Société Mathématique de France
Astérisque 38-39 (1976) p.247-251

SUR UNE CARACTÉRISATION DES PARTIES RECONNAISSABLES D'UN MONOÏDE LIBRE

par

M.P. SCHÜTZENBERGER

1.- INTRODUCTION

Une partie S d'un monoïde M est reconnaissable ssi il existe un morphisme φ de M dans un monoïde fini pour lequel $S = S\varphi\varphi^{-1}$. Une caractérisation remarquable de ces parties est donnée par S. Eilenberg (vol. A ; chap. XIII, Prop. 12.3) dans son traité "Automata, Languages and Machines". On se propose ici de montrer que dans le cas où M est le monoïde libre A^* (engendré par l'ensemble A), on peut légèrement affaiblir les hypothèses de cet énoncé. Plus précisément, nous établirons la :

PROPRIÉTÉ .- Une condition nécessaire et suffisante pour que la partie S de A^* soit reconnaissable est l'existence d'un entier naturel n et de deux applications $\lambda : A^* \to \mathbb{N}^n$ et $\rho : A^* \setminus A^{n+1} A^* \to \mathbb{N}^n$ satisfaisant la condition que pour chaque $a \in A^*$, $f \in A^* \setminus A^{n+1} A^*$ le produit scalaire $a\lambda . f\rho$ ait la valeur 1 ou 0 selon que $af \in S$ ou non.

Il est trivial que la condition est nécessaire. En effet, soit $S = S\varphi\varphi^{-1}$ où φ est un morphisme dans un monoïde P ayant $n < \infty$ éléments. On peut considérer P comme un monoïde d'applications de P dans lui-même et associer à chaque mot a de A^* le P-vecteur ligne $a\lambda$ (resp. colonne $a\rho$) tel que pour chaque $p \in P$ sa coordonnée $a\lambda_p$ (resp. $a\rho_p$) soit égale à 1 ou à 0 selon que $a\varphi = p$ ou non (resp. $a\varphi . p \in S$ ou non). On a donc $a\lambda . f\rho = 1$ ou 0 puisque $a\lambda$ a exactement une coordonnée non nulle et $a\lambda . f\rho = 1$ ssi $a\varphi . f\varphi \in S\varphi$.

Nous ne nous occuperons plus désormais que de la réciproque.

2.- VÉRIFICATION DE LA RÉCIPROQUE

Nous supposons remplies les conditions de l'énoncé. On pose $F = A^* \setminus A^{n+1} A^*$ et on note σ la fonction caractéristique de S ($a\sigma = 1$ ou 0 selon que $a \in S$ ou non pour chaque mot a de A^*). Il est clair que l'on peut supposer qu'aucune des coordonnées des vecteurs $a\lambda$ ($a \in A^*$) ou $f\rho$ ($f \in F$) n'est identiquement nulle. Comme $(af)\sigma = a\lambda . f\rho$, ceci entraîne que ces vecteurs aient toutes leurs coordonnées égales à 1 ou à 0.

Définissons deux relations d'équivalence sur A^* par les conditions : $a \sim a'$ (resp. $a(\sim)a'$) ssi $(af)\sigma = (a'f)\sigma$ pour chaque $f \in A^*$ (resp. $f \in F$).

Il est bien connu que chaque relation $a \sim a'$ implique $ab(\sim)a'b$ et $ab \sim a'b$ pour tout $b \in A^*$ et que réciproquement $ab(\sim)a'b$ pour tout $b \in A^*$ entraîne $a \sim a'$. L'essentiel de la preuve est la remarque suivante :

2.1.- La relation $a(\sim)a'$ implique $a \sim a'$.

Preuve.- Pour chaque indice $j \leqslant n$, soit r_j le F-vecteur ligne dont chaque coordonnée f est égale à la coordonnée j du n-vecteur colonne $f\rho$ ($f \in F$). Le sous-module R de $\mathbb{Z}^F$ sous-tendu par les r_j ($1 \leqslant j \leqslant n$) a donc dimension au plus n.

