SUR UNE PROPRIETE SYNTACTIQUE DES RELATIONS RATIONNELLES

M. P. SCHUTZENBERGER

(IRIA, Paris)

Résumé: On examine dans un cas particulier l'effet d'une relation rationnelle sur les monoïdes syntactiques.

Abstract: One studies in a special case connections between rational relations and syntactic monoids.

I - Introduction:

Une relation rationnelle $\theta : A^* \to B^*$ entre monoïdes libre associe à chaque partie reconnaissable F de B^* la partie reconnaissable $F\theta^{-1}$ de A^*.

Le problème des invariants syntactiques de θ, c'est à dire des propriétés du monoïde syntactique $Synt(F\theta^{-1})$ qui sont fonction de celles de Synt(F) a été posé par S. Eilenberg qui l'a complètement résolu dans les cas fondamentaux où θ est fonctionnelle ($Card(a\theta)\leq 1$ pour chaque $a \in A^*$) et en particulier quand θ est un morphisme. Nous nous proposons ici d'appliquer la théorie générale de la factorisation des morphismes et des cascades de produits en couronne de J.P. Rhodes et BR. Tilson (dont un bon exposé se trouve dans 'Algebraic Theory of Machines, Languages and Semi-groups, M.A. Arbib. Ed(1968))pour borner supérieurement pour certaines parties F les groupes dans $Synt(F\theta^{-1})$ au moyen de ce qu'après M. Nivat nous appelerons un transducteur pour θ.

Dans cette définition, nous notons 2^{B^*} le semi-anneau des parties du monoïde libre B^* (plus généralement 2^S sera le semi-anneau des parties de tout semi-groupe S).

Définition: μ est un transducteur pour θ ssi il existe un ensemble fini Q et deux éléments $q_0, q_+ \in Q$ tel que μ soit un morphisme de A^* dans le semi-anneau Γ_B des QxQ matrices à entrées dans 2^{B^*} satisfaisant la condition que $a\theta$ soit, pour chaque mot $a \in A^*$, l'entrée (q_0, q_+) de la matrice $a\mu$.

La donnée de θ comme partie rationnelle de $A^* \times B^*$ implique celle d'au moins un de ses transducteurs.

Soient maintenant Γ le semi-anneau des relations dans QxQ, Γ_B celui des QxQ matrices à entrées dans 2^G et enfin β le morphisme de Γ_B dans Γ envoyant chaque matrice m sur son <u>support</u>

$$m\beta = \{(q,q') \in QxQ : m_{q,q'} \neq \emptyset\}.$$

Nous appelerons <u>monoïde des supports</u> du transducteur μ le monoïde (nécessairement fini) $M_\mu = A^*\mu\beta$ formé des supports de toutes les matrices a_μ $(a \in A^*)$.

Le résultat principal de ce travail est la propriété ci-dessous dans laquelle la partie F de B^* est supposée être reconnaissable dans un groupe G, c'est à dire satisfaire $F = F\rho\rho^{-1}$ où ρ est un morphisme de B^* dans un groupe <u>fini</u> G.

Dans la section III on donne une application de cette propriété.

<u>Propriété:</u> Soient $\theta : A^* \to B^*$ une relation rationnelle et $F \subset B^*$ une partie reconnaissable dans un groupe fini G. Quelque soit le transducteur μ pour θ, tout groupe dans $Synt(F\theta^{-1})$ divise un produit en couronne $G \circ G'$ où G' est un groupe dans le monoide M_μ des supports du transducteur.

Montrons pour terminer comment la vérification de cet énoncé se ramène à l'application d'un lemme qui sera établi dans la section II.

Etant donnés Q et le morphisme $\rho : B^* \to G$, nous pouvons prolonger ce dernier à un morphisme (de semi-anneau) de 2^{B^*} dans 2^G puis à un morphisme de Γ_B dans le semi-anneau Γ_G des QxQ matrices à entrées dans G.

