Séminaire Dubreil.
Algèbre et théorie
des nombres

Marcel P. Schützenberger

Un problème de la théorie des automates

Séminaire Dubreil. Algèbre et théorie des nombres, tome 13, n° 1 (1959-1960), exp. n° 3, p. 1-6

<http://www.numdam.org/item?id=SD_1959-1960__13_1_A3_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
13e année, 1959/60, n° 3

23 novembre 1959

UN PROBLÈME DE LA THÉORIE DES AUTOMATES

par Marcel P. SCHÜTZENBERGER

Un "one way, one tape" [2] automate A est un algorithme destiné à classer les mots du monoïde libre F_X engendré par $X = \{x\}$, fini, d'après le mécanisme suivant :

A est donné par

1° Un ensemble fini $S = \{s\}$ avec un élément s_0 et un sous-ensemble S_1, distingués.

2° Une application $(S, X) \longrightarrow S$ (notée sx).

Cette application se prolonge de façon naturelle en une représentation de F_X par un monoïde d'applications de S dans lui-même et on dit que $f \in F_X$ est <u>accepté</u> ou non selon que $s_0 f$ appartient ou non à S_1. L'ensemble F' des mots qui peuvent être acceptés par un automate fini a été caractérisé par S. C. KLEENE [1] au moyen d'opérations logiques.

Dans cet exposé, nous montrons que la somme formelle $\sum \{f : f \in F'\}$ peut, dans un certain sens, être considérée comme une fonction "rationnelle" des $x \in X$. Nous généralisons ensuite cette propriété en montrant que si S au lieu d'être fini est le produit direct d'un ensemble fini par Z (le groupe additif des entiers) et si l'application $(S, X) \longrightarrow S'$ et le sous-ensemble S_1 sont définis de façon convenable, alors la somme correspondante est dans un certain sens une fonction "algébrique".

Cette terminologie se justifie par le fait que si les variables x étaient des variables commutatives ordinaires, les sommes correspondantes seraient effectivement rationnelles ou algébriques.

Indépendamment de toute notion d'automate, les sous-ensembles $F' \subset F_X$ considérés peuvent être définis comme des unions finies des sous-ensembles tels que $F' = \varphi^{-1} g$ où g est un élément d'un certain monoïde quotient φF_X de F_X. Quand S est fini, φF_X l'est aussi ; la généralisation que nous proposons contient comme cas particulier celui où φF_X est l'extension de Z par un groupe fini.

NOTATION.I. - Ω un anneau unital ; Ω_n l'anneau des $n \times n$ matrices sur Ω. ; $A_X(\Omega)$, la Ω-algèbre associative libre engendrée par $X = \{x\}$ fini ;

Π_p le projecteur de $A_X(\Omega)$ sur le sous-module dont une base est l'ensemble des $f \in F_X$ de longueur $\leqslant p$.

On complète $A_X(\Omega)$ en une algèbre de série (infinies) $\bar{A}_X(\Omega)$ en posant ab = l'élément unique c tel que, pour tout p , $\Pi_p c = \Pi_p(\Pi_p a \; \Pi_p b)$. Si $a \in \bar{A}_X(\Omega)$ est tel que $\Pi_0 a = 0$, on définit $(1 - a)^{-1}$ comme l'élément unique c tel que, pour tout p , $\Pi_p c = \Pi_p(1 + \sum_{p'=1}^{p} (\Pi_p c)^{p'})$. On vérifie que $(1 - a)(1 - a)^{-1} = (1 - a)^{-1}(1 - a) = 1$ et que $(1 - a)b = 1$ ou $b(1 - a) = 1$ entraînent $b = (1 - a)^{-1}$.

On note $R_X(\Omega)$ la plus petite sous-algèbre de $\bar{A}_X(\Omega)$ qui contienne $A_X(\Omega)$ et qui soit telle que $r \in R_X(\Omega)$ entraîne $(1 + \Pi_0 r - r)^{-1} \in R_X(\Omega)$. On a la propriété suivante.

PROPRIÉTÉ 1. - Une condition nécessaire et suffisante pour que $r \in R_X(\Omega)$ est qu'il existe un homomorphisme γ_r de F_X dans Ω_n $(n < \infty)$ tel que

$$r = \Pi_0 r + \sum_{f \in F_X ; f \neq e_{F_X}} f(\gamma_r f)_{1,n}$$

où $(\gamma_r f)_{1,n}$ désigne l'élément à l'intersection de la première ligne et de la n-ième colonne de la matrice $(\gamma_r f)$.

