A PROPOS DU RELATION RATIONELLES FONCTIONNELLES

M. SCHUTZENBERGER
IRIA - Université - Paris 7
FRANCE

1. - INTRODUCTION

Le théorème de Mc Naughton ([2]) est une généralisation à l'ensemble X^{ω} des mots infinis sur un alphabet X du théorème de Kleene sur le monoïde libre X^*. Nous nous proposons d'en simplifier un peu la preuve originale grâce à l'idée due à Büchi ([1]) d'utiliser un cas particulier du Théorème de Ramsey.

Nous employons les notations standards de Eilenberg : $X^+ = XX^* = X^* \setminus \{1\}$, et $|f|$ = la longueur du mot f de X^* . Une partie A de X^* est reconnaissable (A $\in$ Rec) ssi il existe un morphisme φ de X^* dans un monoïde fini qui satisfait $A\varphi\varphi^{-1} = A$ (qui "reconnaît" A).

L'écriture $s \in \omega(A)$ servira pour exprimer que le mot infini $s \in X^{\omega}$ possède une infinité de facteurs gauches dans la partie A de X^* .

Ceci permet de définir $\overset{\omega}{\text{Rec}}$ comme la plus petite famille R de parties de X^{ω} qui satisfasse les deux conditions :

(i) Pour tout $A \in$ Rec, R contient l'ensemble $\{s \in X^{\omega} = s \in \omega(A)\}$

(ii) R est fermée par rapport aux opérations booléennes , c'est à dire que si P, $Q \in R$, la famille R contient $P \cup Q$, $P \setminus Q$ et $P \cap Q$.

Nous chercherons à établir l'identité de $\overset{\omega}{\text{Rec}}$ et de la famille $\overset{\omega}{\text{Rat}}$ définie comme la plus petite famille R' satisfaisant les deux conditions :

(iii) $c\, B^{\omega} \in R'$ pour tout c, $B \in$ Rat tel que $1 \notin B$, $\emptyset \neq B$.

(iiii) P, $Q \in R' \Longrightarrow P \cup Q \in R'$.

La preuve repose sur le théorème suivant :

<u>THEOREME 1</u> (Ramsey, Büchi).

Soient φ un morphisme de X^* dans un monoïde fini M et $s = a_0\, a_1 \ldots a_n \ldots$ une factorisation d'un mot infini s de X^{ω} . $(a_0, a_1, \ldots, a_n, \ldots \in X^+)$.

Il existe un élément m, un idempotent u et une factorisation $s = c_0\, c_1 \ldots c_n$ obtenue en regroupant les termes de la factorisation précédente qui satisfait les conditions :

$c_0 \varphi = m = m\, u$; et pour tout $n \in \mathbb{N}$ $c_{n+1} \varphi = u = u^2$;

<u>PREUVE</u> - Soit A l'ensemble des facteurs de s de la forme $a_n\, a_{n+1} \ldots a_{n'}$ $(1 \leqslant n \leqslant n')$ et $k = \text{Card}\,(A\varphi)$.

Si $k = 1$, $A\varphi$ se réduit à un idempotent u et le résultat est trivialement vérifié en remplaçant a_0 par $a_0\ a_1$ et en prenant $m = (a_0\ a_1)\varphi = a_0\ \varphi\ u = a_0\ \varphi\ u\ u = m\ u$

Nous pouvons donc procéder par induction sur k.

Prenons $m \in A\varphi$ quelconque et notons $P = \{p_1 < p_2 < \ldots\}$ l'ensemble des indices $p \in \mathbb{N}$ tels qu'aucun des facteurs $a_p\ a_{p+1} \ldots a_{p'}$ $(1 \leqslant p \leqslant p')$ n'appartienne à $m\,\varphi^{-1}$.

Si P est infini, on peut, en regroupant les termes, obtenir la factorisation $a'_0\ a'_1 \ldots a'_n$ de s où chaque a'_n $(n \geqslant 1)$ est égal au produit $a_p\ a_{p+1} \ldots a_{p'-1}$ avec $p = p_n$, $p' = p_{n+1}$. L'ensemble A' des produits $a'_n\ a'_{n+1} \ldots a'_{n'}$ $(1 \leqslant n \leqslant n')$ a son image par φ contenue dans $A\varphi \setminus \{m\}$ et le résultat découle de l'hypothèse d'induction.