Gardant la notation β pour les supports de tous les semi-anneaux considérés, il est clair que $m\rho\beta = m\beta$ pour toute matrice m. Donc si $M' = A^*\mu\rho \subset \Gamma_G$, on a $M'\beta = M_\mu = A^*\mu\beta$. Comme $F\theta^{-1}$ est par définition l'ensemble des mots $a \in A^*$ tels que $a\theta \cap F \neq \emptyset$, nous avons la relation $F\theta^{-1} = \{a \in A^* : (a\mu\rho)_{q_0,q_+} \cap F\rho \neq \emptyset\}$, qui montre que $F' = F\theta^{-1}$ satisfait $F'(\mu\rho)(\mu\rho)^{-1}$. Ceci équivaut à ce que le monoide syntactique de $F\theta^{-1}$ soit une image homomorphe du monoïde <u>fini</u> $M' = A^*\mu\rho$.

Il suffit donc d'établir le lemme énoncé ci-dessous.

II. Un lemme technique:

Nous gardons les mêmes notations.

<u>Lemme:</u> Soit M' un monoïde de QxQ matrices à entrées dans 2^G où G est un groupe fini. Tout groupe H dans M' divise un produit en couronne $G \circ H\beta$ où $H\beta$ est un groupe dans $M'\beta$.

Nous désignons par u l'idempotent de H et nous montrons que la preuve se ramène par des méthodes standard (c'est à dire sans utiliser l'hypothèse que G est un groupe) au cas que nous appelerons positif c'est à dire à celui où le support de u est une classe d'équivalenoe $Q'xQ'$ $(Q'\subset Q)$.

II.1. Le groupe H divise le produit en couronne N Hβ où Hβ est un groupe et où : $N = \{h\in H : h\beta = u\beta\}$.

Preuve: Hβ est un groupe puisque H est un groupe et β un morphisme. De plus N est le noyau de β et la formule est un cas particulier des théorèmes de base des produits en couronne.

Q.E.D.

Etant données une relation quelconque $r\subset QxQ$ et une matrice $m\in M'$, nous designons par $m\wedge r$ la matrice $m'\in \Gamma_G$ telle que l'on ait identiquement $m'_{q,q'} = m_{q,q'}$ ou $= \emptyset$ selon que $(q,q')\in r$ ou non.

II.2. Il existe une famille $\{\varepsilon_i : i\in I\}$ de morphismes de N tels que d'une part chaque $N\varepsilon_i$ soit positif, d'autre part N soit un sous-groupe du produit direct des groupes $N\varepsilon_i$.

Preuve: Comme le support de u est une relation idempotente, il existe une famille de parties de Q non vides disjointes, Q_i $(i\in I)$ et une relation v telles que uβ soit l'union disjointe de $e = \sum_i Q_i xQ_i$ et de v et que $v = ev + ve + v^2$. Ceci entraîne que $\varepsilon_i : h \to h\wedge(Q_i xQ_i)$ soit un morphisme de N pour chaque $i\in I$ et que $\varepsilon : h \to \sum_i h\varepsilon_i$ soit un morphisme de N sur un sous-groupe $N\varepsilon$ du produit direct des groupes positifs $N\varepsilon_i$. Il suffit donc de montrer que le noyeau $E = \{h\in N : h\varepsilon = u\varepsilon\}$ de ε est réduit à {u} puisque N divise $E\circ N\varepsilon$.
Ceci est trivial quand $u\beta = QxQ$. Comme ce cas couvre celui où Q est un singleton, nous pouvons donc procéder par induction sur $Card(Q)\geq 2$ en supposant $e\neq QxQ$. Cette dernière hypothèse implique l'existence d'une partition propre $Q=Q'+Q''$ telle que $h\wedge(Q''xQ') = \emptyset$ pour chaque $h\in N$ et que, par conséquent $h \to h\wedge(Q'xQ'+Q''xQ'')$ soit un morphisme de N. Ceci permet d'écrire $u = \begin{pmatrix} a & c \\ \emptyset & b \end{pmatrix}$ où a et b sont respectivement une $Q'xQ'$ et une $Q''xQ''$ matrice idempotente. Soit $h\in E$. D'après l'hypothèse d'induction $h = \begin{pmatrix} a & x \\ \emptyset & b \end{pmatrix}$, $h^{-1} = \begin{pmatrix} a & y \\ \emptyset & b \end{pmatrix}$.

