Theoretical Computer Science 3 (1976) 243–259.

SUR LES RELATIONS RATIONNELLES ENTRE MONOIDES LIBRES

M.P. SCHÜTZENBERGER

Université de Paris VII, Paris, et I.R.I.A., Le Chesnay, Yvelines, France

Communiqué par Maurice Nivat
Reçu en mars 1976

Résumé. On applique la théorie de S. Eilenberg au moyen de la méthode des transducteurs de M. Nivat pour obtenir quelques indications sur la vitesse de croissance en fonction de la longueur du mot du nombre de mots de l'image d'une relation rationnelle.

1. Introduction

(1) L'objectif du présent travail est de préciser un point de la théorie des relations rationnelles entre monoïdes libres développée par Eilenberg dans le chapitre IX de son traité [1] auquel nous ferons de larges emprunts et auquel nous nous permettons de renvoyer le lecteur pour la motivation et un historique de sujet depuis les travaux fondamentaux de Elgot et Mezei [2].

On rappelle qu'étant donnés deux monoïdes libres A^* et B^* (engendrés respectivement par les alphabets finis A et B), une relation rationnelle $\rho : A^* \to B^*$ est une application de A^* dans le semi-anneau 2^{B^*} des parties de B^* dont le graphe est une partie *rationnelle* [1, chapitre VII] du produit direct $A^* \times B^*$. Ces relations forment elles-mêmes un semi-anneau si l'on définit la somme $\sigma = \rho + \rho'$ et le produit $\pi = \rho\rho'$ de deux d'entre elles par la condition que pour chaque mot a de A^* on ait:

$$a\sigma = a\rho + a\rho' \quad \text{et} \quad a\pi = \{(a'\rho)(a''\rho'):\ a', a'' \in A^*;\ a'a''\}$$

(où $(a'\rho)(a''\rho')$ désigne le produit dans le semi-anneau 2^{B^*} des parties $a'\rho$ et $a''\rho'$ de B^*). La restriction d'une relation ρ à une partie D de A^* est la relation $\rho' : A^* \to B^*$ telle que pour chaque mot a on ait $a\rho = a$ ou $= 0$ selon que $a \in D$ ou non. Quand ρ est rationnelle il en est de même de sa restriction à chaque partie *reconnaissable* D de A^* (c'est-à-dire à chaque D tel que $D\varphi\varphi^{-1} = D$ pour un morphisme φ de A^* dans un monoïde fini). Nous ne considérerons ici que les relations ρ telles que l'image $a\rho$ de chaque mot a de A^* soit une partie *finie* de B^*. Pour abréger on notera $\|X\|$ le nombre d'élément de chaque partie X de B^* et on appelera *norme* de ρ le supremum de $\|a\rho\|$ sur tous les mots a de A^*. Un rôle particulier est joué par les relations de norme un que nous appelerons *fonctionnelles* puisque ce sont des fonctions (= applications partielles) de A^* dans B^*. Notre résultat principal est la propriété ci-dessous. Dans celle-ci, $A^+ = A^*\backslash 1$ est le semi-groupe libre engendré par A et, comme d'usage, $|a|$ désigne la longueur du mot a.

Propriété. *Toute relation rationnelle $\rho : A^* \to B^*$ satisfait l'une des trois conditions suivantes:*

(i) *Il existe trois mots, $a', p, a'' \in A^*$ tels que l'on ait $\|(a'p^np'')\rho\| \geq 2^n$ pour tout $n \in \mathbf{N}$.*

(ii) *Il existe des entiers d et K tels que l'on ait $\|a\rho\| \leq K|a|^d$ pour tout mot a de A^+ et trois mots tels que $\|(a'p^na'')\rho\| \geq n+1$ $(n \in \mathbf{N})$.*

(iii) *ρ est une somme finie de relations rationnelles fonctionnelles (et a donc une norme finie).*

Nous dirons qu'une relation ρ est *cyclique* ssi son image est contenue dans un sous monoïde h^* de B^* engendré par un seul mot h. Une telle relation peut aussi être considérée comme une relation de A^* dans le semi-groupe additif des entiers. On constatera que les relations satisfaisant (ii) ou (iii) sont les polynomes (= sommes finies de produits finis) en des relations fonctionnelles et cycliques. J'ignore si toute relation cyclique est un polynome en des relations fonctionnelles. La distinction entre (i) et (ii) introduit une certaine complication et la preuve de la Propriété ne se trouvera achevée qu'à la fin de la Section 3.

Dans la Section 2 on examinera préalablement les relations fonctionnelles dont on retrouve après Nivat et Eilenberg une représentation maniable. Ces résultats sont nécessaires pour la preuve de la Propriété. Ils sont repris dans la Section 4 où l'on montre notament que quand ρ a une norme finie, on peut la représenter comme la somme d'une relation de domaine fini et de d relations fonctionnelles où $d = \min\{\|A^nA \cap \rho\|: n \in \mathbf{N}\} = \overline{\lim}_{n\to\infty}\{\|a\rho\|: |a| \geq n\}$.

(2) Dans tout ce travail nous employerons la méthode des *transducteurs* de Nivat [4]. Compte-tenu de l'hypothèse selon laquelle la relation rationnelle ρ considérée envoye chaque mot sur une partie *finie* de B^*, ceci signifie que ρ est définie par un ensemble fini Q, deux éléments distingués q_1, q_m de Q, et un morphisme de semi-groupe μ de A^* dans le monoïde $\mathbf{F}$ des $Q \times Q$ matrices ayant pour entrées des parties *finies* du semi-anneau 2^{B^*}. Pour chaque mot a de A^* on a $a\rho = a\mu(q, q_m) =$ l'entrée (q_1, q_m) de la matrice $a\mu$. Le *support* de cette dernière est la relation binaire $a\mu\#$ sur Q formée des paires (q, q') pour lesquelles l'entrée $a\mu(q, q')$ n'est pas nulle. Les théorèmes fondamentaux de la théorie des relations rationnelles permettent de supposer que le transducteur $\mu(q_1, q_m)$ de ρ est *émondé* ("Trim") en ce sens que pour chaque $q \in Q$ il existe $a, a' \in A^*$ tels que $(q_1, q) \in a\mu$ et $(q, q_m) \in a'\mu\#$. On sait en outre que quand $1\rho = 0$ et $q^1 \neq q_m$ ou quand $1\rho = 1$ et $q_1 = q_m$ le morphisme μ est un morphisme de monoïde.

Nous concluons cette introduction par l'énoncé suivant qui couvre une partie des assertions avancées dans la Propriété.

1.1. *Soit ρ une relation rationnelle telle que $a\rho$ soit fini pour tout mot a et que $1\rho = 0$. Il existe un entier K tel que l'on ait identiquement $\|a\rho\| \leq K^{|a|}(a \in A^*)$. Si ρ est cyclique cette inégalité peut être remplacée par $\|a\rho\| \leq K|a|$ $(a \in A^*)$.*

Enfin si ρ est un polynome en des relations cycliques ou fonctionnelles, il existe un entier d pour lequel $\|a\rho\| \leq K|a|^d$ $(a \in A^*)$.

Preuve. On vient de voir que ρ peut être définie par un morphisme μ de A^* dans le monoïde $\mathbf{F}$. Soit L le maximum de la longueur des mots de B^* figurant dans les entrées des matrices génératrices $a\mu$ $(a \in A)$. Pour chaque mot a de A^*, tous les mots figurant dans $a\mu$ sont de longueur au plus $|a|L$. Ceci établit la première inégalité puisque posant $m = \operatorname{card}(B)$, le monoïde B^* a exactement $(m-1)^{-1}(m^{n+1}-1)$ mots de longueur au plus n pour chaque $n \in \mathbf{N}$. Le même argument donne la seconde inégalité puisque, quand ρ est cyclique, son image est contenue dans un sous monoïde cyclique h^* de B^* qui contient au plus $n+1$ mots de longueur $\leq n|h|$.

