Sur Certaines Variétés de Monoïdes Finis

M. P. SCHÜTZENBERGER

Institut Blaise Pascal
Paris, France

Le but de cet exposé est de rassembler un certain nombre d'énoncés de la théorie des monoïdes finis qui semblent pouvoir présenter des applications à l'étude des automates finis et des langages de Kleene.

Nous commencerons par rappeler le résultat suivant de Clifford et de Miller (1956).

Théorème 1. *Soit u un élément idempotent d'un monoïde M et soit*

$$G_u = \{m \in Mu \cap uM : u \in Mm \cap mM\} \tag{1}$$

L'ensemble G_u est un sous groupe de M qui contient tous les sous groupes de M admettant u pour élemént neutre.

Démonstration. Soit $u = u^2 \in M$. Par définition un élément $m \in M$ appartient à G_u si et seulement si il existe $m_1, m_2, m_3, m_4 \in M$ satisfaisant:

$$m = m_1 u = u m_2 \qquad u = m_3 m = m m_4$$

Donc en particulier $u \in G_u$. Les deux premières relations donnent

$$mu = m_1 uu = m_1 u = m \qquad um = uum_2 = um_2 = m$$

Donc u est un élément neutre pour tous les éléments de G_u.

Soit $m' = m'_1 u = u m'_2$ tel que $u = m'_3 m' = m' m'_4$ un autre élément de G_u. On a

$$mm' = mm' u = umm' \qquad m'_3 m_3 mm' = m'_3 um' = m'_3 m' = u$$
$$mm' m'_4 m_4 = mum_4 = mm_4 = u$$

Donc G_u est un sous ensemble stable de M (c'est à dire $G_u G_u \subset G_u$). Enfin, d'après $u^2 = u = m_3 m$ et $m = um$, on voit que $u = um_3 um$ et il n'y a donc pas de perte de généralité à supposer désormais que $um_3 = m_3 u = m_3$.

Considérons le produit mm_3. En utilisant successivement les hypothèses $m_3 = m_3 u$, $u = mm_4$, $m_3 m = u$, $mu = m$, $mm_4 = u$ on obtient:

$$mm_3 = mm_3 u = mm_3 mm_4 = mum_4 = mm_4 = u$$

Nous avons établi que G_u est un sous ensemble stable admettant un élément neutre u et ayant la propriété qu'à tout $m \in G_u$ correspond un élément $m_3 = um_3u$ qui satisfait $u = um_3u.m = mum_3u$.

Ceci montre d'abord que $um_3u \in G_u$ et que l'ensemble G_u muni du produit de M est isomorphe à un groupe puisque chaque élément possède un inverse. Enfin le groupe G_u est maximal car si les éléments m_5 et m_6 de M sont invariant par multiplication par u et satisfont $u = m_5m_6 = m_6m_5$ ils appartiennent à G_u d'après la définition même de cet ensemble. Ceci terminé la démonstration du théorème.

Rappelons maintenant qu'une famille **V** de groupes (monoïdes) est une *pseudo variété de groupes* (*monoïdes*) si elle contient tout sous groupe (sous monoïde) tout groupe (monoïde) quotient, et tout produit direct de deux membres quelconques de ses membres.

Par exemple, les groupes (monoïdes) finis forment une variété de même que les groupes (monoïdes) commutatifs; par contre les groupes cycliques ne forment pas une variété puisque le produit direct de deux groupes cycliques n'est plus nécessairement cyclique. On a

Proposition 1. *Soit* **V** *une variété de groupes et soit* **V'** *la famille de tous les monoïdes finis dont tout les sous groupes appartiennent à* **V**. **V'** *est une pseudo variété de monoïdes que l'on appelara la pseudo variété de monoïdes finis induite par la variété de groupe* **V**.

Démonstration. Soit M un monoïde fini dont tout les sous groupes appartiennent à la variété de group V. Si M' est un sous monoïde de M et G' un sous groupe de M', G' contient un et un seul idempotent u et il résulte immédiatement de (1) que G' est contenu dans $M' \cap G_u$. Donc M' appartient à la variété **V'** de monoïde fini induite par **V**.