Les identités $u = u^2 = uhh^{-1}$ et $h = uhu$ donnent les relations:

$c = ac + cb = axb + ay + cb$ et

$x = axb + ax + bc$.

Donc $x = axb + c = axb + ay + cb = c$ montrant que $h = u$ et $E = \{u\}$.

Q.E.D.

Il suffit donc maintenant de vérifier le lemme dans le cas particulier où $H = N$ est positif et l'on peut même supposer pour simplifier $u\beta = QxQ$.

II.3. Tout groupe H dans M' tel que $h\beta = QxQ$ pour chaque $h \in H$ divise le groupe G.

Preuve: D'après la relation $u^2 = u$ on a $(u_{q,q})^2 \subset u_{q,q}$ pour chaque $q \in Q$, donc $u_{q,q}$ est un sous semi-groupe de G. Comme il est non vide et que G est un groupe fini, c'est un sous-groupe G_q de G.

Soit $h \in H$. La relation $uh = h$ montre que $G_q h_{q,q'} = u_{q,q} h_{q,q'} \subset h_{q,q'}$ pour chaque $q' \in Q$, c'est à dire que $h_{q,q'}$ est une union des cosets de G_q. La même chose vaut pour les entrées $h^{-1}{}_{q',q}$ de h^{-1} et la relation $hh^{-1} = u$ qui implique $h_{q,q'} h^{-1}_{q',q} \subset u_{q,q} = G_q$ montre que de fait chacune de ces entrées de h et de h^{-1} est un coset unique (non vide) de G_q.

Ceci s'applique en particulier à la matrice u elle-même et à chacune de ses entrées, $u_{q',q''}$ qui est donc à la fois un coset à droite de $G_{q'}$ et un coset à gauche de $G_{q''}$. $(q',q'' \in Q)$.

Prenons maintenant un $q_0 \in Q$ fixe et posons pour chaque $h \in H$, $h_0 = h \cap (\{q_0\}, \{q_0\})$ = la matrice obtenue en remplaçant toutes les entrées par $\emptyset$, sauf h_{q_0,q_0}. L'identité $h = uhu$ et les relations précédentes montrent que l'on a identiquement $h = uh_0u$.

Comme $\emptyset \neq h_0 h'_0 \subset (hh')_0$ pour tout $h,h' \in H$, l'application $h \to h_0$ est un morphisme injectif. Donc, enfin, H est isomorphe au groupe G'_{q_0}/G_{q_0} où le sous-groupe G'_{q_0} de G est l'union des cosets H_0 $(h \in H)$ de G_{q_0}.

Q.E.D.

Ceci achève la preuve du lemme, donc aussi de la propriété.
Les techniques restent appliquables quand H est un groupe de matrices à entrées dans 2^S où S est un semi-groupe sans idéaux propres (G est alors son groupe de Suschkewitsch). Ceci donnerait une généralisation assez immédiate de la propriété au cas où F est reconnaissable dans S à condition de considérer seulement les semi-groupes libres A^+ et B^+.

Dans le cas général, les groupes dans $\mathrm{Synt}(F\theta^{-1})$ sont soumis à des contraintes (assez peu strictes, et de nature quasiment numérique) que je

n'ai pas réussi à formuler de façon raisonnablement simple (ou non triviale). Par exemple, si S est le monoïde booleen {1,0} (qui est union de groupes!), le monoide des QxQ matrices positives à entrées dans 2^S contient le groupe symétrique sur Q : il suffit pour cela de représenter ce dernier par le monoïde des bijections et de remplacer chaque entrée vide par {0} et chaque entrée non vide par {1,0}.

