minimal de $\alpha$ a cette propriété.

Pour la notion de transducteur sous-séquentiel minimal, voir l'article de Choffrut [4, Prop. 4] ou [13, Th. 2]. De manière équivalente, en utilisant les notations de ce dernier article, l'action à droite de $A^*$ sur l'ensemble fini $\{\alpha \cdot w | w \in A^*\}$ détermine un monoïde dans $V$. Dans le cas où $\alpha$ est séquentielle, cette définition généralise celle d'Eilenberg [8, p. 81; 7, Th. XII.4.2].

Lorsque $\alpha$ est une fonction rationnelle, nous dirons que $\alpha$ *est dans* $V$ si elle satisfait à l'une des conditions équivalentes suivantes:

- $\alpha$ est réallisée par un transducteur non ambigu dont le monoïde des transitions (obtenu en oubliant les sorties) est dans $V$.
- $\alpha$ est réalisée par une bimachine dont les monoïdes de transitions gauche et droit sont dans $V$.
- $\alpha$ est le produit de deux fonctions séquentielles (ou sous-séquentielles) dans $V$, l'une de gauche à droite et l'autre de droite à gauche.

Pour les notions de transducteurs non-ambigus et de bimachines, voir [7, IX.7; 1, IV. 4 et 5]; il faut ici prendre les bimachines comme dans [14], afin de pouvoir réaliser toutes les fonctions rationnelles. L'équivalence de ces définitions résulte des construc-

tions classiques démontrant qu'une fonction est rationnelle si et seulement si elle est réalisée par un transducteur non ambigu (resp. par une bimachine, resp. est produit d'une fonction séquentielle gauche et d'une droite); voir [1, Th. IV. 5.1 et 5.2; 17, 2.3].

Nous nous intéresserons ici aux cas où $V$ est soit la variété $A$ des monoïdes finis apériodiques, soit la variété $G$ des groupes finis.

Nous dirons $\alpha$ *apériodique* pour $\alpha$ dans $A$, et *à groupe* pour $\alpha$ dans $G$.

Rappelons que par le théorème des variétés d'Eilenberg, il correspond à toute variété $V$ de monoïdes finis, une variété $V$ de langages rationnels; voir [8, Th. VII. 3.4] ou [10, Th. 2.27]. Rappelons aussi que la *période* d'un langage rationnel $L \subseteq A^*$ est le plus petit multiple commun des exposants des groupes de son monoïde syntaxique, ou de manière équivalente, le plus petit $p \geqslant 1$ tel que: $\forall u, x, v \in A^*$, $ux^n v \in L \Leftrightarrow ux^{n+p}v \in L$, pour tout $n$ assez grand. Enfin, rappelons qu'un *langage rationnel à groupe* est un langage rationnel dont le monoïde syntaxique est un groupe.

**Théorème:** *Soit* $\alpha : A^* \to B^*$ *une fonction sous-séquentielle (resp. rationnelle).*

(i) $\alpha$ *est apériodique si et seulement si pour tout langage rationnel* $L$ *dans* $B^*$, *la période du langage* $\alpha^{-1}(L)$ *divise celle de* $L$.

(ii) $\alpha$ *est à groupe si et seulement si pour tout langage rationnel à groupe* $L$ *dans* $B^*$, $\alpha^{-1}(L)$ *est un langage rationnel à groupe.*

La partie (ii) est une extension d'un théorème de Choffrut [3, Prop. III. 2.2], qui l'a démontré dans le cas d'une fonction séquentielle.

La partie directe de ces deux assertions est classique; elle résulte des faits suivants:

- Lers variétés $A$ et $G$ sont fermées par produit en couronne (ou de manière équivalente, par produit semi-direct); voir [8, V.8]. Plus généralement, le produit en couronne d'un monoïde de période $p$ par un monoïde de périoide $q$ est de période divisant $pq$.
- Si $\alpha$ (resp. $\beta$) sont des fonctions rationnelles dans $V$ (resp. $W$), alors la fonction rationnelle produit $\alpha \circ \beta$ est dans $V * W$, la variété engendrée par les produits semi-directs $M * N$, $M \in V$, $N \in W$; voir [8, Prop. VI. 2.1 et Th. 7.3; 16 et 11].
- Le domaine de $\alpha \circ \beta$ est $\alpha^{-1}(\mathrm{dom}\,\beta)$, et la fonction caractéristique $\beta$ d'un langage rationnel est une fonction rationnelle.

La deuxième partie du théorème mérite un commentaire. Rappelons que *la topologie pro-finie* (ou topologie de Hall, ou de Krull) de $A^*$ est la topologie pour laquelle une base d'ouverts est formée par les rationnels à groupe; voir [12, 15].

On a alors le corollaire suivant.

**Corollaire 1.** *Soit* $\alpha : A^* \to B^*$ *une fonction sous-séquentielle (resp. rationnelle). Alors* $\alpha$ *est à groupe si et seulement si* $\alpha|\mathrm{dom}(\alpha)$ *est continue pour la topologie profinie et si* $\mathrm{dom}(\alpha)$ *est un rationnel à groupe.*

La nécessité de cette condition découle des considérations précédentes, puisque $\alpha^{-1}$ préserve alors les rationnels à groupe, donc $\alpha$ est continue. Il n'est pas difficile de voir qu'en fait $\alpha$ est même uniformément continue.

