Séminaire SCHÜTZENBERGER-LENTIN-NIVAT
(Problèmes mathématiques
de la Théorie des automates)
Année 1969/70, n° 5, 4 p.

9 décembre 1969

UNE APPLICATION DE LA THÉORIE DE LA DÉCOMPOSITION DES MONOÏDES

par Marcel P. SCHÜTZENBERGER

1. Introduction.

Etant donnés un alphabet (fini ou non) X, et une famille $\mathfrak{M}$ de monoïdes, désignons par $\mathfrak{M}(X)$ la famille de toutes les parties de X^* de la forme $Y^* \cap M' \mu^{-1}$, où Y est une partie finie de X, μ un morphisme de X^* dans un monoïde $M \in \mathfrak{M}$, et M' une partie de M.

On se propose de caractériser $\mathfrak{M}(X)$ par une traduction à peu près directe de la théorie de la décomposition des monoïdes, dans le cas où $\mathfrak{M}$ est la famille de tous les monoïdes finis tels que leurs groupes appartiennent à une famille donnée $\mathcal{G} \neq \emptyset$ de groupes finis, fermée par produit en couronne, et contenant les diviseurs de ses membres.

Pour ce faire, on supposera X infini, et, étant donnés une famille $\mathfrak{A}$ de parties de X^*, et deux parties finies Y, $Z \subset X$, on désignera par $\Lambda(\mathfrak{A})$ la famille des substitutions $\lambda : Z^* \to Y^*$ satisfaisant les deux conditions suivantes :

- $Z\lambda$ est non ambigu ;
- Il existe une partition $Y = Y_1 \cup Y_2$ telle que, pour chaque $z \in Z$, $z\lambda$ soit une union de parties de la forme $A_y\, y$, où $y \in Y_1$, $A_y \subset Y_2^*$, $A_y \in \mathfrak{A}$.

Ceci posé, on vérifiera la propriété :

Propriété. - $\mathfrak{M}(X)$ est la plus petite famille $\mathfrak{A}$ de parties de X^* telle que :

(i) Toute partie finie non ambigue de X^* appartient à $\mathfrak{A}$;

(ii) $\mathcal{G}(X) \subset \mathfrak{A}$;

(iii) $\mathfrak{A}$ est fermée par les opérations polynomiales non ambigues (i. e., si A, $B \in \mathfrak{A}$,

$$A \cup B \text{ non ambigu} \implies A \cup B \in \mathfrak{A} ,$$

$$AB \text{ non ambigu} \implies AB \in \mathfrak{A}) ;$$

(iv) Si Y et Z sont deux parties finies de X, $\lambda \in \Lambda(\mathfrak{A})$, $B \in \mathfrak{A}$, $B \subset Z^*$, alors $B\lambda \in \mathfrak{A}$.

2. Vérification de $\mathfrak{A} \subset \mathfrak{M}(X)$.

Soit $A \in \mathfrak{A}$. Il résulte immédiatement de la définition de $\mathfrak{S}(X)$ et de $\mathfrak{A}$ qu'il existe une partie finie $V \subset X$ telle que $A \subset V^*$. De plus, A est non ambigu par définition, si A est fini, s'il appartient à $\mathfrak{S}(X)$, ou s'il est union ou produit de deux autres parties de $\mathfrak{A}$. Si A est obtenu par substitution $A = B\lambda$ ($\lambda : Z^* \to Y^*$, $\lambda \in \Lambda(\mathfrak{A})$, $B \subset Z^*$, non ambigu), A est encore non ambigu, puisque $Z\lambda \subset Y_2^* Y_1$, $Y_1 \cap Y_2 = \emptyset$, implique que tout mot de $Z^* \lambda$ ait au plus un facteur gauche dans $Z\lambda$.

Considérant le monoïde syntactique M de A dans V^* , il suffit donc de vérifier que tout groupe dans M appartient à $\mathfrak{S}$. Ceci est clair, si A est fini ou appartient à $\mathfrak{S}(X)$. Le même résultat découle d'un énoncé connu, si $A = B \cup C$ ou $= BC$, où B , $C \in \mathfrak{M}(X)$. Il suffit donc de considérer le cas où $A = B\lambda$, avec $\lambda : Z^* \to Y^*$, $\lambda \in \Lambda(\mathfrak{M}(Y))$, $B \in \mathfrak{M}(Z)$.