III. Une application

Revenant aux notation de l'introduction, nous considérons désormais le cas où la relation θ est l'inverse d'une subtitution (rationnelle) $\theta^{-1} : B^* \to A^*$, c'est à dire d'un morphisme de B^* dans 2^{A^*}, donné par les parties reconnaissables $b\theta^{-1} \subset A^*$ ($b \in B$ où l'alphabet B est évidemment supposé fini). Pour simplifier nous ferons l'hypothèse supplémentaire que $B\theta^{-1}$ est contenu dans le semi-groupe $A^+ (=A^*\setminus\{1\})$, c'est à dire que $1 = 1\theta = 1\theta^{-1}$.

Nous désignerons par $M_2 = A^*\tau_2$ le monoïde syntactique simultané des parties $b\theta^{-1}$ ($b \in B$), par $M_1 = A^*\tau_1$ celui de $B^*\theta^{-1}$, et par M_3 le produit direct $M_1 \times 2^{M_1 \times M_2} \times M_2$.

D'après la théorie générale des produits en couronne, il est possible de munir M_3 d'une structure de monoïde ayant les deux propriétés suivantes:

(i) Tout groupe dans M_3 est produit sous-direct d'un groupe dans M_1 et d'un groupe dans M_2;

(ii) Si σ_3' est l'application envoyant chaque mot $a \in A^*$ sur $a\sigma_3' = \{(a'\sigma_1, a''\sigma_2) \in M_1 \times M_2 : a', a'' \in A^*, a'a'' = a\}$, l'application $\sigma_3 : a \to (a\sigma_1, a\sigma_3', a\sigma_2)$ est un morphisme (de semi-groupe) de A^* dans M_3.

Rappelant que F est une partie de B reconnaissable dans le groupe fini G, nous nous proposons d'établir:

III.1. Tout groupe dans le monoïde syntactique de $F\theta^{-1}$ divise le produit en couronne de G dans un groupe dans M_3.

Nous construisons d'abord en application immédiate de la théorie générale des relations rationnelles, un transducteur (standard) μ pour θ et, d'après la propriété, il suffira de vérifier que son monoide des supports M_μ divise M_3.

Contruction du transducteur.

La donnée des parties $b\theta^{-1}$ ($b \in B$) implique celle d'un ensemble minimal fini Q', d'une action $Q' \times A^* \to Q'$, de parties Q_b de Q' ($b \in B$) et d'un élément distingué $q_o \in Q'$ tels que pour chaque lettre b de B on ait

$$b\theta^{-1} = q_o^{-1} Q_b \quad (=\{a \in A^* : q_o a \in Q_b\}).$$

Nous adjoignons un nouvel élément q_+ à Q' et nous étendons l'action précédente à $Q = \{q_+\} \cup Q'$ en posant $q_+ a = \emptyset$ pour chaque $a \in A^+$.

Nous définissons maintenant pour chaque lettre a deux QxQ matrices $a\mu'$ et $a\mu''$ (à entrées dans le semi-anneau des parties de B*) par les conditions suivantes :

Pour tout $q, q' \in Q$:

$a\mu'_{q',q} = 1$ ou $\emptyset$ selon que $q'a = q$ ou non;

$a\mu''_{q',q} = \emptyset$ pour $q \neq q_o, q_+$ et, sinon,

$= b$ si $q = q_o$ ou q_+ et $q'a \in Q_b$.

De plus nous définissons les deux matrices $1\mu'$ et $1\mu''$ par les conditions :

$1\mu'_{q',q} = 1$ si $q' = q \neq q_+$;

$= \emptyset$ sinon.

$1\mu''_{q',q} = 1$ si $q' = q_o, q = q_+$;

$= \emptyset$ sinon.

L'application $\mu = \mu' + \mu''$ s'étend à un morphisme (de semi-groupe) de A* dans le semi-anneau Γ_B.

III.2 μ est un transducteur pour θ.

Preuve: Notons $a\nu$ le Q-vecteur égal à la ligne q_o de $a\mu$ ($a \in A^*$). Pour $a = 1$, toutes ces coordonnées sont $\emptyset$ sauf la dernière, c'est à dire qui est égale à $1 = 1\theta^{-1}$ d'après l'hypothèse $B\theta^{-1} \subset A^+$.