Nous verrons aussi qu'une telle fonction $\alpha$ est presque sous-séquentielle, en ce sens qu'elle est réunion de fonctions sous-séquentielles dont les domaines sont des rationnels à groupe disjoints: elle est donc *pluri-sous-séquentielle*, dans le sens de [5].

Appelons *morphisme affine* $\alpha: A^* \to B^*$ une fonction de la forme $\alpha(w) = u\,\beta(w)v$, où $u, v \in B^*$ et $\beta$ est un morphisme $A^* \to B^*$.

**Corollaire 2.** *Une fonction rationnelle non vide $\alpha: A^* \to B^*$ est un morphisme affine (resp. un morphisme) si et seulement si $\alpha^{-1}$ divise les périodes et préserve les rationnels à groupe (resp. et si de plus $\alpha(1) = 1$).*

**Preuve.** Sous ces hypothèses, $\alpha$ est apériodique et à groupe; on peut donc la réaliser par un transducteur dont le monoïde des transitions est le groupe trivial. Comme le mot vide induit l'identité sur l'ensemble des états, il en est de même pour toute lettre de $A$. Si donc $\alpha$ est non vide, on obtient par suppression des états inutiles, des états qui sont à la fois initiaux et finaux. Comme le transducteur est non ambigu, il y a en fait un seul tel état et $\alpha$ est un morphisme affine. □

## 3. Généralités

Un transducteur sera pour nous un graphe orienté avec ensemble d'états (sommets) $Q$, avec arêtes étiquetés dans $A \times B^*$, muni de deux fonctions (partielles) $i$ et $f$ (les *sorties initiales* et *finales*). Ce transducteur réalise la relation $\alpha: A^* \to B^*$ dont le graphe est l'ensemble des couples $(u, i(p)\,v\,f(q))$, pour tous les couples d'états $p$ et $q$, et tous les chemins de $p$ vers $q$ d'étiquette $(u, v)$. Une telle relation est dite rationnelle, et c'est une fonction rationnelle si elle est de plus fonctionnelle. Une fonction rationnelle peut toujours être réalisée par un transducteur non ambigu, i.e. tel que pour tout mot $u$, il existe au plus un chemin d'un état initial à un état final d'étiquette de la forme $(u, v)$ (un état $q$ est initial si $i(q) \neq \emptyset$, et final si $f(q) \neq \emptyset$).

La nécessité (mathématique) de la variante ci-dessus des définitions usuelles est illustrée par les transducteurs dans la Fig. 1. Dans celui de gauche, on illustre le fait qu'on a besoin des sorties initiales et finales, car il n'est pas raisonnable d'ajouter un état pour s'en dispenser; dans celui de droite, visiblement à groupe, on voit qu'il faut plusieurs états initiaux et finaux pour avoir un transducteur à groupe.

Le résultat suivant est bien connu. On identifie $\mathbb{N}$ avec le monoïde libre à un générateur.

**Lemme 3.1.** *Soit $\alpha: \mathbb{N} \to B^*$ une fonction rationnelle. Il existe alors une partie finie $F$ de $\mathbb{N}$, des entiers $a, b_i$ avec $a \geqslant 1$, et des mots $x_i, y_i, z_i$ pour $i = 0, \ldots, r-1$, tels que $\mathrm{dom}(\alpha)$ soit la réunion disjointe de $F$ et des $a\,\mathbb{N} + b_i$ et que pour tout $n$ dans $\mathbb{N}$,*

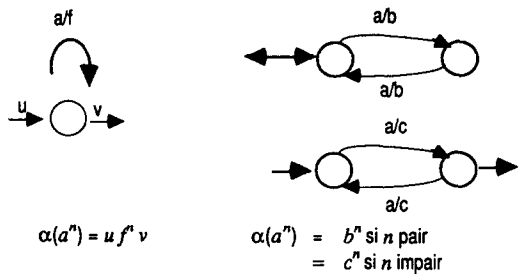


Fig. 1. (a) $\alpha(a^n) = u f^n v$; (b) $\alpha(a^n) = b^n$ si $n$ pair $= c^n$ si $n$ impair.

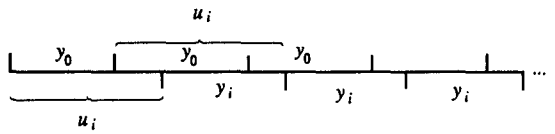


Fig. 2.

$\alpha(an + b_i) = x_i y_i^n z_i$. *On peut borner* $|x_i|$ (*resp.* $|y_i|$, *resp.* $|z_i|$, *resp.* $a, b_i, \max(F)$) *par une fonction ne dépendant que des sorties initiales et des étiquettes* (*resp. que des étiquettes, resp. que des sorties finales et des étiquettes, resp. que du nombre d'états*) *d'un transducteur pour* $\alpha$.