La condition est nécessaire. Ceci est évident quand $r \in A_X(\Omega)$. Supposons que le résultat soit vrai pour r et que $\Pi_0 r = 0$; si $s = (1 - r)^{-1}$, on obtient γ_s comme l'homomorphisme prolongeant les applications $\gamma_s x$ $(x \in X)$ où $(\gamma_s x)$ est la $n \times n$ matrice, somme de $(\gamma_r x)$ et d'une matrice dont toutes les colonnes sont nulles sauf la première qui est égale à la n-ième colonne de $(\gamma_r x)$.

De la même manière, si $\gamma_r : F_X \longrightarrow \Omega_n$; $\gamma_{r'} : F_X \longrightarrow \Omega_{n'}$, $\Pi_0 r = \Pi_0 r' = 0$ $s = r\omega + r'\omega'$; $(\omega , \omega' \in \Omega)$; $t = rr'$, on obtient $\gamma_s : F_X \longrightarrow \Omega_{n+n'+2}$ et $\gamma_t : F_X \longrightarrow \Omega_{n+n'+1}$ en prolongeant les applications.

$$(\gamma_s x) = \begin{pmatrix} 0 & (\gamma_r x)_1 & (\gamma_{r'} x)_1 & \alpha \\ 0 & (\gamma_r x) & 0 & (\gamma_r x)^n \omega \\ 0 & 0 & (\gamma_{r'} x) & (\gamma_{r'} x)^{n'} \omega' \\ 0 & 0 & 0 & 0 \end{pmatrix} ; \quad (\gamma_t x) = \begin{pmatrix} (\gamma_r x) & (\gamma_r x)^n & 0 \\ 0 & 0 & (\gamma_{r'} x)_1 \\ 0 & 0 & (\gamma_{r'} x) \end{pmatrix}$$

(où les notations $(\,)_1$ et $(\,)^n$ (ou $(\,)^{n'}$) désignent respectivement la première ligne, la n-ième (ou la n'-ième) colonne de la matrice correspondante et où $\alpha = (\gamma_r x)_1^n \omega + (\gamma_{r'} x)_1^{n'} \omega'$).

La condition est suffisante. Soit U une $n \times n$ matrice (u_{ij}) dont les éléments sont n_2 indéterminés ; U' la matrice obtenue en supprimant la n-ième ligne et la n-ième colonne de U ;

$$W = I_n + \sum_{p>0} U^p \; ; \quad W' = I_{n-1} + \sum_{p>0} U'^p \quad .$$

On a : $w_{n,n} = (1 - u_{n,n} - \sum_{j,j'<n} u_{n,j}\, w'_{j,j'}\, u_{j',n})^{-1}$ et pour tout i , $i' < n$

$$w_{i,n} = (\sum_{j<n} w'_{i,j}\, u_{j,n})\, w_{n,n} \; ; \quad w_{n,i'} = w_{n,n}(\sum_{j'<n} u_{n,j'}\, w_{j',i'})$$

$$w_{i,i'} = w'_{i,i'} + w_{i,n}(w_{n,n})^{-1} w_{n,i'} \quad .$$

Tous les calculs étant effectués dans $R_{\{u_{i,j}\}}(\Omega)$.

Il en résulte immédiatement que si $U \in R_{\mathcal{L}_n}$, chacune des entrées $(U)_{i,i'}$ de U appartient à $R_{\mathcal{L}}$. Par conséquent, $1 + \sum_{f \in F_X,\, f \neq \ell_{F_X}} f(\gamma_r f)_{1,n}$ étant égal à $((1 - \sum_{x \in X} x(\gamma_r x)^{-1})_{1,n}$ appartient à $R_X(\Omega)$.

REMARQUE. - Soit R_X^{pos} le sous-ensemble de $\bar{A}_X(Z)$ défini à partir de X par les seules opérations d'addition, de multiplication et de l'opération $r \longrightarrow (1 - r)^{-1} - 1$ quand $r \in R_X^{pos}$, $\pi_0\, r = 0$. En utilisant l'identité : $(1 - a + b)^{-1} = (1 - a - b(1 - a)^{-1} b)^{-1} (1 - b(1 - a)^{-1})$ on vérifie que tout $s \in R_X(Z)$ peut être écrit sous la forme $s = r - r'$ avec r , $r' \in R_X^{pos}$. Par construction, si $r \in R_X^{pos}$, toutes les matrices $\gamma_r f$ $(f \in F_X)$ ont leurs entrées non négatives ; il existe donc un monoïde quotient fini $\varphi_r F_X$ tel que $(\gamma_r f)_{1,n} \neq 0$ si et seulement si $\varphi_r f$ appartient à un certain sous-ensemble de $\varphi_r F_X$.