Considérons maintenant un produit $\rho = \rho_1\rho_2 \cdots \rho_k$ où chaque ρ_i est une relation cyclique ou fonctionnelle. L'image $a\rho$ d'un mot quelconque est par définition la somme des produits $(a_1\rho_1)(a_2\rho_2)\cdots(a_k\rho_k)$ sur toutes les factorisations $a = a_1a_2\cdots a_k$ du mot a. Le nombre de celles-ci est borné par une fonction polynomiale de degré $k-1$ en $|a|$ ce qui établit la dernière inégalité. $\square$

2. Le cas fonctionnel

(1) Nous considérons un morphisme de monoïde μ de A^* dans le semi-anneau $\mathbf{F}$ qui a été défini dans l'introduction et $q, q' \in Q$ étant une paire fixe quelconque, nous établissons d'abord le fait suivant:

2.1. *On a $\|a\mu(q,q')\| \leq 1$ pour tout $a \in A^*$ ssi cette inégalité est vérifiée par tous les mots de longueur au plus $1+2m(m-1)$ où $m = \operatorname{card}(Q)$.*

Preuve. Il suffit de vérifier que si $a = a_1a_2\cdots a_n$ $(a_1, a_2, \ldots, a_n \in A)$ est un mot de longueur minimum $|a| = n$ pour lequel $\|a\mu(q,q')\| \geq 2$, l'hypothèse $n > L = 1+2m(m-1)$ conduit à une contradiction.

Comme $|a|$ est minimum, il existe au moins une suite de $n-1$ paires (q_j, q'_j) $(1 \leq j \leq n-1; q_j \neq q'_j)$ telles que posant $q_0 = q'_0 = q$, $q_n = q'_n = q'$ et $b_j = a_j\mu(q_{j-1}, q_j)$, $b'_j = a_j\mu(q'_{j-1}, q'_j)$, les produits $b = b_1b_2\cdots b_n$ et $b' = b'_1b'_2\cdots b'_n$ (qui sont des éléments de $a\mu(q,q')$) sont deux mots distincts.

Supposons $n > L$. Il existe trois indices $i < j < k$ tels que $(q_i, q'_i) = (q_j q'_j) = (q_k, q'_k)$ ce qui détermine une factorisation $a = f_1 f_2 f_3 f_4$ où $f_1 = a_1 a_2 \cdots a_i$; $f_2 = a_{i+1} \cdots a_j$; $f_3 = a_{j+1} \cdots a_k$; $f_4 = a_{k+1} \cdots a_n$. Nous définissons de même les factorisations $b = g_1 g_2 g_3 g_4$ et $b' = g'_1 g'_2 g'_3 g'_4$ en remplaçant dans les expressions ci-dessus les a_s par les b_s ou les b'_s $(1 \leq s \leq n)$. Par construction on a les trois inclusions:

$$g_1 g_4,\ g'_1 g'_4 \in (f_1 f_4)\mu(q, q'); \quad g_1 g_2 g_4,\ g'_1 g'_2 g'_4 \in (f_1 f_2 f_4)\mu(q, q');$$

$$g_1 g_3 g_4,\ q'_1 q'_3 q'_4 \in (f_1 f_3 f_4)\mu(q, q').$$

En raison du caractère minimal de a, on en déduit les équations

$$g_1 g_4 = g'_1 g'_4; \quad g_1 g_2 g_4 = g'_1 g'_2 g'_4; \quad g_1 g_3 g_4 = g'_1 g'_3 g'_4;$$

où l'on peut supposer que, par exemple, $|g_1| \leq |g'_1|$.

La première équation équivaut alors à l'existence d'un mot h tel que $g'_1 = g_1 h$ et $g_4 = h g'_4$. En reportant ceci dans les deux autres, on obtient après simplification, $h g_2 = g'_2 h$ et $h g_3 = g'_3 h$.

Par conséquent $b = g_1 g_2 g_3 g_4 = g_1 g_2 g_3 h g'_4 = g_1 g_2 h g'_3 g'_4 = g_1 h g'_2 g'_3 g'_4 = g'_1 g'_2 g'_3 g'_4 = b'$ en contradiction avec $b \neq b'$. $\square$

(2) Nous dirons qu'un morphisme μ est *fonctionnel* ssi la norme

$$\|a\mu\| = \max\{\|a\mu(q, q')\| : (q, q') \in Q \times Q\}$$

de toutes les matrices $a\mu$ $(a \in A^*)$ est au plus 1, c'est à dire ssi toutes les entrées non nulles des matrices $a\mu$ sont des mots. On voit facilement que si μ est émondé et $\rho = \mu(q_1, q_m)$ l'hypothèse que ρ est fonctionnelle entraine qu'il en soit de même de μ.

Nous nous proposons ici de déduire d'un morphisme fonctionnel μ un autre morphisme λ, qui soit aussi un transducteur pour ρ et qui possède la propriété supplémentaire que son caractère fonctionnel résulte a priori de la structure des supports $a\lambda\#$ des matrices $a\lambda$ $(a \in A^*)$ et des conditions initiales $\|a\lambda\| \leq 1$ $(a \in A)$.

C'est à quelques détails près la théorie développée par Nivat [3, Section 7]. Au moyen d'une construction plus compliquée, nous retrouvons les *bimachines* de Eilenberg [1, chapitre XI, 7] et une partie de son Théorème 7.1. Tout ceci sera utilisé pour étudier la norme d'un polynome en des relations fonctionnelles dans les Sections 2(3) et 4.

Considérons d'abord un monoïde M de $Q \times Q$ matrices sur un semi-anneau unitaire quelconque **B**. Suivant Nivat [4, Section 7] nous dirons que M est un *monoïde* $\{0, 1\}$ ssi les supports $m\#$ de ses éléments satisfont la condition (ZU): Pour chaque paire $m, m' \in M$ et chaque entrée $(q, q') \in (mm')\#$, il existe exactement un $q'' \in Q$ pour lequel $(q, q'') \in m\#$ et $(q'', q') \in m'\#$.

La condition (ZU) a pour conséquence que seule la structure multiplicative de **B** (et le fait que 0 soit un élément neutre additif) interviennent dans le calcul du produit de deux matrices de M. Il en résulte que si μ est un morphisme de A^* dans un sous monoïde $\{0,1\}$ de $\mathbf{F}$ il est fonctionnel ssi chacune des matrices génératrices $a\mu$ $(a \in A)$ a norme au plus 1.

La condition (ZU) est satisfaite en particulier par les matrices dites *monomiales* (resp. *monomiales par colonne*) caractérisées par la propriété que chaque ligne (resp. colonne) a au plus une entrée non nulle. Nous aurons besoin de la généralisation suivante de cette notion. Disons qu'une matrice m est *semi-monomiale* ssi son ensemble d'indice est un produit direct $I \times J$ et si en outre:

(i) il existe une application partielle $i \to i \cdot m$ de I dans lui-même;

(ii) pour chaque $(i,i') \in I \times I$, la $(J \times J)$-sous matrice bloc $m_{ii'} = (m(ij, i'j'))(j, j' \in J)$ est une matrice monomiale par colonne quand $i' = i \cdot m$ et nulle, sinon.

Il est clair que l'ensemble des $(I \times J) \times (I \times J)$ matrices semi-monomiales à entrées dans $\mathbf{B}$ forme un monoïde de matrices $\{0,1\}$.

Il en est de même dans le cas encore plus particulier où toutes les $J \times J$ sous matrices blocs non nulles $m_{ii'}$ de chaque matrice m ont le même support et où nous dirons alors qu'il s'agit d'un *semi-groupe de matrices de bimachines.* De façon équivalente, une $(I \times J) \times (I \times J)$ matrice m est semi-monomiale (resp. de bimachine) ssi elle appartient au produit en couronne (resp. kroneckerien) des $(J \times J)$-matrices monomiales par colonne dans les $(I \times I)$-matrices monomiales.

