Theoretical Computer Science 5 (1977) 325–337.

UNE CARACTERISATION DES FONCTIONS SEQUENTIELLES ET DES FONCTIONS SOUS-SEQUENTIELLES EN TANT QUE RELATIONS RATIONNELLES

Christian CHOFFRUT

Département de Mathématiques, Université Paris VII, 75221 Paris, Cedex 05, France

Communicated by M. Nivat
Received February 1977
Revised July 1977

1. Introduction

La notion de relation rationnelle constitue à l'heure actuelle un concept fondamental de la théorie des langages formels. Elle n'est cependant pas apparue immédiatement dans toute sa généralité. En fait, elle s'est élaborée progressivement sur une dizaine d'années.

La version la plus ancienne de ces objets est constituée par les machines séquentielles de Moore et de Mealy, qui utilisent les automates finis déterministes non pas comme des reconnaisseurs, mais comme des machines produisant des symboles de sortie 0 ou 1 suivant que le mot lu est, ou non, accepté. La notion actuelle, plus générale, de fonction séquentielle (partial generalized sequential function, cf. [2]) est essentiellement obtenue en autorisant la sortie d'être non plus nécessairement réduite à un symbole, mais d'être constituée d'une suite, éventuellement vide, de symboles.

L'idée, décisive pour l'élaboration du concept final, est due à Rabin et Scott et consiste à généraliser aux parties du monoïde produit de deux monoïdes libres, la notion de partie reconnaissable d'un monoïde libre. C'est en systématisant ce point de vue, que la notion actuelle de relation rationnelle a été dégagée en 1965 par Elgot et Mezei, qui prouvèrent la plupart des propriétés de fermeture de ces nouveaux objets. Nivat simplifia considérablement leurs preuves en considérant les relations rationnelles comme définies par des "transducteurs finis", c'est-à-dire des automates finis munis d'une "sortie" leur permettant d'associer à tout mot d'"entrée" un ensemble de mots de "sortie", et en obtenant, grâce aux "bimorphismes", une caractérisation élégante de ces relations. De nombreux problèmes de décision ont depuis lors été résolus. Enfin, il n'est pas possible de parler de relations rationnelles sans rappeler qu'elles sont à l'origine de la théorie des familles agréables de langages (AFL dans la littérature anglo-saxonne) qui fournit une bonne mesure de complexité des langages algébriques.

Les résultats généraux ayant été établis, on assiste à un regain d'intérêt pour des problèmes plus particuliers et notamment ceux posés par les fonctions séquentielles. Il y a, à ce phénomène, plusieurs raisons. La première est que, comme l'ont montré de récents résultats, il est possible, à l'aide d'opérations élémentaires sur les fonctions séquentielles, de reconstruire un certain nombre de relations rationnelles. Citons pour mémoire le résultat de Eilenberg, suivant lequel toute fonction rationnelle (c'est-à-dire toute relation rationnelle qui définit une fonction partielle) peut être obtenue en composant une fonction séquentielle gauche et une fonction séquentielle droite (une fonction séquentielle est gauche ou droite suivant que son automate sous-jacent est gauche ou droit cf. [2]). Une seconde raison est qu'il ne semble pas possible, dans l'état actuel de la théorie, de résoudre dans le cas général des relations rationnelles, certains problèmes qui ont été résolus dans le cas particulier des fonctions séquentielles (cf. [1]).

On doit à Ginsburg et Rose une caractérisation des fonctions séquentielles dans la classe des fonctions d'un monoïde libre dans un autre (cf. [3]). Récemment, Schützenberger a montré que ces fonctions étaient solutions d'équations fonctionnelles définissant des fonctions rationnelles d'un type particulier, qu'il appelle fonctions sous-séquentielles, (cf. [6]). Il montre que la plupart des propriétés des fonctions séquentielles peuvent être généralisées aux fonctions sous-séquentielles et il caractérise ces dernières dans la classe des fonctions rationnelles.

Le but de cet article est de donner une caractérisation alternative des fonctions séquentielles et des fonctions sous-séquentielles, dans la classe des relations rationnelles. Cette caractérisation est constructive car elle montre qu'une relation rationnelle, définie par un transducteur fini donné T, est une fonction séquentielle (resp. sous-séquentielle) ssi les mots de sortie associés aux mots d'entrée de longueur au plus p, où p est un entier calculable à partir de T, satisfont à un ensemble fini de conditions simples du type "être facteur gauche de".

Plus précisément, rappelons qu'un *automate* fini $\mathscr{A}$ est constitué d'une partie $P \subseteq Q \times A \times Q$, où les ensembles finis non vides Q et A sont respectivement l'ensemble des états et l'alphabet d'entrée, d'un état initial $q_- \in Q$ et d'un état final $q_+ \in Q$. Un *transducteur* fini $(\mathscr{A}, h)$ est le couple formé d'un automate fini $\mathscr{A}$ et d'une fonction (de sortie) h de P dans le demi-anneau des parties rationnelles d'un monoïde libre finiment engendré B^*. Un tel transducteur définit de façon classique une relation rationnelle ρ de A^* dans B^*: le mot $x_1x_2\cdots x_n \in B^*$ appartient à l'image par ρ du mot $a_1a_2\cdots a_n \in A^*$ où $a_i \in A$ pour $i = 1, \ldots, n$, s'il existe $q_0, q_1 \cdots q_n \in Q$ tels que l'on ait $q_0 = q_-$, $q_n = q_+$ et $u_i \in (q_{i-1}, a_i, q_i)h$ pour $i = 1, \ldots, n$. Lorsque le transducteur définit une fonction séquentielle gauche, le langage reconnu par $\mathscr{A}$ est le complément d'un idéal à droite. Sous cette hypothèse pour $\mathscr{A}$, nous pouvons énoncer le résultat principal de ce travail, où nous avons noté par le même symbole la fonction h et son extension au demi-anneau des parties de P^*.