Ceci permet de procéder par induction sur la longueur des mots et il suffit de vérifier les deux formules suivantes pour $a'a$ où $a' \in A^+$, $a \in A$ en les supposant établis pour a':

(21). Pour tout $q \in Q$:

$$a'av_q = \Sigma\{b \in B^* : a'a \in b\theta^{-1}q_0^{-1}q\};$$

(22). $$a'av_{q_+} = \Sigma\{b \in B^* : a'a \in b\theta^{-1}\} = a\theta.$$

Nous utilisons le fait que par construction, la ligne q_+ de $a\mu$ est vide et nous observons que les mots $b \in B^*$ qui apparaissent dans (21) le font d'au moins l'une des deux manières suivantes:

(i) Il existe un $q' \in Q'$ et une factorisation $a = a_1a_2 (a_1, a_2 \in A^*)$ tels que

$$a_1 \in b\theta^{-1} \; ; \; q_0a_2 = q' \; ; \; q'a = q.$$

On vérifie directement que la contribution de ces mots est pour $q \in Q'$, la coordonnée q du produit $a'v.a\mu'$ et pour $q = q_+$ celle de $a'v.a\mu"$.

(ii) On a $aa' \in b\theta^{-1}$ et $q = q_0$. Comme $b\theta^{-1} \subset A^+$, il existe un $q' \in Q'$ et des factorisations $b = b_1b'$ $(b_1 \in B^*, b \in B)$ $a = a_1a_2 (a_1, a_2 \in A^*)$ tels que:

$$a_1 \in b_1\theta^{-1} \; ; \; q_0a_2 = q' \; ; \; q'a \in Q_{b'}.$$

Comme ci-dessus la contribution correspondante est la coordonnée q_0 du produit $a'v.a\mu"$.

La formule (21) résulte immédiatement de ce deuxième cas et de la définition de $\mu"$.

Q.E.D.

III.3. Le monoïde $M_\mu = A^*_{\mu\beta}$ est une image homomorphe de M_3.

Preuve: Il suffit de vérifier que pour deux mots a et a' quelconques, $a\mu\beta \neq a'\mu\beta$ implique $a\sigma_3 \neq a'\sigma_3$.

La première relation signifie que les entrées (q',q) des deux matrices sont différentes pour au moins une paire $q',q \in Q$. On peut prendre $a" \in q_0^{-1}q'$ et, posant $a_1 = a"a$, $a_1' = a"a_1'$, on a que les coordonnées q des supports des vecteurs a_1v et $a_1'v$ sont différentes. Ceci entraîne $a_1\sigma_3 \neq a_1'\sigma_3$ (donc le résultat cherché) d'après la formule (21) et la définition de $\sigma_3' : A^* \to 2^{M_1 \times M_2}$ si $q \neq q_+$ et d'après la formule (22) et $\sigma_3 = \sigma_1 \times \sigma_3' \times \sigma_2$ si $q = q_+$.

Q.E.D.

Ceci conclut la preuve de II.1. A titre d'exemple, nous considérons le cas particulier suivant.

III.4. Soient $r \geq 1$ et P l'ensemble générateur minimum d'un sous-monoide de $P^* \in Rat(A^*)$ de A^*. Tout groupe dans le monoide syntactique de $(P^r)^*$ divise le produit en couronne du groupe cyclique $Z_{(r)}$ dans un produit direct de groupes dans le monoïde syntactique de P^*.

Preuve: Prenons $B = \{b\}$ et $\rho : B^* \to G = Z_{(r)}$ tel que b_ρ soit un générateur de ce groupe. Si θ^{-1} est la substitution telle que $b\theta^{-1} = P$, on a $(P^r)^* = 1\rho^{-1}\theta^{-1}$ et le résultat est encore une conséquence de la théorie des produits en couronne puisque d'après celle-ci chaque groupe dans le monoïde syntactique de P divise un groupe dans Synt(P*) quand P est l'ensemble générateur minimum.

Q.E.D.

En particulier tout groupe dans $Synt(P^r)^*$ est résoluble quand ceci est vrai pour Synt(P*).