Pour abréger, si Ket K' sont deux parties de $I \times J$, nous désignons par $m(K, K')$ pour chaque $(I \times J) \times (I \times J)$ matrice m, la somme des entrées $m(ij, i'j')$ pour $(i,j) \in K$, $(i',j') \in K'$.

2.2. *Soit $\rho = \mu(q_1, q_m)$ une relation rationnelle fonctionnelle. Il existe un ensemble fini V, un morphisme fonctionnel λ de A^* dans le monoïde des $(V \times Q) \times (V \times Q)$ matrices semi-monomiales, un $v_1 \in V$ et une partie V_m de V tels que l'on ait identiquement $a\rho = a\lambda(v_1 q_1, V_m q_m)$.*

Preuve. En raison de l'hypothèse faite dans l'introduction que μ est émondé, le caractère fonctionnel de ρ implique que toutes les matrices $a\mu$ $(a \in A^*)$ soient de norme au plus 1.

Soient u le Q-vecteur égal à la ligne q_1 de la matrice 1μ et $v_1 = u\#$ son support. Nous désignons par V l'ensemble des supports non nuls des lignes q_1 des matrices $a\mu$ $(a \in A^*)$ (c'est à dire des vecteurs $u \cdot a\mu$) et nous introduisons une action partielle $V \times A \to V$ en définissant $v' \cdot a$ comme le support commun des vecteurs $u \cdot (a'a\mu)$ pour tous les mots a' tels que $u(a'\mu) = v' \cdot (v' \in V)$.

Nous construisons maintenant le morphisme λ en deux étapes. Tout d'abord pour chaque lettre $a \in A$, $v \in V$ et $q \in Q$ tels que $v \cdot a(q) = 0$, on peut choisir arbitrairement un q' pour lequel on a à la fois $v(q') \neq 0$ et $a\mu(q', q) \neq 0$. Ceci permet de définir la $Q \times Q$ matrice $a\mu'_v$ en posant $a\mu'_v(q'', q) = a\mu(q'', q)$ ou $= 0$

selon que $q'' = q'$ ou non. Il est clair que toutes ces matrices $a\mu'_v$ sont monomiales par colonne et de norme ≤ 1.

Ensuite nous définissons pour chaque lettre a la $(V \times Q) \times (V \times Q)$ matrice $a\lambda$ par la condition que chacun de ses (v, v') blocs $a\lambda_{v,v'}$ $(v, v' \in V)$ soit égal à $a\mu'_v$ où à 0 selon que $v' = v \cdot a$ ou non. Comme $v \to v \cdot a$ est une action partielle, les matrices $a\lambda$ sont bien semi-monomiales et de norme au plus 1.

On vérifie directement (par induction sur la longueur du mot) que pour chaque $a \in A^*$, la ligne $v_1 q_1$ de la matrice $a\lambda$ est un vecteur dont les coordonnées non nulles ont pour index les paires $(v_1 \cdot a, q)$ où $v_1 \cdot a(q) \neq 0$.

Comme le vecteur $u \cdot a\mu$ est par hypothèse un vecteur de norme au plus 1, il en résulte instantanément que la ligne $v_1 q_1$ de a est le $V \times Q$ vecteur dont chaque coordonnée (v, q) est égal à la coordonnée q du vecteur $u \cdot a$ quand $v = v_1 a$ et à 0 sinon. $\square$

(3) Venons en aux bimachines. Modifiant très légèrement la définition de Eilenberg [1, XI, 7] nous appelerons *bimachine* toute application partielle $\nu : A^* \times A^* \times A^* \to B^*$ satisfaisant les deux conditions suivantes:

(i) Pour tout $a_1, a_2, a_3, a_4 \in A^*$ on a

$$(a_1; a_2a_3; a_4)\nu = (a_1; a_2; a_3a_4)\nu \cdot (a_1a_2; a_3; a_4)\nu.$$

(ii) Il existe un morphisme ϕ de A^* dans un monoïde fini tel que pour tout $a, a_1, a_2, a_3, a_4 \in A^*$, les équations $a_1\phi = a_3\phi$ et $a_2\phi = a_4\phi$ impliquent $(a_1; a; a_2)\nu = (a_3; a; a_4)\nu$.

La *relation définie par la bimachine* ν est l'application partielle $\bar{\nu}$ envoyant chaque mot a sur $(1, a, 1)\nu$.

On vérifie facilement que, réciproquement, étant donné un morphisme ϕ de A^* dans un monoïde fini S, toute application partielle $\nu' : S \times A \times S \to B^*$ définit la restriction à A^+ d'une bimachine. En effet, l'identité (i) équivaut à la condition que pour chaque mot $a = a_1a_2 \cdots a_n$ $(n \geq 1, a_1, a_2, \ldots, a_n \in A)$ la valeur de $a\bar{\nu}$ soit le produit sur $i = 1, 2, \ldots, n$ des termes

$$((a_1 \cdots a_{i-1})\phi\ ;\ a_i\ ;\ (a_{i+1} \cdots a_n)\phi)\nu'$$

(avec la convention habituelle que pour $i = 1$ ou $i = n$, le produit vide vaut 1). La même identité détermine presque complètement les valeurs des $(a; 1; a)\nu$ qui ne peuvent être que $1 = 1_{B^*}$ ou 0. Si (comme on peut toujours le supposer) $1\phi\phi^{-1} = 1$, on peut choisir arbitrairement $1\bar{\nu} = 1$ ou $1\bar{\nu} = 0$.

Enfin nous réserverons le nom de *morphisme de la bimachine* ν aux morphismes ϕ de A^* dans un monoïde fini qui, en plus de (ii) satisfont $1\phi\phi^{-1} = 1$ et la condition que pour chaque paire de mots $a_1, a_2 \in A^*$, le domaine D' de la relation $\rho' \mapsto (a_1; a; a_2)\nu$ soit reconnaissable par ϕ (c'est à dire que $D' = D'\phi\phi^{-1}$). Comme ρ' ne dépend que de a_1 et a_2 il n'existe qu'un nombre fini de tels domaines D' et chacun d'eux est reconnaissable. Comme en outre $\{1\}$ est reconnaissable, on peut définir de façon naturelle pour tout morphisme $\phi' : A^* \to S'$ satisfaisant (ii) un morphisme $\phi = \phi' \times \psi : A^* \to S = S' \times T$ qui soit un morphisme de ν.

2.3. *Soit $\rho : A^* \to B^*$ une relation rationnelle fonctionnelle. Il existe un morphisme ϕ de A^* dans un monoïde fini S tel que ρ puisse être définie par l'un quelconque des trois objets suivants:*

(a) *un morphisme μ de A^* dans un monoïde $\{0,1\}$ de matrices tel que $\mu\# = \phi$;*

(b) *une bimachine ν dont ϕ est un morphisme;*

(c) *un morphisme π de A^* dans un monoïde de bimachine de $(S \times S) \times (S \times S)$ matrices tel que $\phi = \pi\#$.*

Preuve. Nous partons d'un morphisme μ de A^* dans un monoïde $\{0,1\}$ de $Q \times Q$ matrices de norme $\leqslant 1$ telle que l'on ait identiquement $a\rho = a\mu(q_1, q')$ pour une certaine paire $q_1 \in Q$, $q' \subset Q$. Pour abréger nous désignons par ϕ le morphisme $\mu\#$ envoyant chaque mot sur le support de la matrice $a\mu$.