De même, si $M_1, M_2 \in \mathbf{V}'$, tout sous groupe de produit direct $M_1 \times M_2$ est le produit direct d'un sous groupe de M_1 et d'un sous groupe de M_2 et par conséquent $M_1 \times M_2 \in \mathbf{V}'$.

Il reste seulement à établir $M' \in V'$ quand $M \in V'$ et quand $M' = \alpha M$ où α est un épimorphisme.

Dans ces conditions soit u' un idempotent de M' et soit $G_{u'}$ le sous groupe maximal de M' qui contient u'. Soit $P = \{m \in M : \alpha m \in G_{u'}\}$ d'après $G'_uG'_u = G'_u \neq \phi$ on a $PP \subset P \neq \phi$.

Considérons un élément $m \in P$ tel que l'ensemble $mP \cap Pm$ ait le plus petit nombre possible d'élément. Cette hypothèse a un sens puisque M est fini. Quelque soit $k > 0$ $m^kP \cap Pm^k = mP \cap Pm$ et en vertu de l'hypothèse de minimalité $m^kP \cap Pm^k = mP \cap Pm$.

De plus comme M est fini l'ensemble $m, m^2, m^3, \ldots, m^k, \ldots$ ne contient qu'un nombre fini de termes, donc $m^{k_1} = k m^{k_1 k'_1}$ pour au moins une paire k_1, k'_1 d'entiers positifs et par consequent toutes les paires k_2, k'_2 où $k_2 \geqslant k_1$ et $k'_2 = k_3 k_1$; donc enfin en prenant $k = k_1 k'_1$ on obtient $m^k = m^{2k}$ et l'on peut supposer désormais que $m = u = u^2$ est un idempotent.

Montrons que $uP \cap Pu = G_u$ est bien un sous groupe de P contenant u. En effet la relation $m \in uP \cap Pu$ signifie que $m = um_1 = m_2 u$ pour au moins une paire $m_1, m_2 \in M$; par conséquent

$$m \in mP \cap Pm = um_1 P \cap Pm_2 u \subset uP \cap Pu$$

ce qui, d'après l'hypothèse de minimalité, entraine $mP \cap Pm = uP \cap Pu$, donc $u \in mP \cap Pm$ puisque $u \in uP \cap Pu$ d'après (1) ceci établit le résultat cherché.

Maintenant la relation $G_u = uG_u = G_u u$ donne $G_u = uG_u u = u(uP \cap Pu)u = uPu$, donc en prenant les images par α et en rappelant que $\alpha P = G'$ on obtient

$$\alpha G_u = \alpha u \,.\, \alpha P \,.\, \alpha u = \alpha u \,.\, G' \,.\, \alpha u = G'$$

et nous avons établi que le sous groupe G' de M' est une image homomorphe du sous groupe G_u de M. Ceci termine la preuve de la Proposition 2.

Il y a évidemment bien des manières d'affaiblir la condition de finitude de M; il est toutefois impossible de se dispenser entièrement d'hypothèses de ce type puisqu'un sous groupe G' d'un monoïde $M' = \alpha M$ peut, pour M infini, être l'image d'un sous ensemble $P \subset M$ ne contenant aucun sous groupe G tel que $\alpha G = G'$. Ceci est illustré par l'exemple où M est un monoïde libre puisque dans ces conditions M n'a qu'un seul sous groupe—à savoir le sous groupe trivial formé par l'élément neutre de M.

On se propose maintenant de définir une opération de composition entre monoïdes. Pour faciliter l'écriture on considère deux monoïdes fixes M_1 et M_2 et l'on désigne par R la famille de tous les ensembles de paires d'éléments $(m_1, m_2) \in M_1 \times M_2$. Etant donnés des éléments quelconques $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\} \in R$; $m_1 \in M_1$ et $m_2 \in M_2$ on définit les éléments $m_1 r$ et $r m_2$ de R par les relations

$$m_1 r = \{(m_1 m_{1,i}, m_{2,i}) : i \in I_r\} \in R$$
$$r m_2 = \{(m_{1,i}, m_{2,i} m_2) : i \in I_r\} \in R$$

Définition 1. *On appelera produit semi direct, booléen $M_1 \circledast M_2$ l'ensemble $M = M_1 \times R \times M_2$ muni de la loi de composition qui associe à tout $m = (m_1, r, m_2)$, $m' = (m'_1, r', m'_2) \in M$ l'élément*

$$mm' = (m_1 m'_1, m_1 r' \cup r m'_2, m_2 m'_2) \in M$$

Il est facile de voir que l'opération $m \times m' \to mm'$ est associative.