Pour deux mots $u, v$, nous notons $\lambda(u, v)$ leur plus long facteur gauche commun. La *distance préfixielle* est définie par $\|u, v\| = |u| + |v| - 2|\lambda(u, v)|$, où $|u|$ est la longueur de $u$. On définit de manière symétrique la *distance suffixielle*. Nous aurons besoin du lemme combinatoire sur les mots suivants.

**Lemme 3.2.** *Soient* $x_i$, $y_i$, $z_i$, $0 \leqslant i \leqslant a - 1$, *des mots tels que pour tous* $i, j$, *les suites* $d(x_i y_i^n z_i, x_j y_j^n z_j)$ *soient bornées, quand* $d$ *est la distance préfixielle et la distance suffixielle. Il existe alors des mots* $h, v, w$, *et des entiers* $s, r_i$ $(0 \leqslant i \leqslant a - 1)$ *tels que pour tout* $n$ $x_i y_i^n z_i = v h^{sn} h^{r_i} w$.

**Preuve.** Clairement, les $y_i$ ont tous la même longueur. Pour $n$ grand, $x_i y_i^n z_i$. et $x_j y_j^n z_j$ ont un long préfixe commun, qui excède $x_i$ et $x_j$: les $x_i$ sont donc tous comparables pour l'ordre préfixiel. Soit $x_0$ le plus petit d'entr'eux: nous avons $x_i = x_0 u_i$; comme $|y_0| = |y_i|$ et que pour $n$ grand, $y_0^n z_0$ et $u_i y_i^n z_i$ ont un long préfixe commun, nous obtenons $u_i y_i = y_0 u_i$(voir Fig. 2).

Par suite, $x_i y_i^n z_i = x_0 u_i y_i^n z_i = x_0 y_0^n u_i z_i$, et nous sommes ramenés au cas où les suites sont de la forme $v y^n z_i$. Comme ci-dessus, les $z_i$ sont tous comparables pour l'ordre suffixiel, et nous écrivons $z_i = p_i z_0$, ce qui donne: $v y^n z_i = v y^n p_i z_0$. Comme

précédemment, $v\,y^n\,z_0$ et $v\,y^n\,p_i z_0$ ont un long facteur droit commun et ceci implique $y\,p_i = p_i\,y$. Mais alors $y = h^s$, $p_i = h^{r_i}$, d'où finalement $x_i\,y_i^n\,z_i = v\,h^{sn}\,h^{r_i}\,z_0$. □

Rappelons qu'une fonction $\alpha: A^* \to B^*$ est sous séquentielle si et seulement si la congruence à droite $\sim$ de $A^*$ définie par: $u \sim v \Leftrightarrow \exists g \in B^{(*)}$ (le groupe libre sur $B$) tel que $\forall f \in A^*$, $\alpha(uf) = g\alpha(vf)$, est d'index fini (voir [4]).

On a $u \sim v \Leftrightarrow \alpha \cdot u = \alpha \cdot v$, où $\alpha \cdot u$ est la fonction obtenue à partir de la fonction $f \mapsto \alpha(uf)$ en enlevant à tous les mots $\alpha(uf)$ leur plus long préfixe commun (voir [13]); $(\alpha, u) \mapsto \alpha \cdot u$ est une action à droite du monoïde libre $A^*$.

Le fait que $\alpha$ est dans une variété $V$ se traduit par le fait que l'action de $A^*$ sur l'ensemble fini $\{\alpha \cdot u | u \in A^*\}$ induit un monoïde dans $V$. Donc $\alpha$ est apériodique si et seulement si: $\forall f \in A^*$, $\exists n \in \mathbb{N}$ tel que $\forall u \in A^*$, $\alpha \cdot uf^n = \alpha \cdot uf^{n+1}$. Et $\alpha$ est à groupe si et seulement si: $\forall f \in A^*$, $\exists n \in \mathbb{N}^*$ tel que $\forall u \in A^*$, $\alpha \cdot u = \alpha \cdot uf^n$. Dans les deux cas, on peut légèrement affaiblir la condition en mettant "$\forall u \in A^*$ "avant "$\exists n \in \mathbb{N}^*$", puisque l'ensemble $\{\alpha \cdot u | u \in A^*\}$ est fini; on fera ainsi dépendre $n$ de $u$, mais il n'y a qu'un nombre fini de cas, et on prendra le maximum (resp. le *ppmc*) de tous ces $n$.

## 4. Le cas apériodique

Nous disons que $\alpha^{-1}$ *divise les périodes* si pour tout langage rationnel $L$, la période de $\alpha^{-1}(L)$ divise celle de $L$. Nous commençons par traiter le cas d'une fonction rationnelle $\mathbb{N} \to \mathbb{N}$. La preuve n'utilise que de l'arithmétique élémentaire.

**Lemme 4.1.** *Soit $\alpha: \mathbb{N} \to \mathbb{N}$ une fonction rationnelle telle que $\alpha^{-1}$ divise les périodes. Alors $\alpha$ est soit de domaine fini, soit de la forme $\alpha(n) = \rho n + \beta_0$ pour $n$ assez grand, où $\rho, \beta_0 \in \mathbb{N}$.*

Le lecteur se convaincra que l'hypothèse "$\alpha^{-1}$ préserve l'apériodicité" ne suffit pas à assurer la conclusion.