Soient a, a', et a'' trois mots dont le produit $aa'a''$ est dans le domaine de ρ. En raison de la propriété (ZU) et du caractère fonctionnel de ρ il existe un et un seul triple $(q, q', q'') \subset Q \times Q \times Q'$ pour lequel les trois entrées $b = a\mu(q_1, q)$, $b' = a'\mu(q_1 q')$ et $b'' = a''\mu(q', q'')$ sont simultanément non nulles. On a alors $(aa'a'')\rho = bb'b''$. Il est clair que le mot b' ne dépend que de la matrice $a'\mu$ et des supports $s = a\phi$ et $s'' = a''\phi$ des matrices $a\mu$ et $a''\mu$. Nous pouvons donc définir une application partielle ν' de $S \times A^* \times S$ dans B^* $(S = A^*\phi)$ en posant $b = (s; a'; s'')\nu'$. Prenant $a = a'' = 1$, le calcul précédent montre que $a'\rho = (1; a', 1)\nu'$ pour tout mot a' de A^*. Prenons maintenant a et a'' quelconques et supposons $a' = a_2 a_3$ $(a_2, a_3 \in A^*)$. On vérifie l'identité

$$(a\phi\,;a_2a_3\,;a''\phi)\nu' = (a\phi\,;a_2\,;(a_3a''\phi)\nu' \cdot ((aa_2)\phi\,;a_3\,;a''\phi)\nu'$$

qui montre que $\nu = (\phi\,;\,;\phi)\nu'$ est une bimachine dont ϕ est un morphisme.

Supposons maintenant donnés ν et ϕ. Pour chaque $s, s'' \in S$, $a' \in A^*$ nous désignons par $(s; a'; s'')\nu'$ la valeur commune de $(a; a'; a'')\nu$ pour n'importe quels mots $a \in s\phi^{-1}$ et $a'' \in s''\phi^{-1}$. Nous associons à chaque mot à $1a$ $(S \times S) \times (S \times S)$ matrice $a\pi$ par la condition que pour tout $s_1, s', s_2, s_2' \in S$ on ait $a\pi(s_1, s_2\,; s_1's_2') = (s_1; a; s_2')\nu'$ ou 0 selon que la double condition $s_1' = s_1 \cdot (a\phi)$ et $s_2 = (a\phi) \cdot s_2'$ est ou non satisfaite.

On vérifie facilement que π est un morphisme de A^* dans un monoïde de matrices de bimachine (de norme $\leqslant 1$) tel que $a\rho$ soit identiquement égal à $a\pi(1, S; S, 1)$ et plus précisément à l'entrée $(1, s\,; s, 1)$ où $s = a\phi$. Le morphisme $\pi\#$ coincide avec ϕ puisque l'on peut considérer $a \to a\pi\#$ comme le produit kronekerien des représentations régulières gauches et droites de A sur $S = A^*\varphi$. Ceci achève la preuve puisque tout monoïde de bimachine est un monoïde (ZU). $\square$

On en déduit:

Théorème (Eilenberg). *Toute relation rationnelle fonctionnelle peut être réalisée par une bimachine.*

Preuve. Ceci découle immédiatement de 2.2 et de l'énoncé précédent. □

(4) Nous terminons cette section en considérant les produits de relations fonctionnelles.

2.4. *Soit $\pi : A^* \to B^*$ un produit de relations rationnelles fonctionnelles qui n'est pas une somme finie de relations rationnelles fonctionnelles. Il existe trois mots $a', p, a'' \in A^*$ tels que $\|(a'p^n a'')\pi\| \geqslant n+1$ pour tout entier positif n.*

Preuve. Par induction sur le nombre de facteurs de produit, il suffit de considérer le cas de $\pi = \bar{\mu} \cdot \bar{\nu}$ où $\bar{\mu}$ et $\bar{\nu}$ sont les relations fonctionnelles définies respectivement par les bimachines μ et ν. Nous pouvons construire un morphisme ϕ de A^* dans un monoïde fini S qui est simultanément un morphisme de μ et de ν. Soit $s \in S$ quelconque. Nous engendrons une bimachine μ_s en posant pour chaque $a \in A$ et $a_1, a_2 \in A^*$,

$$(a_1, a, a_2)\mu_s = 0 \quad \text{si } (a_1 a)\phi \neq s \quad \text{et} \quad (a_1, a_2, a_2)\mu \text{ sinon.}$$

Par définition, le domaine de la relation $\bar{\mu}_s$ est contenu dans $s\phi^{-1}$ et $\bar{\mu}_s$ est égale à $\bar{\mu}$ sur son domaine. La même construction s'applique à ν et nous avons donc que π est égale à la somme finie des produits de relation $\bar{\mu}_s \bar{\nu}_s$, $(s, s' \in S)$. Nous pouvons donc supposer pour simplifier que $\mu = \mu_s$ et $\nu = \nu_t$ pour une certaine paire $s, t \in S \backslash 1$.

Si chacun des mots du domaine de $\pi = \mu\nu$ admet exactement une factorisation comme produit d'un mot de $s\phi^{-1}$ par un mot de $t\phi^{-1}$, le résultat est établi puisqu'alors π est fonctionnelle. Dans le cas contraire, soit a un mot du domaine de π ne satisfaisant pas les conditions d'unicité ci-dessus. Il admet une factorisation maximale unique $a = a' p_1 p_2 \cdots p_n a''$ $(p, \cdots, p_n \in A^+, n \geq 1)$ telle que l'on ait identiquement $a' p_1 \cdots p_i \in s\phi^{-1}$; $p_{i+1} \cdots p_n a'' \in t\phi^{-1}$ $(0 \leqslant i \leqslant n)$.

Son image par π est constituée par les $n+1$ mots $b' q_1 \cdots q_i r_{i+1} \cdots r_n b''$ où pour abréger on a posé $b' = (1; a'; a'')\mu$; $b'' = (a'; a''; 1)\nu$; $q_i = (a'; p_i; a'')\mu$; $r_i = (a'; p_i; 1)\nu$ $(1 \leqslant i \leqslant n)$.

Désignons par P^* le sous monoïde de A^* formé des mots p tels que $s \cdot p\phi = s$ et $p\phi \cdot t = t$. C'est une partie reconnaissable de A^* et nous pouvons tester si les relations rationnelles fonctionnelles $\bar{\mu}' : p \mapsto (a'; p; a'')\mu$ et $\bar{\nu} : p \mapsto (a'; p; a'')\nu$ sont ou non égales sur P^*.

Dans le premier cas on a évidemment $q_i = r_i$ $(1 \leqslant i \leqslant n)$ et par conséquent π est fonctionnelle. Dans le second cas soit $p \in P^*$ tel que $q = p\bar{\mu}' \neq p\bar{\nu}'$. L'image par π du mot $a' p^n a''$ est formée des $n+1$ mots $b' q^m i^{n-m} b''$ $(0 \leqslant m \leqslant n)$ que l'on vérifie immédiatement être distincts puisque toute égalité entre deux d'entre eux entrainerait une équation de la forme $q^k = r^k$ $(k \geq 1)$ en contradiction avec $q \neq r$. □

3. Le cas général

Nous continuons à faire tacitement l'hypothèse que chaque relation considérée donne une image *finie* à chaque mot de son domaine.

(1) Une relation $\rho : A^* \to B^*$ sera dite *minimale* ssi son domaine est $\{1\}$ ou une lettre de A. Elle sera dite *unitaire* ssi elle peut être mise sous la forme $\rho = \mu(q, q)$ où μ est un morphisme de monoïde de A^* dans un semi-anneau de $Q \times Q$ matrices et q un élément quelconque de Q.

Il est clair que chaque relation unitaire ρ satisfait $1\rho = 1$ et est sous-multiplicative en ce sens que $(a\rho)(a'\rho) \subset (aa')\rho$ pour tout $a, a' \in A^*$. Son domaine est donc un sous monoïde P^* de A^* (engendré par un ensemble minimal $P \subset A^+$, qui est vide ssi ρ est *triviale*). On rappelle qu'un morphisme μ de A^* dans un anneau de $Q \times Q$ matrices est *irréductible* ssi $Q \times Q$ est l'union sur tous les mots a des supports des matrices $a\mu$. Par conséquent si $\rho = \mu(q, q)$ où μ est émondé au sens donné à ce terme dans l'introduction, le morphisme μ est irréductible, puisque pour tout $q' \in Q$ il doit exister $a, a' \in A^*$ tels que $(q, q') \in a\mu\#$ et $(q', q) \in a'\mu\#$.