Soit, d'autre part, $a\alpha$ pour chaque mot a de A^* le F-vecteur ligne dont chaque coordonnée f est égale à $(af)\sigma$. Comme $(af)\sigma = a\lambda . f\rho$ ce vecteur est égal à la combinaison linéaire $\sum_j a\lambda_j . r_j$ des vecteurs r_j et appartient donc à R. Pour la même raison, on a que chaque relation $ab(\sim)a'b$ équivaut à $(ab)\alpha - (a'b)\alpha = 0$.

Supposons donc $a(\sim)a'$ et qu'il existe un mot b pour lequel $(ab)\alpha - (a'b)\alpha \neq 0$. On peut prendre $b = b_1, b_2, \ldots, b_m$ $(m \geq 1 ; b_1, b_2, \ldots, b_m \in A)$ de longueur minimale, ce qui fait que si $f \in F$ est tel que les coordonnées $(ab)\alpha_f$ et $(a'b)\alpha_f$ sont différentes, on a $f \in A^n$. En effet, sinon on aurait : $(ab')\alpha_{f'} \neq (a'b')\alpha_{f'}$ avec $b' = b_1, \ldots, b_{m-1}$ et $f' = b_m f \in F$.

Soit π_j le morphisme de R dans lui-même annulant les coordonnées correspondant aux $f' \in F$ de longueur $> n-j$ $(0 \leq j \leq n)$. On vient de montrer que $w_o = (ab)\alpha - (a'b)\alpha$ satisfait $w_o \pi_1 = 0$ et $w_o \pi_o \neq 0$.

Plus généralement, soit $f = a_1 a_2 \ldots a_n$ $(a_1, a_2, \ldots, a_n \in A)$ et pour chaque i, $b_i = b a_1 \ldots a_i$, $w_i = (ab_i)\alpha - (a'b_i)\alpha$. Si $f' \in F$ est de longueur au plus $n-i$, on a l'égalité $(ab_i)\alpha_{f'} = (ab)\alpha_{f''}$ avec $f'' = a_1 \ldots a_i f' \in F$ puisque la valeur commune des deux membres est 1 ou 0 selon que $ab_i f' = abf''$ appartient ou non à S. La même observation s'applique aux $(a'b_i)\alpha$ et il en résulte immédiatement que l'on a $w_i \pi_{i+1} = 0$; $w_i \pi_i \neq 0$ pour $i = 0, 1, \ldots, n$.

Ceci montre que les w_i constituent un système de $n+1$ vecteurs linéairement indépendants de R en contradiction avec $\dim R \leq n$. Par conséquent, $ab(\sim)a'b$ pour tout $b \in A^*$, c'est-à-dire $a \sim a'$.

Q.E.D.

D'après la définition même de cette équivalence, S est une union de classe de $\sim$. Comme cette relation admet la multiplication à droite

il suffit, d'après la théorie classique, de vérifier qu'elle n'a qu'un nombre fini de classes. Pour cela, supposons que $a\lambda = a'\lambda$. Pour chaque $f \in F$, on a $(af)\sigma = (a'f)\sigma$, c'est-à-dire que $a(\sim)a'$ et donc $a \sim a'$ comme on vient de le montrer. Autrement dit, chaque classe de $\sim$ est une union de parties de la forme $v\lambda^{-1}$ où $v \in V = \{a\lambda : a \in A^*\}$, ce qui conclut la preuve puisque V a au plus 2^n éléments.

Q.E.D.

3.- CAS AMBIGU

Nous considérons maintenant une formulation un peu différente de la propriété et nous supposons qu'il existe n paires de parties $X'_i \subset A^*$ et $Y'_i \subset A^* \setminus A^{2^n} A^* = F'$ telles que, pour chaque $(a,f) \in A^* \times F'$, on ait $af \in S$ ssi $a \in X'_i$ et $f \in Y'_i$ pour au moins un indice i.

Observation.- Sous les hypothèses indiquées, S est une partie reconnaissable.