**Preuve.** Nous pouvons supposer sans perte de généralité que $\mathrm{dom}(\alpha)$ est infini. De même, comme $\alpha^{-1}$ divise les périodes, $\mathrm{dom}(\alpha) = \alpha^{-1}(\mathbb{N})$ est apériodique, donc co-fini, et nous pouvons supposer que $\mathrm{dom}(\alpha) = \mathbb{N}$. Utilisant le Lemme 3.1, nous avons donc pour $n$ dans $\mathbb{N}$, $\alpha(an + i) = \pi_i n + \beta_i$, $i = 0, \ldots, a-1$, où $\pi_i, \beta_i \in \mathbb{N}$.

Rappelons qu'une partie reconnaissable de $\mathbb{Z}$ est une réunion de classes mod. $p$ ($p \in \mathbb{N}^*$), et que sa période est le plus petit tel $p$. Nous pouvons prolonger $\alpha$ à $\mathbb{Z}$ en prenant la formule ci-dessus pour $n$ dans $\mathbb{Z}$; alors l'hypothèse sur $\alpha$ implique que $\alpha^{-1}(q\mathbb{Z} + d)$ est une partie reconnaissable de $\mathbb{Z}$ de période divisant $q$. Nous prenons pour $q$ un nombre premier avec $a$ et les $\pi_i$, et assez grand.

Notons $\pi_i^1$ un entier tel que $\pi_i\,\pi_i^1 \equiv 1 \bmod q$. Les solutions $n \in \mathbb{Z}$ de l'équation $\pi_i n + \beta_i \equiv d \bmod q$ forment l'ensemble $\pi_i^1(d - \beta_i) + q\mathbb{Z}$; par suite $\alpha^{-1}(d + q\mathbb{Z}) = \bigcup_{0 \leqslant i \leqslant a-1} (aq\mathbb{Z} + c_i)$, avec $c_i = i + (d - \beta_i)\,\pi_i^1\,a$. Par hypothèse, la période de cet ensemble divise $q$. Il faut donc que, pour un entier $k$,

$\{c_0, \ldots, c_{a-1}\} \equiv \{k, k+q, \ldots, k+q(a-1)\}$ mod. $aq$ Par suite $c_i - c_j \equiv 0 \bmod q$, c'est-à-dire $d\,a(\pi_i^1 - \pi_j^1) + i - j - \beta_i \pi_i^1 a + \beta_j \pi_j^1 a \equiv 0$. Ceci n'est possible pour tout $d$ que si $\pi_i^1 \equiv \pi_j^1$, donc $\pi_i \equiv \pi_j$ et enfin $\pi_i = \pi_j$ par le choix de $q$.

Nous avons donc $\pi_0 = \ldots \pi_{a-1} = \pi$. Par suite, en prenant $j = 0$ ci-dessus, nous obtenons $0 \equiv c_i\pi - c_0\pi = i\pi - a(\beta_i - \beta_0)$. Comme $q$ est grand, on a $i\pi = a(\beta_i - \beta_0)$; pour $i = 1$, nous trouvons que $a$ divise $\pi$, $\pi = \rho a$, donc $\beta_i = \beta_0 + i\rho$.

Enfin, $\alpha(an + i) = \rho an + i\rho + \beta_0 = \rho(an + i) + \beta_0$. Donc $\alpha$ est de la forme voulue. □

Le cas suivant est celui d'une fonction $\mathbb{N} \to B^*$.

Lemme 4.2. *Soit $\alpha: N \to B^*$ une fonction rationnelle telle que $\alpha^{-1}$ divise les périodes. Il existe alors des mots $x, y, z$ dans $B^*$ et un entier $N$ tels que $\forall n \geqslant N$, $\alpha(n) = x y^n z$. On peut borner $|x|$ (resp. $|y|$, resp. $N$) comme dans le Lemme* 3.1.

**Preuve.** Comme dans la preuve précédente, nous pouvons supposer que dom($\alpha$) est infini, donc co-fini.

Par le Lemma 3.1, nous avons alors pour tout $n$ dans $\mathbb{N}$ assez grand,

$$\alpha_i(an + i) = x_i y_i^n z_i, \quad i = 0, 1, \ldots, a-1.$$

Appliquant le Lemme 4.1 à la fonction rationnelle $n \to |\alpha(n)|$, nous obtenons que $|y_i| = \rho a$ et $|x_i| + |z_i| = \beta_0 + i\rho$.

Supposons que $u_i = x_i y_i^n$ et $u_j = x_j y_j^n$ ne soient pas comparables pour l'ordre préfixiel. Alors les langages apériodiques $u_i B^*$ et $u_j B^*$ sont disjoints, et par suite $\alpha^{-1}(u_i B^*)$ contient $a\mathbb{N} + an + i$ et ne rencontre pas $a\mathbb{N} + an + j$. Donc $\alpha^{-1}(u_i B^*)$ n'est apériodique que si $a = 1$.