Un produit $\rho = \rho_1\rho_2 \cdots \rho_k$ de relations est *non ambigu* ssi tout mot a de son domaine admet exactement une factorisation $a = a_1a_2 \cdots a_k$ où chaque a_i est dans le domaine de ρ_i. Plus généralement, un polynome $\rho = \rho'_1 + \rho'_2 + \cdots \rho'_{k'}$ est *non ambigu* ssi tous les produits ρ'_j sont non ambigus et ont des domaines deux à deux disjoints.

3.1. *Soit $\rho = \mu(q_1, q_m)$ une relation rationnelle. Il existe un algorithme ne dépendant que du morphisme $\mu\#$ dans le monoïde des relations binaires sur Q qui permet d'exprimer ρ comme un polynome en des relations rationnelles minimales ou unitaires. Quand μ est un morphisme dans un monoïde* $\{0, 1\}$, *le polynome obtenu est non ambigu.*

Preuve. Nous pouvons supposer que μ est un morphisme de monoïde dans le semi-anneau $\mathbf{F}$ (de $Q \times Q$ matrices) et que $q_1 \neq q_m$. Soit ρ_1 la relation rationnelle unitaire $\mu(q_1, q_1)$.

Nous considérons d'abord le cas ù ρ_1 est triviale (en ce sens que son domaine est $\{1\}$). Ceci équivaut à l'hypothèse que toutes les colonnes q_1 des matrices $a\mu$ $(a \in A^+)$ sont nulles.

Soit $Q' = Q \backslash q_1$. Pour chaque $q \in Q'$, $a \in A$ nous posons $\rho'_q = \mu(q, q_m)$ et $\rho_{a,q}$ = la relation de domaine $\{a\}$ égale à $a\mu(q_1, q)$ sur celui-ci. La relation ρ est la somme sur tous les $q \in Q'$, $a \in A$ des produits non ambigus $\rho_{a,q}\rho'_q$ et chaque $\rho_{a,q}$ est une somme de relations minimales. Soit maintenant μ' la restriction de μ à $Q'\times Q'$, c'est à dire soit $a\mu'(q,q')=a\mu(q,q')$ pour chaque $a\in A^*, q,q'\in Q'$. En raison de l'hypothèse faite sur μ c'est un morphisme de A^* dans un semi-anneau de $Q'\times Q'$ matrice et l'on a $\rho'_q=\mu'(q,q_m)$ pour chacun des q de Q'.

Ceci conclut la preuve par induction sur card(Q) dans ce cas. En effet, quand μ est un morphisme dans un monoïde $\{0,1\}$ il en est encore de même de μ', chaque $\rho_{a,q}$ est minimale et la condition (ZU) montre que les produits $\rho_{a,q}\rho'_q$ ont des domaines disjoints.

Supposons maintenant que ρ_1 n'est pas triviale et définissons un morphisme μ'' de A^* dans F par sa restriction à A en remplaçant par 0 toutes les entrées de la colonne q_1 de chaque matrice $a\mu$ $(a\in A)$. La relation rationnelle $\rho''=\mu''(q_1,q_m)$ satisfait les hypothèses du premier cas traité et il nous suffit donc de montrer que l'on a $\rho=\rho_1\rho''$ où le produit est non ambigu quand ρ est fonctionnelle puisque $A^*\mu''$ et un monoïde $\{0,1\}$ quand μ a la même propriété.

Soit donc $a=a_1\cdots a_n$ $(n\geq 1, a_1,a_2,\ldots,a_n\in A)$ un mot du domaine de ρ. L'entrée $a\mu(a_1,q_m)$ est la somme du produit des entrées $a_i(q'_i,q'_{i+1})$ $(1\leq i\leq n)$ sur toutes les suites $(q'_1=q_1,q'_2,\ldots,q'_{n+1}=q_m)$ de $n+1$ états q'_j pour lesquelles ces entrées sont toutes non nulles. Pour chaque telle suite il existe un plus grand indice j $(1\leq j\leq n)$ tel que $q'_j=q_1$. Le produit correspondant est contenu dans le produit des deux entrées $(a_i\cdots a_j)\mu(q_i,q_i)$ et $(a_{j+1}\cdots a_n)\mu''(q_1,q_m)$. Donc $\rho_1\rho''\subset\rho$, d'où l'égalité cherchée puisque réciproquement toute relation $a'\rho_1\neq 0$, $a''\rho''\neq 0$ implique $(a'a'')\rho\neq 0$. Dans le cas fonctionnel, $a(q_1,q_m)$ est de façon unique un produit d'entrées non nulles et la factorisation $\rho=\rho_1\rho'$ est donc non ambigue. □

On notera que la construction précédente de la suite $(q'_1,\ldots,q'_{n+1})$ montre que quand ρ est fonctionnelle le domaine P^* de ρ_1 est engendré librement par l'ensemble générateur minimal P de P^*.

(2) Nous aurons besoin en outre de quelques résultats propres au semi-anneau 2^{B^*}. Nous les extrayons sans démonstration du livre de Lentin [2].

Pour chaque mot $b\in B^*$ soit $\sqrt{b}$ le plus court mot $h\in B^*$ tel que b soit contenu dans le monoïde cyclique $h^*=\Sigma_{0\leq n}h^n$. On a évidement $h=\sqrt{h}$, c'est à dire que h est un mot *primitif*. Plus généralement, nous dirons qu'une partie P de B^* est *cyclique* ssi il existe un mot h (que l'on peut supposer primitif et noter $\sqrt{P}$) tel que $P\subset h^*$. Donc toute partie P' d'une partie cyclique P est aussi cyclique et $\sqrt{P}=\sqrt{P'}$ sauf si $P'\backslash 1=\emptyset$.

Soit $P=\{b,c\}$ où $b,c\neq 1$. On sait que les assertions suivantes sont équivalentes:

(a) P n'est pas cyclique;

(b) $\sqrt{b}\neq\sqrt{c}$;

(c) $b^*\cap c^*=\{1\}$;

(d) P^* est isomorphe au monoïde libre à *deux* générateurs.

Nous utiliserons plus loin la remarque suivante:

3.2. *Soient $b \in B^+$ et P une partie cyclique de B^* qui n'est pas un singolet. Les parties $b + P$ et bP sont simultanément cycliques ou non.*

Preuve. Il est clair que $b + P$ est cyclique ssi $\sqrt{b} = \sqrt{P}$ et que ceci entraine que $\sqrt{bP} = \sqrt{P}$. Réciproquement, supposons que bP soit cyclique. Comme P n'est pas un singolet, P contient h^r et h^s où $h = \sqrt{P}$, $0 \leq r \leq s$, et bP contient les mots $bh^r = g^{r'}$, $bh^s = g^{s'}$ où $g = \sqrt{bP}$. On a $r' < s'$. Par conséquent $h^{s-r} = g^{s'-r'}$ ce qui entraine $h = g$ puisque ces deux mots sont primitifs et, enfin, $b = h^{r'-r}$. $\square$

(3) Pour alléger l'écriture nous supposons ici que $Q = \{1, 2, \ldots, m\}$. Un morphisme μ de A^* dans F sera dit de *type cyclique* ssi il est possible de réindexer les éléments de Q de telle sorte que la matrice $A^*\mu$ (somme des matrices $a\mu$ pour $a \in A^*$) soit contenue dans une $Q \times Q$ matrice H satisfaisant les conditions suivantes:

Il existe m mots $b_j \in B^*$ tels que, posant $h_j = b_j b_{j+1} \cdots b_m b_1 \cdots b_{j-1}$ $(1 \leq j \leq m)$, on ait pour tout i, j, $H(i, i) = h_i^*$, et pour $i \neq j$, $H(i, j) = h_i^* H'(i, j)$ avec $H'(i, j) = b_i b_{i+1} \cdots b_{j-1}$ si $i < j$ ou si $i < j$ et $h_i = h_j$ et $H'(i, j) = b_i b_{i+1} \cdots b_m b_1 \cdots b_{j-1}$ sinon.