Théorème 1.1. *Pour tout automate $\mathcal{A} = (P, q_-, q_+)$ on peut déterminer deux parties finies $K_1 \subseteq (P^*)^4$ et $K_2 \subseteq (P^*)^2$ telles que pour toute fonction h de P dans un monoïde libre B^*, le transducteur $(\mathcal{A}, h)$ définisse une fonction séquentielle gauche ssi les deux conditions suivantes sont satisfaites:*

(i) *pour tout $(p_1, p_2, p_3, p_4) \in K_1$, si p_3h ou p_4h est distinct du mot vide, il existe $b \in B^*$ tel que:*

— *ou bien $p_1h = p_2h \cdot b$ et $b \cdot p_4h = p_3h \cdot b$,*

— *ou bien $p_2h = p_1h \cdot b$ et $b \cdot p_3h = p_4h \cdot b$.*

(ii) *pour tout $(p_1, p_2) \in K_2$, p_1h est facteur gauche de p_2h.*

Nous verrons dans la quatrième partie que K_2 est union de deux parties disjointes K_2' et K_2'': la condition (i) et la condition (ii) pour les couples de K_2' expriment que la fonction rationnelle est sous-séquentielle. La condition (ii) pour les couples de K_2'' exprime une propriété de conservation des facteurs gauches.

Le résultat a ainsi deux conséquences. D'abord en vertu de ce qui précède, il prouve qu'il est possible de décider si une relation rationnelle définie par un transducteur donné, est une fonction séquentielle (resp. sous-séquentielle) gauche. Ensuite pour des raisons intuitives de symétrie que nous préciserons dans la dernière partie de ce travail, il existe un énoncé semblable pour les fonctions séquentielles droites: on peut donc décider si une relation rationnelle est une fonction biséquentielle (resp. bisous-séquentielle) c'est-à-dire séquentielle (resp. sous-séquentielle) gauche et droite.

La démonstration du résultat s'effectue suivant le schéma suivant.

Dans la deuxième partie nous faisons un rappel de définitions et résultats bien connus concernant les relations rationnelles.

Nous utilisons dans la troisième partie une distance sur les mots qui nous permet de définir les fonctions à variation bornée. Nous montrons que les fonctions rationnelles à variation bornée sont les fonctions sous-séquentielles.

Enfin, nous rappelons la notion de relation rationelle transposée, dans la quatrième partie et nous démontrons le Théorème 1.1, ce qui nous permet d'établir qu'il est possible de décider si une relation rationnelle est une fonction séquentielle (resp. sous-séquentielle) ou biséquentielle (resp. bisous-séquentielle).

2. Relations rationnelles. Fonctions séquentielles et fonctions sous-séquentielles

Nous noterons A^* (resp. A^+) le monoïde libre (resp. le demi-groupe libre) engendré par l'ensemble non vide A. Les éléments de A^* sont des *mots*. Son élément neutre — ou mot *vide* — est noté 1. Les monoïdes libres que nous envisagerons par la suite sont tous supposés finiment engendrés.

2.1. *Relations rationnelles*

Une *relation rationnelle* ρ du monoïde libre A^* dans le monoïde libre B^* — nous noterons $\rho : A^* \to B^*$ — est une application de A^* dans l'ensemble des parties de B^*, pour laquelle il existe un ensemble fini Q, deux éléments distingués $q_-, q_+ \in Q$, un morphisme de demi-groupe μ de A^* dans un monoïde de $Q \times Q$-matrices à entrées dans le demi-anneau $\mathrm{Rat}\, B^*$ des parties rationnelles de B^*, le tout vérifiant: $u\rho = u\mu_{q_-q_+}$.

Le triplet $T = (\mu, q_-, q_+)$ est un *transducteur* réalisant ρ et le nombre d'éléments de Q est sa *dimension.*

Le transducteur est *normalisé* si μ est un morphisme de monoïde, si q_- et q_+ sont distincts et si l'on a pour tout $u \in A^+$ et $q \in Q$: $u\mu_{qq_-} = u\mu_{q_+q} = 0$. Il est *émondé* si pour tout $q \in Q$ il existe $u_1, u_2 \in A^*$ tels que l'on ait: $u_1\mu_{q_-q} \cdot u_2\mu_{qq_+} \neq 0$.

On sait que toute relation rationnelle ρ est union de deux relations rationnelles ρ_1 et ρ_+ qui sont respectivement les restrictions de ρ à $\{1\}$ et à A^+ et que ρ_+ peut être réalisée par un transducteur normalisé et émondé (cf. [2]). Nous confondrons les relations de A^* dans B^* qui ont même restriction à A^+, ce qui nous permettra de n'envisager que des transducteurs normalisés et émondés.

2.2. *Fonctions rationnelles*

Une *fonction rationnelle* est une relation rationnelle $\rho : A^* \to B^*$ pour laquelle l'ensemble $x\rho$ possède au plus un mot, quelque soit x dans A^*.

Nous conviendrons de considérer toute fonction partielle d'une partie X de A^* dans B^* comme une fonction de X dans $B^* \cup 0$ où 0 est le zéro du demi-anneau des parties de B^*. Une fonction rationnelle peut ainsi être interprétée comme une relation rationnelle définissant une fonction partielle. Nous allons nous intéresser à un cas particulier de fonctions rationnelles.

2.3. *Fonctions sous-séquentielles*

Soit $k \geq 0$ un entier fixe. Une *fonction sous-séquentielle gauche* (resp. *droite*) est une fonction partielle $\alpha : A^* \to B^*$ pour laquelle il existe un ensemble fini Q, un morphisme de monoïde μ de A^* dans un monoïde de $Q \times Q$-matrices à entrées dans $B^* \cup 0$ ayant au plus une entrée non nulle par ligne (resp. par colonne), un Q-vecteur ligne (resp. colonne) λ ayant une seule entrée non nulle et une fonction v de A^k dans les Q-vecteurs colonnes (resp. lignes) à entrées dans $B^* \cup 0$, de telle façon que l'on ait: $ux\alpha = \lambda \cdot u\mu \cdot xv$ (resp. $xu\alpha = xv \cdot u\mu \cdot \lambda$). Le triplet (μ, λ, v) est un *transducteur sous-séquentiel gauche* (resp. *droit*) réalisant α.