Nous en concluons que soit $a = 1$ (auquel cas le lemme est démontré), soit que $x_i y_i^n$ et $x_j y_j^n$ sont comparables pour l'ordre préfixiel: donc l'un est préfixe de l'autre et $d(x_i y_i^n z_i, x_j y_j^n z_i)$ est borné pour $n \in \mathbb{N}$, quand $d$ est la distance préfixielle. Il en est de même pour la distance suffixielle.

Nous appliquons le Lemme 3.2 et obtenons que $x_i z y_i^n z_i = v h^{sn} h^{ri} w$. Par suite, $a\rho = |y_i| = s|h|$ et $|v| + |w| + r_i|h| = \beta_0 + i\rho$. On en déduit $\rho = (r_1 - r_0)|h| = r|h|$, d'où $s = ar$ et $r_i = ir + t$. Finalement, $\alpha_i(an + i) = x_i y_i^n z_i = v h^{arn + ir} h^t w = v(h^r)^{an+i} h^t w$, donc $\alpha(n) = v(h^r)^n h^t w$ pour $n$ assez grand, ce qu'il fallait démontrer.

Les assertions sur les bornes découlent des assertions analogues dans le Lemme 3.1. □

Nous pouvons maintenant démontrer le théorème dans le cas apériodique.

Nous supposons d'abord que $\alpha$ est sous-séquentielle. Fixons les mots $u$ et $f$. Alors pour tout mot $v$, la fonction $\beta: \mathbb{N} \to B^*$, $n \mapsto \alpha(uf^n v)$ est rationnelle et $\beta^{-1}$ divise les périodes car $\beta$ est composée de deux fonctions ayant cette propriété. On a donc d'après le Lemme 4.2: $\alpha(uf^n v) = x_v y_v^n z_v$ pour $n$ assez grand. Comme $\alpha$ est sous-séquentielle, donc uniformément bornée pour la distance préfixielle (voir [14]; à variation bornée selon [4, 1], nous pouvons choisir $x_v$ et $y_v$ indépendamment de $v$.

On a donc $\alpha(uf^n v) = xy^n z_v$ et $\alpha(uf^{n+1}v) = xy^{n+1}z_v$, ce qui prouve que $\alpha$ est apériodique (cf. la fin du Section 3).

Prenons maintenant une fonction $\alpha$ rationnelle. Dans [14] a été définie la *congruence syntaxique gauche* $\sim$ de $\alpha$, qui est une congruence à gauche de $A^*$. Nous montrons que $\sim$ est apériodique, i.e. que pour tout mot $f$, il existe $n$ tel que pour tout mot $v$, on ait $f^n v \sim f^{n+1}v$. Ceci revient à montrer que $d(\alpha(uf^n v), \alpha(uf^{n+1}v))$ est borné quand $u$ parcourt $A^*$, où $d$ est la distance préfixielle. Nous pouvons fixer $v$ (car d'après [14], $\sim$ est d'index fini) et $f$.

D'après le Lemme 4.2 (appliqué à $\beta_u : n \mapsto \alpha(uf^n v)$), nous avons $\alpha(uf^n v) = x_u y_u^n z_u$ pour $n \geqslant N_u$. On obtient un transducteur $T_u$ pour $\beta_u$ simplement à partir d'un transducteur pour $\alpha$, et quand $u$ varie, seul varient l'ensemble des états initiaux et les sorties initiales de $T_u$.

Donc d'après le même lemme, les mots $y_u$, $z_u$ sont en nombre fini quand $u$ varie, et $N_u$ est borné. Par suite, $d(\alpha(uf^n v), \alpha(uf^{n+1}v)) = d(x_u y_u^n z_u, x_u y_u^{n+1} z_u) = d(z_u, y_u z_u)$ est borné quand $u \in A^*$, pour $n \geqslant \max_u(N_u)$. Ceci montre que $\sim$ est apériodique.

Nous suivons maintenant la construction de [14, p. 675]. On obtient une transduction séquentielle injective de droite à gauche $\gamma$, dont l'automate des entrées est $A^*/\sim$ (donc $\gamma$ est apériodique), dont l'inverse $\gamma^{-1}$ est la restriction d'un morphisme à un langage local (donc $\gamma^{-1}$ est apériodique et $\gamma$ divise les périodes), et une fonction sous-séquentielle de gauche à droite $\beta$ telle que $\alpha = \beta \circ \gamma$ et $\beta = \alpha \circ \gamma^{-1}$. Alors $\beta^{-1}(L) = \gamma(\alpha^{-1}(L))$, pour tout langage $L$, et $\beta$ divise les périodes. Par ce qui précède, $\beta$ est apériodique, et il en est donc de même pour $\alpha$.

**Remarque.** Soit $n$ un entier et $V$ la variété des monoïdes finis dont la période divise $n$ (cf. [8, p. 280]). Il serait intéressant de caractériser les fonctions rationnelles dans $V$; la partie (i) du théorème concerne le cas $n = 1$.

## 5. Le cas des groupes

Rappelons que la topologie pro-finie de $B^*$ est compatible avec sa structure de monoïde, et que $\lim g^{n!} = 1$.