Adjoignant au besoin une lettre supplémentaire à Z , il est loisible de supposer que $Z\lambda = Y_2^* Y_1$.

Considérons les parties $A_y \subset Y_2^*$ $(y \in Y_1)$ intervenant dans la définition de λ . Chacune d'elles a son monoïde syntactique dans $\mathfrak{M}$. Comme Y_1 est fini, il existe donc un monoïde $P \in \mathfrak{M}$, et un morphisme $\pi : Y^* \to P$ tel que chaque A_y soit de la forme $P_y \pi^{-1}$ $(P_y \subset P)$.

Soit, d'autre part, $\chi : Z^* \to Q$ le monoïde syntactique de $B \subset Z^*$.

Nous définissons un morphisme ρ de Y^* dans le monoïde des applications $Q \times P \to Q \times P$ en posant, pour chaque $(q , p) \in Q \times P$, $y \in Y$,

$$\begin{aligned} (q , p)y &= (q , p . y\pi) , \quad \text{si } y \in Y_2 , \\ &= (q . z\chi , 1) , \quad \text{si } y \in Y_1 , \\ & p \in P_y , \qquad A_y\, y \subset z\lambda . \end{aligned}$$

Par construction, $B\lambda$ est image inverse d'une partie du monoïde $R = Y^* \rho$, et R est un sous-monoïde du produit en couronne $Q \circ \overline{P}$, où $\overline{P}$ est obtenu en "ajoutant les constantes au t. m. (P , P) " (c'est-à-dire, où $\overline{P}$ est isomorphe au quotient du produit libre $P \star u = P'$ par les relations $p'u \equiv u$ $(p' \in P')$). Il est connu que Q , $P \in \mathfrak{M}$ implique $\overline{P} \in \mathfrak{M}$ et $Q \circ P \in \mathfrak{M}$, et le résultat est donc établi.

3. Vérification de $\mathcal{M}(X) \subset \mathcal{A}$.

Considérons $A \in \mathcal{M}(X)$. Par hypothèse, il existe une partie finie $Y \subset X$, un monoïde $M \in \mathcal{M}$, et un morphisme $\mu : Y^* \to M$, tels que A soit une union de parties de la forme $m\mu^{-1}$ $(m \in M)$. Sans perte de généralité, on supposera désormais que $A = m\mu^{-1}$, et on prouvera $A \in \mathcal{A}$ par induction sur Card M , en éliminant d'abord trois cas particuliers.

(1) M est un groupe. - La conclusion $A \in \mathcal{A}$ résulte immédiatement de $\mathcal{G}(X) \subset \mathcal{A}$.

Comme $\{1\}$ est un groupe dans $\mathcal{G}$, ceci couvre le premier cas de l'induction. Il en résulte de plus que $Z^* \in \mathcal{A}$, pour toute partie finie Z de X , puisque $Z^* = 1\nu^{-1}$, où ν est le morphisme de Z^* sur $\{1\}$.

(2) M est cyclique. - On a $\mu = \psi\mu'$, où $\psi : Y^* \to \underline{N}$ et $\mu' : \underline{N} \to M$ sont deux morphismes. Donc, il existe p , $q \in \underline{N}$ tels que

$$A = (p + q\underline{N})\psi^{-1} \quad (= A(p , q)) \quad ,$$

où, en outre, $\underline{Z}_q \in \mathcal{G}$, en convenant que $\underline{Z}_0 = \{0\}$.

Si $0 = p = q$, ou si $q > 0$, $0 \leqslant p \leqslant q - 1$, on a

$$A(p , q) = p(\psi\pi)^{-1} \quad ,$$

où π est le morphisme naturel de $\underline{N}$ sur $\underline{Z}_q$, et le résultat découle du (1) ci-dessus.