On vérifie directement que $H(i, j) = H'(i, j) h_j^*$ et que par conséquent $HH = H$.

Soit maintenant μ un morphisme irréductible au sens donné à ce terme à la fin de 3.1. Nous posons $A\mu = \Sigma\{a\mu = a \in A\}$, $A^*\mu = \Sigma\{a\mu : a \in A^*\}$, $\bar{M} = A\mu + A^2\mu + \cdots + A^{2m-1}\mu$ et $P = \bar{M}(1, 1)$. Il est clair que P est une partie cyclique de B^* quand μ est de type cyclique.

Réciproquement:

3.3. *Une condition suffisante pour que le morphisme irréducible μ soit de type cyclique est que P soit une partie cyclique de B^*.*

Preuve. L'énoncé est trivial si aucune des entrées de $A\mu$, (donc de $A^*\mu$) ne rencontre B^+ car il suffit de prendre alors tous les b_j égaux à 1 dans la définition de H. Nous supposons donc ce cas écarté.

Soient q et q' deux états *distincts* de Q. Comme μ est irréductible, la paire (q, q') est dans le support de la matrice $A^*\mu$, ce qui signifie qu'il existe une suite $(q'_1 = q, q'_2, \ldots, q'_n = q')$ et n lettres $a_i \in A$ tels que les entrées $a_i\mu\,(q'_i, q'_{i+1})$ $(1 \leq i \leq n-1)$ sont non nulles. On peut choisir les q'_i distincts et, puisque $m = \mathrm{Card}(Q)$, ceci montre que la matrice $M' = A\mu + A^2\mu + \cdots + A^{m-1}\mu$ a toutes ses entrées non diagonales non nulles. Comme au moins une des entrées de $A\mu$ rencontre B^+ il en résulte que la même chose est vraie de l'entrée $(1, 1)$ de $\bar{M} = M'(A\mu)M'$ et que le mot $h = \sqrt{P}$ appartient à B^+.

Considérons un état $q \neq 1$. On a l'inclusion $M'(1, q) \cdot M'(q, 1) \subset \bar{M}(1, 1) \subset h^*$.

Si $M'(1, q)$ n'est pas contenue dans h^*, ceci implique l'existence d'une factorisation bien définie $h = g'_q g''_q$ pour laquelle $M'(1, q) \subset h^* g'_q$ et $M'(q, 1) \subset g''_q h^*$. Dans le cas contraire, on doit avoir aussi $M'(q, 1) \subset h^*$ et nous posons $g'_q = g''_q = 1$.

Nous choisissons maintenant un indexage de Q tel que la suite des longueurs des mots g'_q soit non décroissante. Les $m-1$ équations $g'_q g''_q = h$ (ou $=1$) déterminent sans ambiguité m mots b_j tels que $g'_j = b_1 \cdots b_{j-1}$ $(2 \leq j \leq m)$. Maintenant pour chaque $(i, j)(i, j \neq 1)$ on a l'inclusion:

$$M'(1, i) \cdot A\mu(i, j) \cdot M'(j, 1) \subset \bar{M}(1, 1) \subset h^*$$

où $M'(1, i)$ et $M'(j, 1)$ sont des parties non vides de $h^* g'_i$ et de $g''_j h^*$ respectivement. Exprimant ceci en fonction des mots b_h, on obtient la relation $A(i, j) \subset H(i, j)$ d'où le résultat puisque $HH = H$. □

3.4. *Soit $\mu : A^* \to \mathbf{F}$ un morphisme irréductible qui n'est pas fonctionnel. Il existe trois mots p, a', a'' tels que l'on ait $\|(a'p^n a'')\mu\| \geq \alpha(n)$ $(n \in \mathbf{N})$ avec $\alpha(n) = n+1$ ou $= 2^n$ selon que μ est ou non de type cyclique.*

Preuve. L'hypothèse que μ n'est pas fonctionnelle implique l'existence d'un mot p et d'états q, q' tels que $P = p\mu(q, q')$ contienne au moins deux mots distincts b et c. D'autre part quelques soient q_1 et q'_1 l'hypothèse que μ est irréductible implique l'existence de mots a' et a'' tels $a'\mu(q_1, q)$ et $a''\mu(q', q'_1)$ ne soient pas nuls et que par conséquent $\|(a'pa'')\mu(q_1, q'_1)\| \geq \|P\|$.

Il suffit donc de considérer une seule paire (q, q') et on peut même supposer que $q = q'$ ce que nous ferons désormais.

Pour chaque entier n on a $\{b, c\}^n \subset P^n \subset P^n\mu(q, q)$. Ceci établit l'inégalité cherchée quand P n'est pas cyclique puisque l'on peut alors prendre $b, c \in P$ tels que $\{b, c\}^*$ soit isomorphe au monoïde libre à deux générateurs, c'est à dire que $\|\{b, c\}^n\| = 2^n$ identiquement.

Si P est cyclique mais que μ ne l'est pas, nous pouvons trouver deux mots a_1 et a_2 tels que $\{d_1 = a_1\mu(q, q),\ d_2 = a_2\mu(q, q)\}$ ne soit pas cyclique. On a $d_iP \subset (a_ip)\mu(q, q)$, $i = 1, 2$, et d'après 3.2, l'un au moins de ces deux ensembles n'est pas cyclique. Ceci achève la preuve quand μ n'est pas cyclique.

Supposons maintenant P cyclique c'est à dire $b = h^r$, $c = h^s$ $(r, s \in \mathbf{N})$ où $h = \sqrt{P}$. Pour chaque $n \in \mathbf{N}$, P^n contient les $n+1$ mots distincts h^{n_i} où $n_i = ir + (n-i)s$ $(0 \leq i \leq n)$ concluant la preuve. □

Ceci achève d'établir la Propriété énoncée dans l'introduction. En effet, soit $\rho : A^* \to B^*$ une relation rationnelle. S'il existe un mot de A^* dont l'image par ρ est infinie, l'eventualité (i) est réalisée (avec $p = 1$). Sinon (comme nous le supposons désormais) nous savons d'après 1.1 que ρ est un polynome en des relations fonctionnelles ou unitaires et nous distinguons deux cas selon que ces dernières sont toutes fonctionnelles ou que l'une au moins ne l'est pas.

Compte tenu de 1.2, l'énoncé 2.4 (resp. 3.4) montre alors que dans le premier (resp. second) cas l'une des éventualités (i) ou (ii) ou (iii) est réalisée.

Nous terminons la discussion dans la section suivante, en utilisant le résultat (qui vient d'être établi) qu'une relation rationnelle a une nomme finie ssi elle est la somme d'un nombre fini de relations rationnelles fonctionnelles.

4. Les relations de norme finie

(1) Faisant référence à la terminologie introduite au début de la Section 3, nous considerons une relation rationnelle fonctionnelle ρ de domaine infini qui est un produit non ambigu de relations minimales ou unitaires. Regroupant les termes et omettant ceux qui sont triviaux, on en déduit de façon unique une expression de ρ comme un produit non ambigu $p = \tau_0\sigma_1 \cdots \tau_{k-1}\sigma_k\tau_k$ $(k \geqslant 1)$ où chaque τ_i est une relation dont le domaine est un mot $y_i \in A^*$ et chaque σ_i une relation fonctionnelle unitaire dont le domaine est le sous-monoïde X_i^* engendré librement par la partie non vide X_i de A^+.