**Lemme 5.1.** *Soit $\alpha : \mathbb{N} \to B^*$ une fonction rationnelle telle que* $\mathrm{dom}(\alpha)$ *soit un rationnel à groupe $\neq \emptyset$ et que $\alpha \mid \mathrm{dom}(\alpha)$ est continue pour la topologie pro-finie. Il existe alors $a \geqslant 1$, $D \subseteq \{0, 1, \ldots, a-1\}$ et des mots $x_i$, $y_i$, $z_i$ tels que pour $i$ dans $D$ et $n$ dans $\mathbb{N}$, $\alpha(an + i) = x_i y_i^n z_i$, et que* $\mathrm{dom}(\alpha) = \bigcup_{i \in D}(a\mathbb{N} + i)$. *Les nombres $|x_i|$ (resp. $|y_i|$, resp. $|z_i|$, resp. a) peuvent être bornés comme dans le Lemme* 3.1.

**Preuve.** Comme $\mathrm{dom}(\alpha)$ est un rationnel à groupe, le Lemme 3.1 nous donne que $\mathrm{dom}(\alpha) = \bigcup_{i \in D}(a\mathbb{N} + i)$, $D \subseteq \{0, 1, \ldots, a-1\}$ et que pour $i \in D$, $\alpha(an + i) = x_i y_i^n z_i$ sauf peut-être pour un nombre fini de $n$; mais cette formule est valable pour tout

$n$, par continuité de $\alpha$, car $\alpha(an+i) = \lim_{k\to\infty} \alpha(a(n+k!)+i) = \lim_{k\to\infty} x_i y_i^n y_i^{k!} z_i = x_i y_i^n z_i$. □

Pour démontrer le théorème dans le cas (ii), il suffit de démontrer le Corollaire 1, puisque si $\alpha^{-1}$ préserve les langages rationnels à groupe, dom($\alpha$) est un rationnel à groupe, et $\alpha \mid \mathrm{dom}(\alpha)$ est continue.

Soit d'abord $\alpha$ sous-séquentielle. Pour tout mot $f$, il existe des entiers $p$ et $N$ tels que pour tout mot $u$, $\alpha \cdot uf^n = \alpha \cdot uf^{n+p}$ pour $n \geqslant N$. Nous montrons qu'on peut prendre $N = 0$, ce qui prouvera que $\alpha$ est à groupe.

Fixons $u$ et $f$. Il existe un élément $g$ du groupe libre $B^{(*)}$ tel que $\alpha(uf^{n+p}v) = g\alpha(uf^n v)$ pour tout $n \geqslant N$ et tout mot $v$. Fixons $v$. La fonction (partielle) $\gamma : \mathbb{N} \to B^{(*)}, n \mapsto \alpha(uf^{n+p}v)\alpha(uf^n v)^{-1}$ satisfait donc à $\gamma(n) = g$ si $n \in \mathrm{dom}(\gamma)$ et $n \geqslant N$.

Or, la fonction $n \mapsto uf^n v$ est sous-séquentielle à groupe, donc $\beta : n \mapsto \alpha(uf^n v)$ est sous-séquentielle, son domaine est un rationnel à groupe et $\beta \mid \mathrm{dom}(\beta)$ est continue. Nécessairement, dom($\beta$) est une réunion de classes mod. $p$. Alors, dom($\gamma$) = dom($\beta$), pour $n$ dans dom($\beta$), $\gamma(n) = \beta(n+p)\,\beta(n)^{-1}$ et $\gamma \mid \mathrm{dom}(\gamma)$ est continue.

Si $0 \notin \mathrm{dom}(\beta)$, nous avons $p \notin \mathrm{dom}(\gamma)$ et $\beta(p) = g\beta(0)$. Si $0 \in \mathrm{dom}(\beta)$, alors $p\,\mathbb{N} \subseteq \mathrm{dom}(\beta)$, et par continuité, $\gamma(0) = \lim_{n\to\infty} \gamma(pn!) = g$. Donc $\beta(p) = g\beta(0)$. Nous avons donc $\alpha(uf^p v) = g\,\alpha(uv)$ pour tout $v$, ce qui montre que $\alpha \cdot uf^p = \alpha \cdot u$. Donc $\alpha$ est à groupe.

Soit maintenant $\alpha$ une fonction rationnelle, avec dom($\alpha$) rationnel à groupe et $\alpha \mid \mathrm{dom}(\alpha)$ continue. Nous montrons que la congruence syntaxique gauche de $\alpha$ définit un groupe. Il s'agit de montrer que pour tous mots $f$ et $v$, il existe $p \geqslant 1$ tels que $d(\alpha(uf^p v), \alpha(uv))$ est borné quand $u$ parcourt $A^*$ ($d$ est la distance préfixielle). Fixons $f$ et $v$ et considérons la fonction $\beta_u : \mathbb{N} \to B^*$, $\beta_u(n) = \alpha(uf^n v)$.