Dans les autres cas, on a la formule

$$A(p , q) = \sum_{1 \leqslant j} (Y_n \circ \psi^{-1})^* (Y_n \, j\psi^{-1}) \, A(p_j' , q) \quad ,$$

où p_j' est le plus petit élément de $\underline{N} \cap (p - j + q\underline{N})$. Comme le membre de droite est manifestement non ambigu, le résultat découle de l'hypothèse d'induction du cas traîté ci-dessus, puisque $p_j' \geqslant q \implies p_j' < p$.

(3) $M = 1 \cup L$, où L est une $\mathcal{L}$-classe. - On sait qu'il existe un groupe G , et un morphisme $\gamma : M \to G$ tel que, pour chaque $h \in L$, la restriction à hM de γ soit un isomorphisme.

Ceci implique

$$h\mu^{-1} = (Y_n \, 1\mu^{-1})^* \sum \{ (Y_n \, h'\mu^{-1}).g(\mu\gamma)^{-1} : \; h' \in hM \, , \; g = (h'\gamma)^{-1} (h\gamma) \in G \} \quad ,$$

établissant $h\mu^{-1} \in \mathcal{A}$ pour $h \in L$. Comme $L^2 = L$, on a $1\mu^{-1} = (Y_n \, 1\mu^{-1})^*$, un cas déjà traîté.

Nous considérons maintenant le cas où M ne rentre dans aucune des catégories envisagées ci-dessus. D'après le lemme de Krohn et Rhodes, il existe :

- Un idéal à gauche non vide $L \not\subseteq M \setminus 1$,
- Un sous-monoïde $T \neq 1 , M$,

tels que $M \subset L \cup T$.

Posons

$$Y_1 = Y \cap L\mu^{-1} \; ; \qquad Y_2 = (Y \setminus Y_1) \cap T\mu^{-1} \; .$$

L'hypothèse d'induction permet de supposer que Y_1 et Y_2 sont non vides, et comme M est fini, nous pouvons prendre un alphabet fini Z et une bijection $\nu : Z \to L' = L \cap (Y_2^* Y_1)\mu$. Définissons une substitution $\lambda : Z^* \to Y^*$, en posant, pour chaque $z \in Z$,

$$z\lambda = \{g \in Y_2^* Y_1 : g\mu = z\nu\} \; .$$

Par construction, $z\lambda$ est union disjointe de parties de la forme $A_y\, y$, où $y \in Y_1$, $A_y \in Y_2^*$, $Y_2 \cap Y_1 = \emptyset$, et où $A_y \in \mathfrak{A}$, puisque A_y est image inverse, donc partie du sous-monoïde $T \not\subseteq M$. Donc $\lambda \in \Lambda(\mathfrak{A})$.

Maintenant, l'identité $Y^* = (Y_2^* Y_1)^* Y_2^*$ montre que chaque $a \in A$ a exactement une factorisation $a = a_1 a_2$, où $a_1 \in (Y_2^* Y_1)^*$, $a_2 \in Y_2^*$. Par conséquent, A est une union finie disjointe de produits non ambigus de la forme $A_1 A_2$, où

$$A_1 = (Y_2^* Y_1)^* \cap m\mu^{-1} \qquad (m \in 1 \cup L) \; ,$$

$$A_2 = Y_2^* \cap m\mu^{-1} \qquad (m \in T) \; .$$

La deuxième relation implique $A_2 \in \mathfrak{A}$, d'après $T \not\subseteq M$ et l'hypothèse d'induction, et, puisque $\mathfrak{A}$ est fermé, par les opérations polynomiales non ambigues, il suffit de montrer $A_1 \in \mathfrak{A}$. Or la première relation équivaut à $A_1 = B\lambda$, où $B = m\nu^{-1}$, et où $\nu : Z^* \to 1 \cup L$ est le morphisme étendant la bijection $\nu : Z \to L'$. Comme $L \not\subseteq M \setminus 1$, on a $\mathrm{Card}(1 \cup L) < \mathrm{Card}(M)$, d'où $B \in \mathfrak{A}$, par induction, et le résultat est établi.

(Texte reçu le 19 janvier 1971)

Marcel P. SCHÜTZENBERGER
9 villa Poirier
75 - PARIS 15