II. - Soit $Y = X \cup U$ où $U = \{u_j\}_{j=1,2,\ldots,m}$.

Soient r_1 , r_2 , ... , $r_m \in R_Y(\Omega)$ tel que

$$r_1 = r_2 = \ldots = r_m = 0 \qquad \text{quand} \qquad x_1 = x_2 = \ldots = x_n = 0$$

et

$$r_1\, r_2 \ldots r_m \neq 0 \qquad \text{quand} \qquad u_1 = u_2 = \ldots = u_m = 0 \quad .$$

Dans ces conditions, si θ' est une application de U dans $\bar{A}_X(\Omega)$ telle que $\pi_0\, \theta' u = 0$, θ'_n l'application $\pi_n \circ \theta$ et θ et θ_n les homomorphismes $\bar{A}_Y(\Omega) \longrightarrow \bar{A}_X(\Omega)$ qui les prolongent, on a, pour tout n et $n' \geq n$, $\pi_{n+1}(\theta_n\, r_j) = \pi_{n+1}(\theta_{n'}\, r_j)$. Les "équations" $u_j = r_j$ et les séries formelles

u_j en les x peuvent donc être "résolues" en calculant par des opérations rationnelles les coefficients successifs $\Pi_p u_j$ et l'on dira que chacune de ces séries est un "élément algébrique" de $\bar{A}_X(\Omega)$. On désignera par $S_X(\Omega)$ la plus petite sous-algèbre de $\bar{A}_X(\Omega)$ qui contienne tous les éléments algébriques et qui soit telle que $s \in S_X(\Omega)$ entraîne $(1 + \Pi_0 s - s)^{-1} \in S_X(\Omega)$.

III. - Soit $\varphi : F_X \longrightarrow G$ un homomorphisme de F_X dans un monoïde fini et $\beta_1 : (G , X) \longrightarrow Z$ une application quelconque.

On prolonge β_1 en un "coset mapping" $\beta : (G , F_X) \longrightarrow Z$ en posant $\beta(g ; e_{F_X}) = 0$ et inductivement

$$\beta(g ; fx) = \beta(g ; f) + \beta_1(g\varphi f ; x) \quad .$$

Les définitions précédentes déterminent sur (F_X , Z) une structure de monoïde avec $(f , a)(f' , a') = (ff' , a + \beta(\varphi f ; f') + a')$; $(f ; a) \equiv f' ; a')$ et seulement si $\varphi f = \varphi f'$ et $a = a'$.

Soit $h^+ = \sup \beta_1(g ; x)$; $h^- = \inf \beta_1(g , x)$ $(g \in G , x \in X)$, et pour tout $g , g' \in G$; $0 \leqslant a , b \leqslant h^+$ les éléments suivants de $\bar{A}_X(Z)$

$$B^+_{g,g'} = \sum \left\{ f : f \in F_X ; g\varphi f = g' ; \beta(g , f) = 0 ; \beta(g ; f') \geqslant 0 \right\}$$
pour tous les facteurs à gauche propres f' de f

$$A^+_{g,g'}(a , b) = \sum \left\{ f : f \in F_X ; g\varphi f = g' ; a + \beta(g , f) = b ; a + \beta(g , f') > 0 \right\}$$
pour tous les facteurs à gauche propres f' de f

On a les équations $(c = \inf(a , b))$

$$(1) \quad A^+_{g,g'}(a , b) = \sum_{0<a'<c} \sum_{g'',g'''} A^+_{g,g''}(a - a' , 0) B^+_{g'',g'''} A^+_{g''',g'}(0 , b - a')$$
$$+ \left(A^+_{g,g'}(0 , b - a) \text{ ou } A^+_{g,g'}(a - b ; 0) \right.$$
$$\left. \text{selon que } b \geqslant 0 \text{ ou non.} \right)$$

$$(2) \quad A^+_{g,g'}(0 , a) = \sum_{x \in X^+_g} x \, A_{g\varphi x,g'}(\beta(g , x) , a)$$

où $X^+_g = \left\{ x : x \in X ; \beta_1(g , x) > 0 \right\}$.

$$(2)' \quad A^+_{g,g'}(a , 0) = \sum A_{g,g''}(a , b) \, x$$

où cette sommation est étendue à tous les triples $b \in Z$, $x \in X$, $y'' \in G$ tels que $-\beta_1(g'' , x) = b > 0$, $g''\varphi x = g'$.