Nous appelerons $(X) = (y_0, X_1, y_1, \ldots, X_k, y_k)$ $(k \geqslant 1)$ un *monome*. Son *domaine* sera la partie infinie $y_0X_1^*y_i \cdots x_k^*y_k = x$ de A^* et nous dirons que la relation ρ est *compatible* avec (X). La suite $(\sigma) = (\tau_0, \sigma_1, \ldots, \sigma_k, \tau_k)$ sera dite *induite* par (X) sur ρ.

Nous montrons d'abord que l'ensemble Σ des suites induites par (X) sur ρ contient un élément distingué σ.

4.1. *La condition que la séquence* $(|y_0\tau_0|, |y_1\tau_1|, \ldots, |y_{k-1}\tau_{k-1}|)$ *soit minimale pour l'ordre léxicographique caractérise de façon unique une suite* σ *de* Σ. *Celle-ci jouit de la propriété que pour* $i = 0, 1, \ldots, h-1$ *les mots* $y_i\tau_i$ *et* $x\sigma_{i+1}$ $(x \in X_{i+1})$ *de* B^+ *n'ont pas de facteur droit commun non trivial.*

Preuve. Soient (σ) et (σ') deux suites de Σ, (σ) étant choisie de telle sorte que $t = y_0\tau_0$ soit de longueur minimale. Quelque soit le mot x de X_1 on a identiquement: $(y_0x^hy_1 \cdots y_h)\rho = ts^hu = t's'^hu'$ $(n \in \mathbf{N})$ où $s = x\sigma_1$, $u' = (y_1\tau_1)\cdots(y_h\tau_h)$; $t' = y_0\tau_0'$; $s' = x\sigma_1'$, $u' = (y_1\tau_1')\cdots(y_k\tau_k')$. Considérant ces équations pour $n = 0$ et pour $n = 1$ on obtient $tu = t'u'$ et $|s| = |s'|$.

Par conséquant t (donc t et s) est déterminé de façon unique par la condition que t soit le facteur gauche commun de tous les mots de la forme $y_0\tau_0''$ $(\sigma'' \in \Sigma)$.

Ceci entraine qu'il n'existe pas de lettre b de B qui soit facteur gauche commun des mots t et $x\sigma_1$ $(x \in X_1)$. En effet, si tel était le cas, on pourrait remplacer t par tb^{-1}, $y_1\tau_1$ par $b(y_1\tau_1)$ et chaque $x\sigma_1 \in B^+$ par $b((x\sigma_1)b^{-1})$, en contradiction avec le caractère minimal de $|t|$.

Le résultat est établi pour $k = 1$. Si $k \geqslant 2$, on le vérifie par induction sur k en considérant le monome $(y_1, X_1, y_2, \ldots, X_k, y_k)$ et la relation définie par la suite induite $(\tau_1, \sigma_1, \ldots, \tau_k)$. $\square$

Ceci nous permettra une économie de notations puisque, pour tout segment $X_i^*y_i \cdots X_j^*$ (ou $y_{i-1}^*X_i^*y_i \cdots X_j^*$ ou $X_i^*y_i \cdots X_j^*y_j$ etc.) du domaine X et tout mot

x de celui-ci nous pourrons sans ambiguité désigner par $x\rho$ le produit correspondant des images de ses facteurs par les relations de la suite distinguée (σ) que l'on vient de définir.

(2) Nous vérifions d'abord un résultat technique.

4.2. *Soit $\rho = \rho_1 + \rho_2 + \cdots + \rho_d$ une somme finie de relations rationnelles fonctionnelles ρ_i. Il existe une relation ρ_0 de domaine fini et un système fini de monomes disjoints $(X^{(j)})$ et de relations rationnelles ρ_{ji} telles que chaque paire $(X^{(j)}, \rho_{ji})$ soit compatible et que ρ soit la somme de ρ_0 et des ρ_{ji}.*

Preuve. Chacune des relations initiales ρ_i peut être définie par une bimachine ν_i. Celles-ci étant en nombre fini, on peut choisir un morphisme ϕ de A^* dans un monoïde fini S qui en soit simultanément un morphisme. Donc pour tout ρ_i et $s \in S$ la partie $s\phi^{-1}$ est contenue dans le domaine de ρ_i ou dans son complément.

On définit maintenant la relation ρ_0 comme la restriction de ρ à l'union D de celles des parties $s\phi^{-1}$ $(s \in S)$ qui sont finies. Remplaçant ρ par sa restriction au complément de D, on peut désormais supposer $\rho_0 = 0$ et même, pour simplifier, que toutes les relations ρ_i ont le même domaine $s\phi^{-1}$ pour un certain $s \in S$.

D'après 2.3 et ses corollaires, on peut trouver des morphismes μ_i dans des monoïdes $\{0,1\}$ de $Q \times Q$ matrices $(Q = S \times S)$ qui définissent les ρ_i et satisfont identiquement $\mu_i \# = \phi$.

Appliquons maintenant la construction de 3.1 à l'une quelconque des relations ρ_i. Elle permet d'exprimer cette relation come une somme finie de produits ρ_{j1} $(j = 1, 2, \ldots, k)$ de relations et chacun de ceux-ci donne de façon unique une paire compatible $(X^{(j)}, \rho_{j1})$. Par construction les domaines des monomes $(X^{(j)})$ sont deux à deux disjoints. En vertu des égalités $\phi = \mu_i \#$, les mêmes monomes $(X^{(j)})$ auraient été obtenus si cette construction avait été effectuée à partir de l'une quelconque des autres relations ρ_i. □

Nous considérons désormais un monome fixe (X) avec lequel toutes les relations considérées seront supposées compatibles. Puisque chaque segment X_i^* de (X) est engendré librement par X_i, le monoïde $M = X_1^* \times X_2^* \cdots \times X_k^*$ est isomorphe à un produit direct de monoïdes libres. Il existe donc une bijection η de M sur le domaine X de (X) envoyant chaque $m = (x_1, \ldots, x_h)$ sur $y_0 x_1 y_1 \cdots x_h y_k$. En particulier $1\eta = y_0 y_1 \cdots y_k$.

Enfin pour chaque relation fonctionnelle ρ compatible avec (X) nous désignons par $\hat{\rho}$ le morphisme de M dans $\mathbf{N}$ tel que $m\hat{\rho} = |m\eta\rho| - |1\eta\rho| = |x_1\rho| + |x_2\rho| + \cdots + |x_k\rho|$ pour chaque $m = (x_1, \ldots, h_k) \in M$. On a donc identiquement

$$|(m^n w m'^{n'})\eta\rho| = |w\eta\rho| + (n + n') \cdot m\hat{\rho}$$

pour tout $m, w, m' \in M$ et $n, n' \in \mathbf{N}$.

L'énoncé 2.1 permet de tester si deux relations rationnelles fonctionnelles ρ et ρ' sont telles que $\hat{\rho} = \hat{\rho}'$ c'est-à-dire telles que $|x\rho| = |x\rho'|$ pour tout mot x appartenant à l'union des X_i. En effet il suffit pour cela de prendre un morphisme β de B^* envoyant l'alphabet B sur une lettre unique et de vérifier pour $l = 1, 2, \ldots, k$ l'égalité sur X_l^* des relations induites sur $\rho\beta$ et $\rho'\beta$.

4.3. *Soient ρ et ρ' deux relations fonctionnelles distinctes compatibles avec le monome (X) et satisfaisant $\hat{\rho} = \hat{\rho}'$. Il existe un idéal non vide W de M tel que $w\mu\rho \neq w\mu\rho'$ pour chacun de ses éléments w.*

Preuve. Soit $\delta = |1\eta\rho| - |1\eta\rho'|$. Si $\delta \neq 0$ on a $|m\eta\rho| - |m\eta\rho'| = \delta \neq 0$ pour chaque m de M en raison de $\hat{\rho} = \hat{\rho}'$ et on peut donc prendre $W = M$. Soient $b = y_0\rho$ et $b' = y_0\rho'$. Si l'un de ces deux mots n'est pas facteur gauche de l'autre, les idéaux à droite bB^* et $b'B^*$ sont disjoints. Il en est donc de même de $X\rho$ et de $X\rho'$ et on peut encore prendre $W = M$.