Une fonction $\alpha : A^* \to B^*$ est *bisous-séquentielle* si elle est sous-séquentielle gauche et sous-séquentielle droite.

Proposition 2.1. *Toute fonction sous-séquentielle gauche est rationnelle.*

Preuve. Soit (μ, λ, v) un transducteur sous-séquentiel réalisant la fonction sous-séquentielle gauche α et $q_- \in Q$ l'indice de l'unique entrée non-nulle de λ.

Si k n'est pas nul, on considère l'ensemble $Q' = Q \times (A^* \setminus A^*A^k) \cup \{q_+\}$ où q_+

est un nouveau symbole et on associe à tout $a \in A$ la $Q' \times Q'$-matrice à entrées dans Rat B^* définie par:

$$\begin{cases} a\mu'_{(q,1)(q',1)} = a\mu_{q,q'} & \text{si } q, q' \in Q, \\ a\mu'_{(q,u)(q,ua)} = 1 & \text{si } (q,u) \in Q \times (A^* \setminus A^* A^{k-1}), \\ a\mu'_{(q,u)q_+} = (uav)_q & \text{si } (q,u) \in Q \times A^{k-1}, \\ a\mu'_{qq'} = 0 & \text{dans les autres cas.} \end{cases}$$

Alors (μ', q_-, q_+) est un transducteur réalisant α.

Si k est nul, α a même restriction à A^+ que la fonction sous-séquentielle gauche α' réalisée par le transducteur sous-séquentiel (μ, λ, v') où v' est la fonction de A dans les vecteur-colonnes à entrées dans $B^* \cup 0$, définie par $av' = a\mu \cdot 1v$, ce qui nous ramène au cas précédent.

Rappelons le résultat suivant qui caractérise les fonctions sous-séquentielles dans la classe des fonctions partielles d'un monoïde libre dans un autre, cf. [6].

Théorème 2.2. (Schützenberger.) *La fonction partielle* $\alpha : A^*A^k \to B^*$ *est sous-séquentielle s'il existe une fonction partielle* $\beta : A^* \to B^*$ *et une application* $u \to \rho_u$ *de* A^* *dans un ensemble fini de fonctions partielles de* A^kA^* *dans* B^*, *tels que l'on ait identiquement*: $uw\alpha = u\beta w\rho_u$.

Nous montrons dans la troisième partie comment sont obtenues les fonctions ρ_u à partir d'un transducteur réalisant α.

2.4. Fonctions séquentielles

Une *fonction séquentielle gauche* (resp. *droite*) est une fonction sous-séquentielle gauche (resp. droite) réalisée par un transducteur sous-séquentiel gauche (resp. droit) pour lequel k vaut 0, l'unique entrée non nulle du vecteur λ est égale à 1 et $1 \cdot v$ est le vecteur dont toutes les entrées sont égales à 1. Une fonction est *biséquentielle*, si elle est séquentielle gauche et séquentielle droite.

Le Théorème 2.2. est une généralisation du résultat suivant, cf. [3].

Théorème 2.3. (Ginsburg et Rose.) *Soit* $\alpha : A^* \to B^*$ *une fonction rationnelle telle que* $1\alpha = 1$. *Alors* α *est séquentielle ssi il existe un entier* $r \geq 0$ *tel que pour tout* $u \in A^*$ *et* $a \in A$ *on ait*: $ua\alpha \in u\alpha \cdot (B^* \setminus B^*B^r) \cup 0$.

3. Fonctions rationnelles à variation bornée

3.1. Groupe libre

Soit A^{-1} un ensemble en bijection avec A tel que $A \cap A^{-1} = \emptyset$. On note a^{-1} l'élément qui correspond à $a \in A$ dans la bijection. Considérons sur le monoïde libre $(A \cup A^{-1})^*$ la congruence engendrée par les relations $aa^{-1} = a^{-1}a = 1$ pour

$a \in A$. Le quotient de $(A \cup A^{-1})^*$ par cette congruence est équivalent au *groupe libre* $A^{(*)}$ engendré par A. Nous conviendrons de confondre A^* avec son image par le morphisme canonique $\mathscr{F}$ de $(A \cup A^{-1})^*$ sur $A^{(*)}$, ce qui nous permettra de considérer A^* comme sous-monoïde de $A^{(*)}$.

On rappelle que tout $x \in A^{(*)}$ est image par $\mathscr{F}$ d'un unique mot u de $(A \cup A^{-1})^*$ ne contenant aucun facteur de la forme aa^{-1} ou $a^{-1}a$ (cf. par ex. [4]). La *longueur* $|x|$ de x sera par definition la longueur du mot (*réduit*) u sur l'alphabet $A \cup A^{-1}$. On a évidemment: $|xy| \leq |x| + |y|$ pour x, y dans $A^{(*)}$.

3.2. Une distance sur A^*

On définit une distance sur A^* en posant $\langle x, y\rangle = |x^{-1}y|$. Les propriétés habituelles de la distance sont aisément vérifiées:

(i) $\langle x, y\rangle = 0$ ssi $x = y$.

(ii) $\langle x, y\rangle = \langle y, x\rangle$.

(iii) $\langle x, y\rangle = |x^{-1}y| = |x^{-1}z \cdot z^{-1}y| \leq |x^{-1}z| + |z^{-1}y| = \langle x, z\rangle + \langle z, y\rangle$.

Une fonction partielle $\alpha : A^* \to B^*$ est à *variation bornée* (v.b.) si pour tout $l \geq 0$ il existe $L \geq 0$ tel que $\langle x\alpha, y\alpha\rangle \leq L$ dès que $x\alpha \cdot y\alpha \neq 0$ et $\langle x, y\rangle \leq l$.

3.3. Quelques propriétés combinatoires du monoïde libre

Les propositions suivantes sont des lemmes qui seront utilisés dans le dernier paragraphe de cette partie.