Considérons donc, maintenant, le cas où P est fini. Il existe un $q \in \mathbb{N}$ tel que pour tout $n > q$, au moins un des produits $a_n\ a_{n+1} \ldots a_{n'}$ $(n' > n)$ appartiennent $m\,\varphi^{-1}$.

Ceci permet de trouver une factorisation $s = a'_0\ a'_1 \ldots a'_n \ldots$ où $a'_n\varphi = m$ pour tout n positif.

Maintenant comme M est fini m a une puissance positive m^r qui est un idempotent. Regroupant les termes r par r on est ramené au cas de k = 1. Q.E.D.

Nous dirons que la factorisation $c_0\ c_1 \ldots c_n \ldots$ décrit dans l'énoncé une <u>mu-factorisation de s subordonnée</u> à $a_0\ a_1 \ldots a_n$.

Nous désignerons par $\Pi(s)$ l'ensemble des paires $(m = m\ u,\ u = u^2) \in M \times M$

tel que s admette au moins une mu-factorisation subordonnée à la factorisation $s = x_0 x_1 \ldots x_n \ldots$ où $x_0, x_1, \ldots, x_n, \ldots \in X$ (donc à n'importe quelle autre factorisation).

2. - UNE CONSTRUCTION

Nous considérons deux parties reconnaissables non vides $B, C \in X^*$, où $1 \notin B$, et d'après le Théorème de Kleene il existe des morphismes φ' et φ de X^* dans des monoïdes finis M' et M et une application $[\ ]$ de M dans $M' \times M'$ qui satisfont les conditions suivantes :

(1) φ' reconnaît CB^* et B^+;

(2) Pour tout mot f de X^*, $[f\varphi]$ est l'ensemble des paires $(f'\varphi', f''\varphi')$ où $f', f'' \in X^*$, $f = f'f''$.

Il sera commode (et toujours possible) de supposer $1\varphi'\varphi'^{-1} = 1\varphi\varphi^{-1} = 1$.
Désignons maintenant par V l'ensemble des paires $(m = m\,u,\ u = u^2) \in M \times M$ tel qu'il existe $q, r, s \in M'$ satisfaisant les conditions :
$q \in C\,B^*\varphi'$; $r\,s \in B^+\varphi'$;
$(q, r) \in [m]$; $(s, r) \in [u]$.

PROPRIETE 1- Soient $s \in X^\omega$ et $(m, u) \in U(s)$. On a $s \in C\,B^\omega$ ssi $(m, u) \in V$.

PREUVE : Supposons d'abord $(m, u) \in V$ et considérons une mu-factorisation $a_0\, a_1 \dots a_n \dots$ de s.

Notre hypothèse implique l'existence de factorisations $a_n = a'_n\, a''_n$ telles que l'on ait identiquement $a'_0\,\varphi' = q \in (C\,B^*)\,\varphi'$; $a''_n\,\varphi' = r$; $a'_{n+1}\,\varphi' = s$ où $r\,s \in B^+\varphi'$ et où, par conséquent :
$a'_0 \in C\,B^*$, $a''_n\, a'_{n+1} \in B^+$ ce qui établit $s \in C\,B^\omega$.

Réciproquement soit $s \in C\,B^\omega$, c'est-à-dire $s = c\, b_0\, b_1 \dots b_n \dots$ où $c \in C\,B^*$, $b_n \in B^+$.

Nous pouvons choisir une mu-factorisation $s = a_0\, a_1 \ldots a_n \ldots$ de telle sorte que les conditions suivantes soient vérifiées :

$a_0 = c\, b_0 \ldots b_n\, f \qquad (n \geqslant 0);$

$b_{n+1} = f\, g\ ;$

$a_1 = g\, b_{n+2} \ldots b_{n'}\, f' \qquad (n' \geqslant n+2);$

$b_{n'+1} = f'\, g'\ ;$

$f\, \varphi' = f'\, \varphi' \quad (= r).$

Posant $q = (c\, b_0 \ldots b_n)\, \varphi'$

et $s = g\, b_{n+2} \ldots b_{n'}$, on en déduit immédiatement que $(m, u) \in V$.