Nous supposons donc désormais ces deux cas écartés, c'est-à-dire $\delta = 0$ et par exemple, en simplifiant à gauche, $b' = y_0\rho' = 1$.

Soit V l'ensemble des mots v de X_1^* pour lesquels $|v\rho| \geqslant |b|$. On définit quatre relations α', β, β' et γ de domaine V par les équations suivantes pour chaque v de V: $v\rho = (v\beta)(v\gamma)$; $v\rho' = (v\alpha')(v\beta')$; $|v\gamma| = |v\alpha| = |b|$, $(b = y_0\rho)$. Autrement dit $v\gamma$ et $v\gamma'$ sont respectivement le facteur droit et le facteur gauche de longueur $|b|$ de $v\rho$ et de $v\rho'$ et $v\beta = (v\rho)(v\gamma)^{-1}$ et $v\beta' = (v\alpha')^{-1}(v\rho')^{-1}$ sont les cofacteurs associés. Donc $|v\gamma| = |v\alpha'|$ et comme V est un idéal non vide X_1 on a identiquement $(xv)\beta = x\rho \cdot v\beta$; $(vx)\beta' = v\beta' \cdot x\rho'$ pour chaque $v \in V$, $x \in X_1^*$.

On vérifie facilement que V est une partie reconnaissable et que les relations α', β, β', γ sont rationnelles en même temps que ρ et ρ'. Ceci permet de tester si l'ensemble V' des mots v de V pour lesquels $v\beta \neq v\beta'$ est vide ou non.

Supposons maintenant $v \in V' \neq \emptyset$. Quelque soit le mot x de X_1^*, l'égalité de longueur des mots $x\rho$ et $x\rho'$ entraîne celle des mots $b(x\rho)(v\beta)$ et $(x\rho'')(v\rho') = (x\rho')(v\alpha')(v\beta')$.

Comme $v\beta \neq v\beta'$ ces deux mots engendrent des idéaux à droite dans B^* disjoints. Par conséquent $w\mu\rho \neq w\mu\rho'$ pour tout $w \in M$ appartenant à l'idéal (bilatère) de ce monoïde engendré par $v\eta^{-1} = (v, 1, \ldots, 1)$. Le résultat est donc établi dans ce cas et nous pouvons désormais supposer que V' est vide, c'est-à-dire que $\beta = \beta'$.

Prenant deux mots quelconques u et v dans V, le calcul:

$$u\beta \cdot u\gamma \cdot v\beta = u\rho \cdot v\beta = (uv)\beta = (uv)\beta' = u\beta' \cdot v\rho' = u\beta' \cdot v\alpha' \cdot v\beta'$$

établit l'existence d'un mot c de longueur $|b|$ tel que l'on ait identiquement $u\gamma = v\alpha' = c$, c'est-à-dire $v\rho = v\beta \cdot c$; $v\rho' = c \cdot v\beta$ pour chaque $v \in V$. Si $c \neq b$ on a évidemment $m\eta\rho \neq m\eta\rho'$ pour chaque $m \in M$. Il ne reste donc à considérer que le cas ou $c = b$.

Comme $V = VX_1^*$, les relations $b = y_0\rho$ et $v = v\beta \cdot b$ ($v \in V$) montrent que si b était différent de 1, les mots $y_0\rho$ et $x\rho$ ($x \in X_1$) auraient un facteur droit commun non trivial en contradiction avec les conventions adoptées à la fin de 4.1. Par conséquent $b = 1$ et β est la valeur commune des restrictions à V de ρ et de ρ'. Comme $V^* = V^*X_1^*$ on en conclut que de fait ρ et ρ' ont même restriction à X_1.

Il est clair que seul ce dernier cas est à considérer pour achever la preuve. Si $k = 1$ l'hypothèse $\rho \neq \rho'$ implique $y_1\rho \neq y_1\rho'$ ce qui entraîne que $X\rho$ et $X\rho'$ soient disjoints. Si $k \geq 2$ le résultat énoncé découle de la même manière des remarques précédentes par induction sur k en considérant les restrictions à $(y_1, X_2, \ldots, y_k)$ de ρ et de ρ'. $\square$

Gardant le même monome (X) nous considérons enfin un ensemble R de $d < \infty$ relations rationnelles fonctionnelles compatibles avec lui et la somme σ de ces dernières.

4.4. *Le monoïde M contient un sous semi-groupe non vide S' tel que* $\| s\eta\sigma \| = d$ *pour chacun de ses éléments s.*

Preuve. Comme la famille des idéaux non vides de M contient l'intersection de deux de ses membres, l'énoncé précédent permet de trouver un idéal $W \neq \emptyset$ tel que pour chacun de ses éléments w et $\rho, \rho' \in R$ on ait $w\eta\rho = w\eta\rho'$ seulement si $\rho = \rho'$ ou $\hat{\rho} \neq \hat{\rho}'$.

Soit d'autre part $R' = \{\rho_1, \ldots, \rho_p\}$ une partie maximale de R telle que $\hat{\rho}_i \neq \hat{\rho}_j$ pour deux quelconques de ses éléments distincts. Comme chaque $\hat{\rho}$ est un morphisme de M dans $\mathbf{N}$ on peut trouver un élément m de M et un indexage de R' tels que $m\hat{\rho} < m\hat{\rho}_2 \cdots < m\hat{\rho}_p$.

Ces inégalités restent vérifiées par n'importe quelle puissance de m et, prenant un w dans W quelconque on peut trouver une puissance m^n de m telle qu'en posant $s' = wm^n$ on ait $|s\eta\rho_1| < |s\eta\rho_2| \cdots < |s\eta\rho_p|$ pour chaque élément s du sous semi-groupe S de M engendré par s' ce qui établit le résultat puisque S est contenu dans l'idéal W de M. $\square$

Nous avons terminé la preuve des propriétés énoncées dans l'introduction.

En effet si la relation rationnelle ρ n'admet aucun triple de mots a', p, a'' pour lequel $\|(a'p^na'')\rho\| \geq n + 1$ identiquement, la première partie de la preuve montre quelle est la somme d'un nombre fini de relations rationnelles fonctionnelles. D'après 4.2 nous pouvons la représenter comme la somme d'une relation ρ_0 de domaine fini et de relations fonctionnelles ρ_{ji} dont les domaines sont ceux de monomes disjoints $(X^{(j)})$. Sur chacun de ceux-ci, le dernier énoncé montre que la norme de ρ est la même que celle de la restriction de ρ à tous les mots de longueur supérieure à une valeur finie arbitraire. Si donc d est le maximum de la norme de $X^{(j)} \cap \rho$ sur tous les domaines $(X^{(j)})$ on peut regrouper ceux-ci et exprimer ρ comme somme de ρ_0 et d'exactement d relations fonctionnelles.

On notera que les constructions effectuées permettraient de vérifier si une relation rationnelle ρ' de norme finie satisfait ou non $a\rho \subset a\rho'$ pour tous les mots assez longs. Il serait curieux que ceci ne reste pas vrai pour des relations rationnelles ρ et ρ' satisfaisant seulement la condition (ii) de la Propriété.

Références

[1] S. Eilenberg, *Automata, Languages and Machines*, Vol. A (Academic Press, New York, 1974).

[2] C. Elgot and G. Mezei, On operations defined by generalised automata, *IBM J. Res. Dev.* **9** (1965) 47–68.

[3] A. Lentin, *Equations dans les monoïdes libres* (Gauthier Villars, Paris, 1972).

[4] M. Nivat, Transductions des languages de Chomsky, *Ann. Institut Fourier* **18** (1968) 335–455.