Proposition 3.1. *Soit $a, b, c \in A^*$ et $p > 0$ tels que $a^p b = bc^p$. Alors on a pour tout $n \geq 0$: $a^n b = bc^n$.*

Preuve. L'assertion est trivialement vérifiée lorsque a (et donc b) est le mot vide. Nous supposerons donc $a \neq 1$ (et donc $b \neq 1$).

L'égalité $a^p b = bc^p$ entraîne pour tout $k \geq 0$: (1) $a^{p\cdot k} b = bc^{p\cdot k}$. Il existe donc un entier $m \geq 0$ et $a_1, a_2 \in A^*$ tels que $b = a^m a_1$, $a = a_1 a_2$ et $a_1 \neq 1$. En comparant les facteurs droits de longueur $|b|$ dans (1) on a: $b = c_2 c^m$, $c = c_1 c_2$ et $c_1 \neq 1$, ce qui entraîne $a_2 a_1 = c_1 c_2$. Mais alors $ab = a^{m+1} a_1 = a_1(a_2 a_1)^m c = bc$ et par conséquent $a^n b = bc^n$ pour tout $n \geq 0$. $\square$

Pour la résolution de l'équation $ab = bc$ on peut consulter [5].

Proposition 3.2. *Soit $a_1, b_1, a_2, b_2 \in A^*$ et supposons $b_1 \neq 1$ ou $b_2 \neq 1$. Alors on a:*

$$a_2^{-1} a_1 b_1 = b_2 a_2^{-1} a_1 \tag{1}$$

ssi il existe $u \in A^*$ tel que l'on ait:

$$a_2 = a_1 u \quad \text{et} \quad ub_2 = b_1 u,$$

ou

$$a_1 = a_2 u \quad \text{et} \quad ub_1 = b_2 u.$$

Preuve. La condition est évidemment suffisante. Pour montrer qu'elle est nécessaire considérons $a \in A^*$ le plus long facteur gauche commun de a_1 et a_2: $a_1 = ax$ et $a_2 = ay$. De (1) on déduit: $xb_1 = yb_2y^{-1}x$ c'est-à-dire $xb_1 = b_2x$ si $y = 1$. Comme $b_2 = 1$ entraîne $b_1 = 1$, l'hypothèse $y \neq 1$ implique $x = 1$, c'est-à-dire $yb_1 = b_2y$, ce qui achève la vérification. □

Proposition 3.3. *Considérons $a_i, b_i, c_i \in A^*$ où i appartient à un ensemble I et $x \in A^*$ (resp. $y \in A^*$) le plus long facteur gauche commun des mots $a_ib_ic_i$ (resp. a_ic_i). Si pour tout $i, j \in I$ on a: $a_j^{-1}a_ib_i = b_ja_j^{-1}a_i$ alors on a pour tout $k \in I$:*

$$x^{-1}a_kb_kc_k = y^{-1}a_kc_k.$$

Preuve. Par définition de x et de y on a pour tout $i \in I$: $a_ib_ic_i = xh$ et $a_ic_i = yl$ où h et l sont dans A^*. Alors: $h^{-1}(x^{-1}a_kb_kc_k) = (a_ib_ic_i)^{-1}\ a_kb_kc_k = c_i^{-1}b_i^{-1}a_i^{-1}a_kb_kc_k = c_i^{-1}a_i^{-1}a_kc_k = l^{-1}(y^{-1}a_kc_k)$ ce qui montre que $x^{-1}a_kb_kc_k$ est facteur droit de $y^{-1}a_kc_k$ pourvu que l'on ait choisi $a_ib_ic_i$ tel que x soit le plus long facteur gauche commun de $a_ib_ic_i$ et $a_kb_kc_k$. De même en choisissant $a_ib_ic_i$ tel que y soit le plus long facteur gauche commun de a_ic_i et a_kc_k on voit que $y^{-1}a_kc_k$ est facteur droit de $x^{-1}a_kb_kc_k$ c'est-à-dire finalement: $x^{-1}a_kb_kc_k = y^{-1}a_kc_k$. □

3.4. *Caractérisation des fonctions rationnelles à v.b.*

Le but de ce paragraphe est de caractériser les fonctions rationnelles qui sont à variation bornée. Nous introduisons au préalable une définition.

Le transducteur (μ, q_-, q_+) satisfait le condition de *jumelage à l'ordre p* ssi pour tout x, $u \in A^+$, $q_1, q_2 \in Q$ et $a_1, a_2, b_1, b_2 \in B^*$ tels que $|xu| \leq p$, $a_1 \in x\mu_{q_-q_1}$, $b_1 \in u\mu_{q_1q_1}$, $a_2 \in x\mu_{q_-q_2}$ et $b_2 \in u\mu_{q_2q_2}$ on a: $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$. On dira simplement qu'il satisfait la condition de jumelage s'il la satisfait à tout ordre.

Proposition 3.4. *Soit $T = (\mu, q_-, q_+)$ un transducteur de dimension n et $\alpha: A^* \to B^*$ la relation rationnelle qu'il réalise. Les conditions suivantes sont équivalentes:*

(i) *α est une fonction sous-séquentielle gauche.*

(ii) *α est une fonction à v.b.*

(iii) *pour tout mot $x \in A^*$ de longueur au plus $(n-2)^2 + 1$, $x\alpha$ possède au plus un mot et T satisfait la condition de jumelage à l'ordre $2(n-2)^2$.*

(iv) *Pour tout mot $x \in A^*$ de longueur au plus $(n-2)^2 + 1$, $x\alpha$ possède au plus un mot et T satisfait la condition de jumelage.*

Preuve. (i) $\Longrightarrow$ (ii) Soit (μ, λ, v) un transducteur sous-séquentiel réalisant α et posons

$$M = \sup\left(\sup_{\substack{a \in A \\ q,q' \in Q}} |a\mu_{qq'}|, \frac{1}{k} \sup_{\substack{|w|=k \\ q \in Q}} |(wv)_q| \right),$$

car on peut toujours supposer $k > 0$.