Finalement si (B^+) et (A^+) désignent des matrices carrées dont l'ensemble

d'indice est en correspondance biunivoque avec G et qui sont telles que $(B^+)_{g,g'} = B^+_{g,g'}$; $(A^+)_{g,g'} = A^+_{g,g'}(0\ ,\ 0)$; on a évidemment :

$$(B^+) = (I - (A^+))^{-1} \qquad (3)$$

Éliminant les $A^+_{g,g'}(a\ ,\ b)$ $(ab \neq 0)$ au moyen de (1), il résulte de (2), (2)' et (3) que les $A^+_{g,g'}(0\ ,\ b)$, les $A^+_{g,g'}(a\ ,\ 0)$, les $B^+_{g,g'}$ et finalement les $A^+_{g,g'}(a\ ,\ b)$ appartiennent tous à $S_X(Z)$.

Ceci naturellement vaudrait aussi bien pour les éléments $A^-_{g,g}(a\ ,\ b)$ $(h^- \leqslant a\ ,\ b \leqslant 0)$ ou $B^-_{g,g'}$ définis de façon symétrique.

Soit enfin $K = \{k\}$ un ensemble en correspondance biunivoque avec les paires $(g\ ,\ c)$, $g \in G$; $h^- \leqslant c \leqslant h^+$. On considère les $K \times K$ matrices (X) et (A) avec

$$(X)_{k,k'} = x \in X \text{ si } k = (g\ ,\ c)\ ;\ k' = (g'\ ,\ c')\ \text{ et } g\varphi x = g'\ ;$$
$$cc' \leqslant 0\ ;\ c \neq 0\ ;\ c + \beta_1(g\ ,\ x) = c'$$
$$= 0, \text{ autrement.}$$
$$(A)_{k,k'} = A^+_{g,g'}(a\ ,\ b) \text{ si } k = (g\ ,\ a)\ ;\ k' = (g'\ ,\ b)\ ;\ 0 \leqslant a\ ,\ b \leqslant h^+\ ;$$
$$= A^-_{g,g'}(a\ ,\ b) \text{ si } k = (g\ ,\ a) : k' = (g'\ ,\ b)\ ;\ h^- \leqslant a\ ,\ b \leqslant 0\ ;$$
$$= 0 \text{ autrement.}$$

Finalement si $(B) = (I - (A)(X))^{-1}$ tous les éléments de (B) appartiennent à $S_X(Z)$.

En particulier, ceci est vrai des sommes $B_{g'c} = \sum \{f \in F_X : \varphi f = g'\ ; \beta(e_{F_X}\ ,\ f) = c\}$ qui correspondent par construction à $k = (e_{F_X}\ ,\ 0)$; $k' = (g'\ ,\ c)$

REMARQUE. - Le résultat ne se généralise pas au cas où β serait un "coset mapping" de G, fini, dans un groupe abélien de dimension $\geqslant 2$ et où l'on chercherait la somme

$$\sum \{f : \varphi f = g\ ;\ \beta(e_{F_X}\ ,\ f) = 0\}$$

Considérons en effet le cas où φ est trivial ($\varphi f = e_G$ pour tout f) et où, X étant égal à $\{x_1\ ,\ x_2\ ,\ x_3\}$, on a :

$$\beta(x_1) = (0\ ,\ 1)\ ;\ \beta(x_2) = (1\ ,\ 0);\ \beta(x_3) = (-1\ ,\ -1) \qquad .$$

Dans ce cas, si α désigne l'homomorphisme de $\bar{A}_X$ dans l'algèbre des séries formelles en les variables commutatives t_1, t_2 et t_3, on a :

$$\alpha_s = \alpha_\Sigma\{f : \beta(f) = 0\} = (4\pi)^{-2} \int_0^{2\pi}\int_0^{2\pi} (1 - t_1 \exp iu - t_2 \exp iv - t_3 \exp -i(u+v))^{-1}\, du\, dv \quad ;$$

$$= 1 + \sum_{p>0} (3p)!\, (p!)^{-3}\, (t_1 t_2 t_3)^p \quad .$$

Quand $t_1 = t_2 = t_3 = 1/3\ t$, cette fonction a, pour $t \longrightarrow 1$, une singularité non algébrique puisque

$$\frac{(3n)!}{(n!)^3 3^{3n}} \sim \frac{1}{2\pi n} \quad .$$

Donc, a fortiori, $s \notin S_X(Z)$.

BIBLIOGRAPHIE.

[1] KLEENE (S. C.). - Representation of events in nerve nets and finite automata, Automata studies, p. 3-41. - Princeton, Princeton University Press, 1956 (Annals of mathematical Studies, 34).

[2] RABIN (M. O.) and SCOTT (D.). - Finite automata and their decision problems, IBM Research J., t. 3, 1959, p. 114-117.