Elle satisfait aux hypothèses du Lemma 5.1, et nous en concluons l'existence de mots $x_{iu}$, $y_{iu}$, $z_{iu}$, d'un entier $a_u$ et de $D_u \subseteq \{0, 1, \ldots, a_u - 1\}$ tels que $\mathrm{dom}(\beta_u) = \bigcup_{i \in D_u} (a_u\mathbb{N} + i)$ et $\beta_u(a_u n + i) = x_{iu} y_{iu}^n z_{iu}$ pour $n \in \mathbb{N}$ et $i \in D_u$. Un transducteur pour $\beta_u$ s'obtient simplement à partir d'un transducteur pour $\alpha$, et quand $u$ varie, seuls varient l'ensemble des états initiaux et les sorties initiales. Par suite, les $y_{iu}$, $z_{iu}$, $a_u$ et $D_u$ sont en nombre fini quand $u$ parcourt $A^*$.

Soit $p$ le $ppmc$ des $a_u$. Alors, soit $\beta_u(0) = \beta_u(p) = \emptyset$, soit $\beta_u(0) = x_{0u} z_{0u}$ et $\beta_u(p) = x_{0u} y_{0u} z_{0u}$. Donc $d(\alpha(uv), \alpha(uf^p v)) = d(\beta_u(0), \beta_u(p)) = d(x_{0u} z_{0u}, x_{0u} y_{0u} z_{0u}) = d(z_{0u}, y_{0u} z_{0u})$ qui est borné quand $u$ parcourt $A^*$.

Comme la congruence syntaxique gauche de $\alpha$ est à groupe, il existe un groupe fini $G$ et un homomorphisme $\varphi : A^* \to G$ tel que: $\forall x, y \in A^*$, $\varphi(x) = \varphi(y) \Rightarrow d(\alpha(fx), \alpha(fy))$ est borné quand $f$ parcourt $A^*$.

Soit $L_g = \varphi^{-1}(g)$. Nous montrons que $\alpha \mid L_g$ est sous-séquentielle à groupe. On en déduira que $\alpha$ est à groupe: on obtient en effet un transducteur non ambigu pour $\alpha$ en prenant la réunion des transducteurs non ambigus des $\alpha \mid L_g$, $g \in G$.

Il suffit de monter que $\alpha \mid L_g$ est sous-séquentielle, puisqu'alors son domaine est le rationnel à groupe $\mathrm{dom}(\alpha) \cap L_g$, et que sa restriction à ce domaine est continue. D'après le théorème de Choffrut [4], il est suffisant de montrer que $\alpha \mid L_g$ est

uniformément bornée, i.e. $\forall k$, $\exists K$ tel que $\forall u$, $v \in L_g$, $\alpha(u) \neq \emptyset \neq \alpha(v)$ et $d(u,v) \leqslant k \Rightarrow d(\alpha(u), \alpha(v)) \leqslant K$. Si $d(u,v) \leqslant k$ et $u$, $v \in L_g$, nous avons $u = fx$, $v = fy$ avec $|x| + |y| \leqslant k$. De plus, $\varphi(u) = \varphi(v) = g \Rightarrow \varphi(x) = \varphi(y)$. De la relation après la définition de $\varphi$ et de la finitude de l'ensemble des mots $x$, $y$ sujets à $|x| + |y| \leqslant k$, nous pouvons déduire l'existence d'une borne $K$, ne dépendant pas de $f$, telle que $d(\alpha(u), \alpha(v)) \leqslant K$.

> "... *Je désirerais que vous développassiez les raisons pour lesquelles on commence plutôt cette dernière par la gauche que par la droite ...*"
> *Placiard* [6, p. 197]

## 6. Exemples

Soit $b$ un entier $\geqslant 2$ fixé, et $A = \{0, 1, \ldots, b-1\}$. Pour un entier $a \geqslant 1$ fixé, soit $d_a : A^* \to A^*$ la *division euclidienne par a en base b*, i.e. la fonction qui à un mot $u$, représentant l'entier $n$ en base $b$, associe l'unique mot $v$ de même longueur que $u$, représentant l'entier $q$ tel que $n = qa + r$, $0 \leqslant r < a$.

La fonction $d_a$ est séquentielle de gauche à droite. Si $a$ et $b$ sont premiers entr'eux, elle est sous-séquentielle à groupe, et le groupe associé est le groupe des transformations de $\mathbb{Z}/a\mathbb{Z}$ engendré par les $b$ transformations $r \mapsto rb + i$ mod. $a$, pour $i = 0, 1, \ldots, b-1$.

La fonction $d_a$ est donc pluri-sous-séquentielle de droite à gauche, et l'on peut faire la division de droite à gauche, pourvu qu'on ait sur $n$ une information supplémentaire: à savoir $n$ mod. $a$. Voir Fig. 3, où il faut lire le nombre binaire $n$ de droite à gauche, en partant de l'état $n$ mod. 3.

Lorsque $a$ et $b$ ne sont pas premiers entr'eux, la division se fait en deux temps: on écrit $a = a'a''$, $(a', b) = 1$, où tout diviseur premier de $a''$ divise $b$. Alors, comme on l'a vu, $d_{a'}$ est pluri-sous-séquentielle de droite à gauche, et $d_{a''}$ est sous-séquentielle de droite à gauche (voir [13] par exemple). On a $d_a = d_{a'} d_{a''}$, et l'on observe que le produit de deux fonctions pluri-sous-séquentielles l'est aussi.