Soit $l \geqslant 0$ un entier et $x, y \in A^*$ des mots vérifiant $x\alpha \cdot y\alpha \neq 0$ et $\langle x, y\rangle \leqslant l$. Il existe des mots $u, x_1, x_2 \in A^*$ tels que l'on ait: $x = ux_1$, $y = uy_1$, $|x_1| \geqslant k$, $|y_1| \geqslant k$ et $|x_1y_1| \leqslant l + 2k$. Il vient alors: $\langle x\alpha, y\alpha\rangle \leqslant (l+2k) \cdot M$.

(ii) $\Longrightarrow$ (iii) Il suffit de montrer que T satisfait la condition de jumelage à l'ordre $2(n-2)^2$.

Soit $x, u \in A^+$, $q_1, q_2 \in Q$ et $a_1, a_2, b_1, b_2 \in B^*$ tels que l'on ait: $|xu| \leqslant 2(n-2)^2$, $a_1 = x\mu_{q_-q_1}$, $b_1 = u\mu_{q_1q_1}$ $a_2 = x\mu_{q_-q_2}$ et $b_2 = u\mu_{q_2q_2}$. Il existe des mots $w_1, w_2 \in A^*$ de longueur au plus $n-2$ tels que $w_1\mu_{q_1q_+}$ et $w_2\mu_{q_2q_+}$ soient non nuls. Pour tout entier $p \geqslant 0$ on a: $\langle xu^pw_1, xu^pw_2\rangle \leqslant |w_1| + |w_2| \leqslant 2(n-2)$. Comme α est à variable bornée, il existe des entier $r, s > 0$ vérifiant l'égalité $(xu^{r+s}w_1\alpha)^{-1} \cdot xu^{r+s}w_2\alpha = (xu^rw_1\alpha)^{-1}xu^rw_2\alpha$, c'est-à-dire: $a_1^{-1}a_2b_2^s = b_1^sa_1^{-1}a_2$ ce qui en vertu des Propositions 3.1 et 3.2. entraîne: $a_1^{-1}a_2b_2 = b_1a_1^{-1}a_2$.

(iii) $\Longrightarrow$ (iv) Supposons par l'absurde qu'il existe un couple (x, u) pour lequel la condition de jumelage est mise en défaut. Nous pouvons choisir un tel couple de façon à ce que la longueur $|xu|$ soit minimale.

Soit $q_1, q_2 \in Q$ et $a_1, a_2, b_1, b_2 \in B^*$ tels que l'on ait $a_1 \in x\mu_{q_-q_1}$, $a_2 \in x\mu_{q_-q_2}$, $b_1 \in u\mu_{q_1q_1}$ et $b_2 \in u\mu_{q_2q_2}$. Puisque $|xu| > 2(n-2)^2$ on doit avoir $|x| > (n-2)^2$ ou $|u| > (n-2)^2$.

Dans le premier cas on peut décomposer $x = x_1hx_2$ où $x_1, x_2, h \in A^*$, $h \neq 1$ et $|h| \leqslant (n-2)^2$ de telle façon qu'il y ait des états $r_1, r_2 \in Q$ et des mots $c_1, d_1, e_1, c_2, d_2, e_2 \in B^*$ vérifiant:

$$c_1 \in x_1\mu_{q_-r_1}, \qquad d_1 \in h\mu_{r_1r_1}, \qquad e_1 \in x_2\mu_{r_1q_1}, \qquad c_1d_1e_1 = a_1,$$

$$c_2 \in x_1\mu_{q_-r_2}, \qquad d_2 \in h\mu_{r_2r_2}, \qquad e_2 \in x_2\mu_{r_2q_2}, \qquad c_2d_2e_2 = a_2.$$

Puisque par hypothèse le transducteur satisfait la condition de jumelage pour les couples (x_1, h) et (x_1x_2, u) on a respectivement:

$$c_2^{-1}c_1d_1 = d_2c_2^{-1}c_1$$

et

$$(c_2e_2)^{-1}c_1e_1b_1 = b_2(c_2e_2)^{-1}c_1e_1. \tag{2}$$

En remplaçant $c_2^{-1}c_1$ par $d_2^{-1}c_2^{-1}c_1d_1$ dans (2) on obtient:

$$e_2^{-1}(d_2^{-1}c_2^{-1}c_1d_1)e_1b_1 = b_2e_2^{-1}d_2^{-1}c_2^{-1}c_1d_1e_1$$

c'est-à-dire $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$.

Dans le second cas on décompose $u = u_1hu_2$ avec $u_1, u_2, h \in A^*$, $h \neq 1$ et $|h| \leqslant (n-2)^2$ de telle façon qu'il y ait des états $r_1, r_2 \in Q$ et des mots $c_1, d_1, e_1, c_2, d_2, e_2 \in B^*$ vérifiant:

$$c_1 \in u_1\mu_{q_1r_1}, \qquad d_1 \in h\mu_{r_1r_1}, \qquad e_1 \in u_2\mu_{r_1q_1}, \qquad c_1d_1e_1 = b_1,$$

$$c_2 \in u_1\mu_{q_2r_2}, \qquad d_2 \in h\mu_{r_2r_2}, \qquad e_2 \in u_2\mu_{r_2q_2}, \qquad c_2d_2e_2 = b_2.$$

Si $u_2 = 1$ on a $r_1 = q_1$, $r_2 = q_2$ et donc $e_1 = e_2 = 1$. Le transducteur vérifie la condition de jumelage pour les couples (x, u_1) et (x, h) ce qui donne respectivement $a_2^{-1}a_1c_1 = c_2a_2^{-1}a_1$ et $a_2^{-1}a_1d_1 = d_2a_2^{-1}a_1$ c'est-à-dire $a_2^{-1}a_1c_1d_1 = c_2d_2a_2^{-1}a_1$ ou encore $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$.