En effet, si $m'' = (m_1'', r'', m_2'') \in M$, on a

$$\begin{aligned}(mm')m'' &= (m_1 m_1' m_1'', (m_1 m_1')r'' \cup (m_1 r' \cup rm_2)m_2'', m_2 m_2' m_2'') \\ &= (m_1 m_1' m_1'', m_1 m_1' r'' \cup m_1 r' m_2'' \cup rm_2 m_2'', m_2 m_2' m_2'') \\ &= m(m' m'')\end{aligned}$$

De plus M a un élément neutre [à savoir (e_1, ϕ, e_2) où e_1 et e_2 sont des éléments neutres de M_1 et de M_2 et où $\phi \in R$ est l'ensemble vide] et par conséquent M est un monoïde.

Proposition 2. *Soit* **V** *une variété de groupe. Si* M_1 *et* M_2 *appartiennent à la pseudo variété de monoïde finis induite par* **V** *il en est de même de leur produit semi-direct booléen* $M = M_1 \circledast M_2$.

Démonstration. Soit $u = (u_1, r, u_2) \in M$ un idempotent de M et soit G_u le sous groupe maximal de M qui le contient. Il est clair que $u_1 = u_1^2$, $u_2 = u_2^2$, et que l'application qui envoie tout $g = (r_1, r_g, m_2) \in G_u$ sur la paire $(m_1, m_2) \in M_1 \times M_2$ est un homomorphisme γ de G_u dans le produit direct $G_{u_1} \times G_{u_2}$ des sous groupes maximaux $G_{u_1} \in M_1$ et $G_{u_2} \in M_2$. Par construction, le noyeau de γ est l'ensemble N des éléments de M de la forme (u_1, s, u_2) qui appartiennent à G_u. Donc si nous pouvons prouver que N se réduit à $\{u\}$ nous aurons établi que γ est un monomorphisme, c'est à dire que G_u est isomorphe à un sous groupe de $G_{u_1} \times G_{u_2}$. Soit donc $m = (u_1, s, u_2) \in N$. Puisque $m \in G_u$, m possède un inverse $\bar{m}$ (relativement à u) c'est à dire qu'il existe un élément $\bar{m} = u\bar{m} = \bar{m}u$ tel que $u = m\bar{m} = \bar{m}m$. Il est clair que $\bar{m}$ a la forme $\bar{m} = (u_1, \bar{s}, u_2)$ pour un certain $\bar{s} \in R$. Nous avons les relations suivantes:

$$r = u_1 r \cup ru_2 \qquad \text{(d'après } u = u^2\text{)}$$

$$r = u_1 \bar{s} \cup su_2 \qquad \text{(d'après } u = m\bar{m}\text{)}$$

$$s = u_1 r \cup u_1 su_2 \cup u_2 \qquad \text{(d'après } m = umu\text{)}$$

La première relation montre que $u_1 r \subset r$; par conséquent $u_1 r = u_1 u_1 \bar{s} \cup u_1 su_2 \subset r$ d'après la seconde relation et, a fortiori $u_1 su_2 \subset r$. Or la troisième relation s'écrit aussi $s = r \cup u_1 su_2$ et, par conséquent, on a établi $s = r$, c'est à dire $m = u$ pour tout $m \in N$. Ceci achève la vérification que tous les sous groupes du produit semi direct M appartiennent à **V**.