Venons-en à la *multiplication par a en base b* $m_a : A^* \to A^*$.

Cette fonction est sous-séquentielle de droite à gauche comme on le sait intuitivement (voir [13] pour une preuve formelle). Elle est apériodique. Nous le vérifions pour $1 \leqslant a \leqslant b-1$.

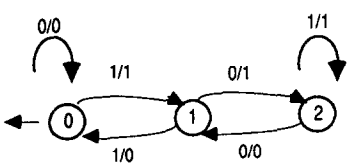


Fig. 3. La division par 3 en base 2 de droite à gauche.

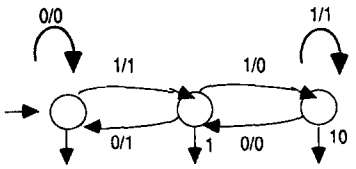


Fig. 4. La multiplication par 3 en base 2.

Dans ce cas, on réalise la fonction $m_a$ à l'aide d'un transducteur sous-séquentiel de droite à gauche, dont l'ensemble des états est $R = \{0, 1, \ldots, a-1\}$, i.e. les reports, ou retenues, possibles quand on multiplie par $a$. Chaque lettre $i$ de l'alphabet $\{0, 1, \ldots, b-1\}$ induit sur $R$ la fonction $f_i(r) = [(ai + r)/b]$. Chaque fonction $f = f_i$ satisfait à $r \leqslant r' \Rightarrow f(r) \leqslant f(r')$, et il en est de même pour toute fonction dans le sous-monoïde engendré par les $f_i$. Donc aucune de ces fonctions n'induit de bijection non triviale sur une partie de $R$, ce qui montre que ce monoïde est apériodique.

Ainsi $m_a$ est apériodique.

Dans la Fig. 4, nous donnons l'exemple de la multiplication par 3 en base 2 (cet automate nous a été aimablement communiqué par Colin de la Higueira, et simplifie celui de [13]); il faut y lire les nombres binaires de droite à gauche. On peut vérifier que l'automate de gauche à droite associé (obtenu en renversant les flèches) a des branchements absolus et par suite [5, Th. IV. 1] la multiplication n'est pas pluri-sous-séquentielle de gauche à droite.

Aux exemples précédents, il faut rajouter les travaux de [2], qui considère divers types d'addition, ainsi que ceux de [9], pour la base Fibonacci; il s'y pose aussi le problème de la normalisation dans cette base, qui est une fonction rationnelle.

## Références

[1] J. Berstel, *Transductions and Context-Free Languages* (Teubner, Leipzig, 1979).
[2] J. Berstel, Fonctions rationnelles et addition, École de Printemps d'Informatique Théorique, Murol, Litp/Ensta, Paris, 1981.
[3] C. Choffrut, Contribution à l'étude de quelques familles remarquables de fonctions rationnelles, Thèse Doctorat d'Etat, Univ. Paris VII, 1978.
[4] C. Choffrut, A generalization of Ginsburg and Rose's characterization of *g-s-m* mappings, dans: Lecture Notes in Computer Science, Vol. 71 (Springer, Berlin, 1979) 88–103.
[5] C. Choffrut et M.P. Schützenberger, Décomposition des fonctions rationnelles, dans: Lecture Notes in Computer Science, Vol. 210 (Springer, Berlin, 1986) 213–226.
[6] J. Dhombres, *L'École Normale de l'An III, Leçons de Mathématiques* (Laplace, Lagrange et Monge) (Dunod, Paris, 1992).
[7] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).
[8] S. Eilenberg, *Automata, Languages and Machines, Vol. B* (Academic Press, New York 1976).
[9] C. Frougny, Representation of numbers and finite automata, *Math. Systems Theory* **25** (1992) 37–60.
[10] J.-E. Pin, *Variétés de Langages Formels* (Masson, Paris, 1984).

[11] J.-E. Pin, J. Sakarovitch, Une application de la représentation matricielle des transductions, *Theoret. Comput. Sci.* **35** (1985) 271–293.
[12] J.-E. Pin, Topologies for the free monoid, *J. Algebra* **137** (1991) 297–337.
[13] C. Reutenauer, Subsequential functions: characterizations, minimization, examples, dans Lecture Notes in Computer Science, Vol. 464 (Springer, Berlin, 1990) 62–79.
[14] C. Reutenauer et M.P. Schützenberger, Minimization of rational word functions, *SIAM J. Comput.* **20** (1991) 669–685.
[15] L. Ribes et P.A. Zaleskii, On the profinite completion on a free group, *Bull. London Math. Soc.* **25** (1993) 37–43.
[16] J. Sakarovitch, Sur la définition du produit en couronne, dans: G. Pirillo, éd., *Actes du Colloque "Codages et Transductions"* (CNR, Rome, 1979) 285–300.
[17] M.P. Schützenberger, Sur les relations rationnelles entre monoïdes libres, *Theoret. Comput. Sci.* **3** (1976) 243–259.