Si $u_2 \neq 1$ on peut exprimer la condition de jumelage pour les couples (x, u_1u_2) et (xu_1, h). On obtient les égalités

$$a_2^{-1}a_1c_1e_1 = c_2e_2a_2^{-1}a_1$$

et

$$(a_2c_2)^{-1}a_1c_1d_1 = d_2(a_2c_2)^{-1}a_1c_1. \tag{3}$$

En multipliant chaque membre de (3) à droite par e_1 et à gauche par c_2, il vient:

$$a_2^{-1}a_1c_1d_1e_1 = c_2d_2c_2^{-1}a_2^{-1}a_1c_1e_1 = c_2d_2e_2a_2^{-1}a_1$$

c'est-à-dire $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$ ce qui achève la vérification.

(iv) $\Longrightarrow$ (i) Nous allons d'abord vérifier que α est une fonction partielle. Supposons donc par l'absurde qu'il existe un mot $x \in A^+$, que nous pouvons choisir de longueur minimale, tel que $x\alpha$ possède deux mots distincts $d_1, d_2 \in B^*$. Comme on a $|x| > (n-2)^2 + 1$, il existe $q_1, q_2 \in Q$, $x_1, x_2, h \in A^*$ où $h \neq 1$ et $|h| \leq (n-2)^2$, et $a_1, b_1, c_1, a_2, b_2, c_2 \in B^*$ tels que l'on ait: $d_1 = a_1b_1c_1$, $d_2 = a_2b_2c_2$, $a_1 \in x_1\mu_{q_-q_1}$, $b_1 \in h\mu_{q_1q_1}$,

$$c_1 \in x_2\mu_{q_1q_+}, \qquad a_2 \in x_1\mu_{q_-q_2}, \qquad b_2 \in h\mu_{q_2q_2} \quad \text{et} \quad c_2 \in x_2\mu_{q_2q_+}.$$

La condition de jumelage pour le couple (x_1, h) entraine $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$ et le fait que a_1c_1 et a_2c_2 appartiennent à $x_1x_2\alpha$ implique $a_1c_1 = a_2c_2$. Mais alors on a:

$$d_1 = a_1b_1c_1 = a_2b_2a_2^{-1}a_1c_1 = a_2b_2c_2 = d_2$$

d'où la contradiction.

Il nous suffit à présent de vérifier les conditions du Théorème 2.2.

Pour tout mot u de A^* on note $u\beta$ le plus long facteur gauche commun des mots $u\mu_{q_-q}$ où $q \in Q$, et on convient alors $u\beta = 0$ si $u\mu_{q_-q} = 0$ pour tout $q \in Q$. Nous allons montrer qu'il existe un entier $H \geq 0$ tel que $|u\beta^{-1}u\mu_{q_-q}| \leq H$ pour tout $u \in A^*$ et $q \in Q$ dès que $u\beta \neq 0$.

Soit $u \in A^*$ un mot de longueur au moins égale à n^n. Considérons la partie $Q' = \{q_i\}_{1 \leq i \leq r}$ de Q constituée des éléments q tels que $u\mu_{q_-q} \neq 0$. Il existe une factorisation $u = u_1xu_2$ où $u_1, u_2, x \in A^*$ et $x \neq 1$ et des états q'_i, pour $1 \leq i \leq r$, vérifiant $a_i = u_1\mu_{q_-q'_i} \neq 0$ $b_i = x\mu_{q'_iq'_i} \neq 0$ et $c_i = u_2\mu_{q'_iq_i} \neq 0$.

Le mot $u_1u_2\beta$ est facteur gauche du plus grand facteur gauche commun $t \in B^*$ des mots $a_ic_i = u_1u_2\mu_{q_-q_i}$. On a donc $u_1u_2\beta \cdot h = t$ où $h \in B^*$. En vertu dela condition de jumelage il vient: $(u_1xu_2\beta)^{-1}a_ib_ic_i = t^{-1}a_ic_i$.

L'inégalité $|t^{-1}a_ic_i| \leq |(u_1u_2\beta)^{-1}a_ic_i|$ permet de conclure à l'existence de l'entier H.

Pour achever la démonstration il suffit de considérer pour tout $u \in A^*$ la fonction partielle ρ_u de A^nA^* dans B^* définie par $w\rho_u = 0$ si $u\beta = 0$ et $w\rho_u = u\beta^{-1}uw\alpha$ sinon. Si $w\rho_u$ est non nul il existe $q \in Q$ tel que $uw\alpha = u\mu_{q-q}\ w\mu_{qq+}$ ce qui entraîne: $w\rho_u = (u\beta^{-1}u\mu_{q-q}) \cdot w_{qq+}$. Comme Q est fini et que $u\beta^{-1}u\mu_{q-q}$ est bornée, il existe un nombre *fini* de fonctions ρ_u ce qui achève la démonstration. □

Il s'ensuit immédiatement le:

Corollaire 3.5. *On peut décider si une relation rationnelle définie par un transducteur donné est une fonction sous-séquentielle gauche.*

On a aussi en vertu du Théorème 2.3. le:

Corollaire 3.6. *Une fonction sous-séquentielle gauche $\alpha : A^* \to B^*$ qui vérifie $ua\alpha \in u\alpha \cdot B^* \cup 0$ pour tout $u \in A^*$ et $a \in A$. est une fonction séquentielle gauche.*

4. Démonstration du Théorème 1.1. et applications

4.1. Démonstration du théorème

La restriction à A^+ du morphisme μ défini par un transducteur normalisé et émondé dont l'automate $\mathscr{A} = (P, q_-, q_+)$ est donné, est entièrement déterminée par la fonction h qui à tout $(q, a, q') \in P$ associe $(q, a, q')h = a\mu_{qq'} \in \operatorname{Rat} B^*$. Pour que la relation rationnelle réalisée par le transducteur — que nous identifierons au couple $(\mathscr{A}, h)$ — soit une fonction séquentielle gauche, il faut bien évidemment que h applique P dans B^* — c'est-à-dire $a\mu_{qq'} = \{b\}$ pour un certain $b \in B^*$ — et que, en vertu du Théorème 2.3. le langage reconnu par l'automate $\mathscr{A}$ soit le complément d'un idéal à droite, hypothèse que nous faisons dans le Théorème 1.1. que nous rappelons ici:

Théorème 1.1. *Pour tout automate $\mathscr{A} = (P, q_-, q_+)$ on peut déterminer deux parties finies $K_1 \subseteq (P^*)^4$ et $K_2 \subseteq (P^*)^2$ telles que pour toute fonction h de P dans un monoïde libre B^*, le transducteur $(\mathscr{A}, h)$ réalise une fonction séquentielle gauche ssi les deux conditions suivantes sont satisfaites:*

(i) *pour tout $(p_1, p_2, p_3, p_4) \in K_1$, si p_3h ou p_4h est distinct du mot vide, il existe $b \in B^*$ tel que:*

— *ou bien $p_1h = p_2h \cdot b$ et $b \cdot p_4h = p_3h \cdot b$*

— *ou bien $p_2h = p_1h \cdot b$ et $b \cdot p_3h = p_4h \cdot b$*

(ii) *pour tout $(p_1, p_2) \in K_2$, p_1h est facteur gauche de p_2h.*

Preuve. Soit π_1, π_2, π_3 les applications qui envoient tout élément de $P \subseteq Q \times A \times Q$ sur sa première, deuxième et troisième composante respectivement. On étend naturellement ces applications à P^+ par récurrence: $uv\pi_1 = u\pi_1$, $uv\pi_2 = u\pi_2 \cdot v\pi_2$ et $uv\pi_3 = v\pi_3$ pour $u, v \in P^+$. On pose $n = \text{Card}\, Q$,

$I = \{p \in P \mid p\pi_1 = q_-\}$, $\quad F = \{p \in P \mid p\pi_3 = q_+\}$ et

$D = \{(p_1, p_2) \in P^2 \mid p_1\pi_3 \neq p_2\pi_1\}$ et on considère les ensembles:

$$K_1 = \{(p_1, p_2, p_3, p_4) \in (P^* \setminus P^*DP^*)^4 \mid p_1\pi_1 = p_2\pi_1 = q_-, p_1\pi_3 = p_3\pi_1 = p_3\pi_3,$$
$$p_2\pi_3 = p_4\pi_1 = p_4\pi_3, p_1\pi_2 = p_2\pi_2, p_3\pi_2 = p_4\pi_2 \text{ et } |p_1p_3| = |p_2p_4| \leq 2(n-2)^2\},$$

$$K_2' = \{(p_1, p_2) \in P^2 \mid p_1\pi_1 = p_2\pi_1 = q_-, p_1\pi_2 = p_2\pi_2, p_1\pi_3 = p_2\pi_3 = q_+$$
$$\text{et } |p_1| = |p_2| \leq (n-2)^2 + 1\},$$

$$K_2'' = \{(p_1, p_2) \in P^2 \mid p_1\pi_1 = p_2\pi_1 = q_-, p_2 \in p_1 \cdot P, p_1\pi_3 = p_2\pi_3 = q_+$$
$$\text{et } |p_1| \leq (n-2)^2 + 1\},$$

enfin $K_2 = K_2' \cup K_2''$.

Soit $(\mathscr{A}, h)$ un transducteur comme dans l'énoncé du théorème. Nous dirons que le quadruplet $(p_1, p_2, p_3, p_4) \in (P^*)^4$ satisfait la condition (i) si, lorsque p_3h ou p_4h est distinct du mot vide, il existe $b \in B^*$ tel que ou bien $p_1h = p_2h \cdot b$ et $b \cdot p_4h = p_3h \cdot b$ ou bien $p_2h = p_1h \cdot b$ et $b \cdot p_3h = p_4h \cdot b$. Nous dirons que le couple $(p_1, p_2) \in (P^*)^2$ satisfait la condition (ii) si p_1h est facteur gauche de p_2h.

En vertu des Propositions 3.4 et 3.2, l'hypothèse que tout élément de K_1 satisfait la condition (i) et que tout élément de K_2' satisfait la condition (ii) équivaut au fait que $(\mathscr{A}, h)$ définisse une fonction sout-séquentielle α. Pour montrer le théorème, il suffit donc, en raison du Théorème 2.3 et du corollaire 3.6, de prouver qu'avec l'hypothèse supplémentaire que tout couple de K_2'' vérifie la condition (ii), pour tout $u \in A^*$ et $a \in A$ on a: $ua\alpha \in u\alpha \cdot B^* \cup 0$.

Supposons par l'absurde qu'il existe un mot $u \in A^*$ et une lettre $a \in A$ tel que $u\alpha \neq 0$ et $u\alpha^{-1}ua\alpha \notin B^*$. Nous pouvons choisir u de longueur minimale pour cette propriété. Puisque les couples de K_2'' vérifient la condition (ii) on a $|u| > (n-2)^2 + 1$ et il existe $q_1, q_2 \in Q, u_1, u_2, \quad x \in A^*$ avec $x \neq 1$ et $|x| \leq (n-2)^2$, et $a_1, b_1, c_1, a_2, b_2, c_2 \in B^*$ tels que l'on ait:

$$u = u_1xu_2, \quad a_1 = u_1\mu_{q_-q_1}, \quad b_1 = x\mu_{q_1q_1}, \quad c_1 = u_2\mu_{q_1q_+}, \quad a_2 = u_1\mu_{q_-q_2},$$
$$b_2 = x\mu_{q_2q_2}, \quad c_2 = u_2\mu_{q_2q_+}, \quad u\alpha = a_1b_1c_1 \quad \text{et} \quad ua\alpha = a_2b_2c_2.$$