Afin de rattacher les sonsidérations précédentes à la théorie des langages formels nous considérons maintenant un ensemble fixe X et le monoïde libre X^* engendré par cet ensemble. Les éléments de X^* sont appelés "*mots*" et nous appelerons "*langages formels sur* X" tout sous ensemble de

X^*. Enfin étant donnée une *pseudo* variété $\mathbf{V}'$ de monoïdes finis induites par une variété de group $\mathbf{V}$ nous dirons qu'un langage formel $F \subset X^*$ est un $\mathbf{V}'$-langage si et seulement si il existe un monoïde quotient $M \in V'$ et un homomorphisme $\alpha: X^* \to M$ tel que l'ensemble F soit précisèment égal à l'image inverse $\overset{-1}{\alpha}\alpha F$ de son image αF dans M par α. Formellement,

$$F = \{f' \in X^* : \exists_F f : \alpha f' = \alpha f\}$$

Proposition 3. *Si F_1 et F_2 sont deux $\mathbf{V}'$-langages sur X il en est de même de leur union $F_1 \cup F_2$, du complément relatif $F_1 \backslash F_2$ et du produit $F_1 F_2$*

$$F_1 F_2 = \{ff' \in X^* : f \in F_1, f' \in F_2\}.$$

Démonstration. Soient $\alpha_1: X^* \to M_1$ et $\alpha_2: X^* \to M_2$ tels que $M_1, M_2 \in \mathbf{V}'$ $\overset{-1}{\alpha_1}\alpha_1 F_1 = F_1$; $\overset{-1}{\alpha_1}\alpha_2 F_2 = F_2$. Nous considérerons le produit semi-direct $M = M_1 \oplus M_2$ et nous définissons une application $\alpha: X^* \to M$ en posant $\alpha e = (\alpha_1 e, \{(\alpha_1 e, \alpha_2 e)\}, \alpha_2 e)$ et pour tout $f \in X^*$

$$\alpha f = (\alpha_1 f, \{(\alpha_1 f', \alpha_2 f'') : f', f'' \in X^*; f' f'' = f\}, \alpha_2 f)$$

Il est clair que α est un homomorphisme de X^* sur un certain sous monoïde $\bar{M}$ de M. De plus si $f \in X^*$ on peut savoir en connaissant seulement son image $\alpha f \in \bar{M}$ si $f \in F_1 \cup F_1$ ou $f \in F_1 \backslash F_2$ ou $f \in F_1 F_2$. Donc $\overset{-1}{\alpha}\alpha F = F$ pour $F = F \cup F_1, = F_1 \backslash F_2$ ou $= F_1 F_2$ et la validité l'énoncé résulte de la Proposition 4.

Si la variété de groupe $\mathbf{V}$ est la variété $\mathbf{V}_1$ des groupes triviaux (c'est à dire des groupes réduits à leurs éléments neutres) la famille correspondantes de langage a été étudiée par McNaughton et Trachtenbrot et c'est la plus petite famille fermée par les opérations d'union de complémtement relatif et de produit qui contienne tous les sous ensembles de X. On sait aussi que quand $\mathbf{V}$ contient tous les groupes *abeliens* et que F est un $\mathbf{V}$ langage il en est de même du sous monoïde de X^* engendré par le langage $F' = X^* F \backslash X^* F X X^*$ formé de tous les mots de l'idéal $X^* F$ qui n'ont aucun facteur propre gauche dans $X^* F$. Cette deuxième forme de langage a aussi été étudiée par McNaughton (1960). Nous ne reproduirons par les démonstrations ici et nous terminerons en proposant le problème de prouver (ou de refuter) l'hypothèse selon laquelle les opérations d'union, complémentation produits et la formation de sous monoïdes du type qui vient d'être décrit permet d'engendrer tout les V'_{ab}-langages (à partir des $X' \subset X$) où V_{ab} est la *pseudo* variété de monoïdes finis induite par la variété des groupes abéliens.

BIBLIOGRAPHIE

McNaughton, R. (1960). Symbolic logic and automata, *Wright Air Development Div. Tech. Note* 60–244, Cincinnati, Ohio.

Miller, D. D., et Clifford, A. H. (1956). Regular D-classes in semigroups, *Trans. Am. Math. Soc.* **82**, 270–280.

Petrone, L., et Schützenberger, M. P. *Sur un problème de McNaughton* (à paraître).