Preuve.- Pour chaque $a \in A^*$, soit $a\lambda' = \{i \in [n] : a \in X_i\}$ où $[n] = \{1 < 2 < \ldots < n\}$. Posons $m = \mathrm{Max}\ \{\mathrm{Card}\ a\lambda' : a \in A^*\}$ et définissons Q comme l'ensemble des paires de la forme $(i,\overline{q})$ où $i \in [n]$ et où $\overline{q}$ est une partie de $[i-1]$ ($=\emptyset$ pour $i=1$) ayant au plus $m-1$ éléments. Puisque Q est en bijection avec les parties non vides de $[n]$ ayant m éléments au plus, on a $\mathrm{Card}\, Q \leqslant 2^n - 1$.

A chaque mot a de A^*, on associe le Q-vecteur ligne $a\lambda$ par la condition que si $q = (i,\overline{q}) \in \overline{Q}$, sa coordonnée $a\lambda_q$ soit 1 ou 0 selon que l'on a ou non $i \in a\lambda'$ et $\overline{q} = a\lambda' \cap [i-1]$.

De façon analogue, si $f \in F$, on pose $f\rho' = \{j \in [n] : f \in Y_j\}$ et on définit le Q-vecteur colonne $f\rho$ par la condition que $f\rho_q = 1$ ou 0 selon que l'on a ou non $j \in f\rho'$ et $\overline{q} \cap f\rho' = \emptyset$ $(q = (j,\overline{q}))$.

Considérons un produit scalaire $s = a\lambda . f\rho$. Par hypothèse $af \notin S$ ssi l'intersection $I = a\lambda' \cap f\rho'$ est vide et dans ce cas $s = 0$ d'après la définition des vecteurs $a\lambda$ et $f\rho$. Dans le cas contraire où I est non vide, soit i son plus petit élément. Si $\overline{q} = [i-1] \cap a\lambda'$, les vecteurs $a\lambda$ et $f\rho$ ont tous les deux leur coordonnée $(i,\overline{q})$ égale à 1, et par conséquent, $s \geqslant 1$. De fait, on a exactement $s = 1$. En effet, suppsons que $a\lambda_{q'} = a\rho_{q'} = 1$ pour un certain $q' = (i',\overline{q}')$ de Q. On doit avoir $i' \in I$ et $\overline{q}' = [i'-1] \cap a\lambda'$ (d'après la définition de λ). Ceci implique $i' = i$ et donc $\overline{q}' = \overline{q}$ puisque $i' \geqslant i$ (d'après le choix initial de $i = \mathrm{Min}\, I$) ou en cas d'inégalité stricte, on aurait $i \in \overline{q}' \cap f\rho'$ en contradiction avec $f\rho_{q'} = 1$ (d'après la définition de ρ). Par conséquent, on a identiquement $(a\,f)\sigma = a\lambda . f\rho$ pour tout $a \in A^*$, $f \in A^* \setminus A^{2^n} A^*$ et comme $\operatorname{Card} Q < 2^n$, le résultat découle de la Propriété en remplaçant n par Card Q.

Q.E.D.

On notera que dans la Propriété il n'est pas possible de remplacer F par $A^* \setminus A^{n'+1} A^*$ où $n' < n$. Considérons, en effet, le cas où A consiste en une seule lettre a, et, posant $D = \{2^p : p \in \mathbb{N}\}$, définissons les applications λ et ρ dans $\mathbb{N}^2$ par :

$a^m\lambda = (1,0)$ si $m \in D$; $= (0,1)$ si $m \in D+1$; $= (0,0)$ dans les autres cas.

$$a\rho = (0,1) \; ; \; a^2\rho = (1,0).$$

On a donc que $a^{m+2}\sigma = a^{m+1}\lambda . a\rho = a^m \lambda . a^2\rho$ est égal à 1 ou à 0 selon que $m \in D+2$ ou non, ce qui donne la partie $S = 1\sigma^{-1} = \{a^{2+d} : d \in D\}$ qui n'est évidemment pas reconnaissable.

* * *

Marcel Paul SCHÜTZENBERGER
Département de Mathématiques
Université de Paris VII
Tour 45-55
2 place Jussieu
75005 PARIS