Puisque les quadruplets de K_1 vérifient la condition (i), en vertu de la Proposition 3.2 on a $a_2^{-1}a_1b_1 = b_2a_2^{-1}a_1$. Alors il vient:

$$\begin{aligned} u_1xu_2\alpha^{-1}u_1xu_2a\alpha &= (a_1b_1c_1)^{-1}a_2b_2c_2 = c_1^{-1}b_1^{-1}a_1^{-1}a_2b_2c_2 = c_1^{-1}a_1^{-1}a_2c_2 \\ &= u_1u_2\alpha^{-1}u_1u_2a\alpha \in B^* \end{aligned}$$

ce qui achève la preuve. $\square$

4.2. Relation rationnelle transposée. Applications du Théorème 1.1

A tout mot $u = a_1 \cdots a_n$ de A^* où $a_i \in A$ pour $i = 1, \ldots, n$, on associe le mot *miroir* $u^t = a_n \cdots a_1$ et on convient que $1^t = 1$. Cette application s'étend naturellement aux parties de A^* en posant $0^t = 0$, puis aux $Q \times Q'$-matrices à entrées dans le demi-anneau 2^{A^*} des parties de A^* en associant à la $Q \times Q'$-matrice m, la $Q' \times Q$-matrice m^t définie par: $(m^t)_{q_1q_2} = (m_{q_2q_1})^t$, pour $q_1 \in Q'$ et $q_2 \in Q$.

Si φ est une fonction de A^* dans 2^{B^*} ou dans un ensemble de $Q \times Q'$-matrices à entrées dans 2^{B^*}, on note φ^t la fonction *transposée* de φ définie par: $u\varphi^t = (u^t\varphi)^t$ pour tout $u \in A^*$. On a évidemment: $(\varphi^t)^t = \varphi$. En particulier si φ est un morphisme de A^* dans un demi-anneau de $Q \times Q$-matrices à entrées dans 2^{B^*}, il en est de même pour φ^t car on a pour tout $u, v \in A^*$ et $q_1, q_2 \in Q$:

$$(uv\varphi^t)_{q_1q_2} = (((uv)^t\varphi)^t)_{q_1q_2} = (v^tu^t\varphi_{q_2q_1})^t = \left(\sum_{q_3 \in Q} v^t\varphi_{q_2q_3}u^t\varphi_{q_3q_1}\right)^t$$

$$= \sum_{q_3 \in Q} (u^t\varphi_{q_3q_1})^t(v^t\varphi_{q_2q_3})^t = \sum_{q_3 \in Q} (u^t\varphi)^t_{q_1q_3}(v^t\varphi)^t_{q_3q_2} = (u\varphi^t v\varphi^t)_{q_1q_2}.$$

On peut ainsi définir le transducteur *transposé* de $T = (\mu, q_-, q_+)$ comme étant le transducteur $T^t = (\mu^t, q_+, q_-)$. Le résultat suivant découle des définitions antérieures.

Proposition 4.1. *Soit T un transducteur réalisant la relation rationnelle ρ. Alors T^t réalise ρ^t.*

De même le transposé du transducteur sous-séquentiel gauche (resp. droit) (μ, λ, v) est le transducteur sous-séquentiel droit (resp. gauche) (μ^t, λ^t, v^t).

Proposition 4.2. *Le transducteur sous-séquentiel (resp. séquentiel) gauche (μ, λ, v) réalise la fonction sous-séquentielle (resp. séquentielle) gauche α, ssi le transducteur sous-séquentiel (resp. séquentiel) droit (μ^t, λ^t, v^t) réalise la fonction sous-séquentielle (resp. séquentielle) droite α^t.*

Preuve. Il suffit de montrer que si $\alpha : A^* \to B^*$ est réalisée par le transducteur sous-séquentiel gauche (μ, λ, v), alors α^t est réalisée par le transducteur sous-séquentiel droit (μ^t, λ^t, v^t).

Soit $u \in A^*$, $x \in A^kA^*$. Si q_- est l'indice de l'unique entrée non-nulle du vecteur λ, il existe un unique $q \in Q$ tel que:
$ux\alpha = \lambda_{q_-} \cdot u\mu_{q_-q} \cdot (xv)_q$. On a donc:

$$ux\alpha = ((xv)^t_q \cdot (u\mu_{q_-q})^t \cdot \lambda^t_{q_-})^t = ((xv^t)_q \cdot (u^t\mu^t)_{qq_-} \cdot \lambda^t_{q_-})^t = (((x^tv)^t)_q \cdot (u^t\mu^t)_{qq_-} \cdot \lambda^t_{q_-})$$

$$= ((ux)^t\alpha^t)^t, \text{ ce qui établit le résultat. } \square$$

On obtient directement le résultat suivant.

Corollaire 4.3. *La relation rationnelle ρ est une fonction bisous-séquentielle (resp. biséquentielle) ssi ρ et ρ' sont des fonctions sous-séquentielles (resp. séquentielles) gauches.*

En vertu de la Proposition 3.4, du Théorème 1.1 et du corollaire précédent, on a finalement le:

Corollaire 4.4. *On peut décider si une relation rationnelle définie par un transducteur donné est une fonction séquentielle gauche (resp. séquentielle droite, biséquentielle, sous-séquentielle gauche, sous-séquentielle droite, bisous-séquentielle).*

Nous apprenons que des résultats très proches de ceux présentés dans cet article ont été découverts récemment par A. Demers, C. Kelemen et B. Reusch, dans un article communiqué personnellement à l'auteur et intitulé "On encryption systems realized by finite transducers".

Bibliographie

[1] C. Choffrut, Transducteurs conservant l'imprimitivité, in: M. Nivat, ed., *Automata, Languages and Programming* (North-Holland, Amsterdam, 1973).

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

[3] S. Ginsburg, *The Mathematical Theory of Context-free-Languages* (McGraw-Hill, New York, 1966).

[4] M. Hall, *The Theory of Groups* (Macmillan, New York, 1959).

[5] R.C. Lyndon and M.P. Schützenberger, The equation $a^m = b^n c^p$ in a free group, *Michigan Math. J.* **9** (1962) 289–298.

[6] M.P. Schützenberger, Sur une variante des fonctions séquentielles, *Theoret. Comput. Sci.* **4** (1977) 47–57.