Q.E.D.

Soit maintenant $u \neq 1$ un idempotent de M. D'après l'hypothèse $1\varphi\varphi^{-1} = 1$ on a $1 \notin u\varphi^{-1}$. Nous notons E_u la plus petite partie de X^+ telle que $u\varphi^{-1} = E_u^+$ et nous posons :

$E'_u = E_u \setminus E_u X^+$ ce qui entraine que tout mot de $u\varphi^{-1}$ ait exactement un facteur gauche dans E'_u.

Nous aurons besoin de la :

<u>REMARQUE 2</u>. La relation $a, b, abc \in u\varphi^{-1}$ $(a, b, c \in X^+)$ implique $b\, c \in u\varphi^{-1}$.

<u>PREUVE</u> - Soit $m = c\varphi \in M$. les hypothèses équivalent à $u\, u\, m = u$.
Donc $(bc)\, \varphi = u\, m = u$. Q.E.D.

Soit enfin :

$$K_u = \cup \{X^* E'_{u'} : u' \in W_u\}$$ où, par commodité,

$W_u = \{u' = u'^2 \in M : u \notin M u' M\};$

La propriété suivante traduit en termes de monoïdes la méthode de Mc Naughton.

On pourrait (au prix d'une légère complication) remplacer K_u par R_u^* où $R_u = R'_u \setminus R'_u X^+$ avec R'_u = l'ensemble des mots $f \in X^+$ tels que $u \notin M. f \varphi. M$.

PROPRIETE 3 - Soit $(m,u) \in V$.

La partie $A = m \varphi^{-1} (u \varphi^{-1})^{\omega}$ de X^{ω} est l'ensemble des mots infinis tels que l'on ait :

(1) $s \in \omega(F)$ où $F = m\varphi^{-1}. E_u. E'_u$;

(2) $s \notin \omega(K_u)$.

PREUVE. Soit d'abord $s \in C B^{\omega}$ et $(m, u) \in U(s)$. On peut trouver une mu-factorisation $s = a_0 a_1 \dots a_n \dots$ dans laquelle tous les a_{n+1} appartiennent à E_u. Comme $(a_0 a_1 \dots a_n) \varphi = m$, identiquement, ceci montre que $s \in \omega$ (F).

Supposons maintenant $u' \in W_u$, $h \in E'_{u'}$ et que g h soit un facteur gauche de s. Comme $u \in M. b \varphi. M$ pour tout facteur b de $a_1 \dots a_n \dots$, on a que g est un facteur gauche de a_0, donc que $s \notin \omega$ (K_u) puisque tout mot a au plus un facteur gauche dans chacun des $E'_{u'}$ $(u' \in W_u)$.

Réciproquement soit s un mot infini ayant une infinité de facteurs gauches $f_n = g_n e_n e'_n$ dans F $(g_n \in m\varphi^{-1}; e_n \in E_u; e'_n \in E'_u)$.

Supposons d'abord qu'il existe un mot g tel que $g_n = g$ pour une suite infinie de f_n. Comme aucun mot n'a plus de un facteur gauche dans E'_u, nous pouvons prendre une sous suite de la précédente telle que chaque $e_n e'_n$ soit un facteur gauche de e_{n+1}. La conclusion $s \in A$ résulte alors immédiatement de la Remarque 2

Supposons maintenant qu'un tel mot g n'existe pas. Nous pouvons prendre une sous suite telle que chaque g_{n+1} ait la forme $f_n\, h_n$ ($h_n \in X^+$), ce qui donne une factorisation $s = a_0\, a_1 \dots a_n$ où $a_0 = g_0\, e_0$ et, identiquement, $a_{n+1} = e'_n\, h_{n+1}\, e_{n+1}$. Utilisant le théorème 1, il existe un idempotent $\bar{u}$ et une $\bar{m}\,\bar{u}$-factorisation subordonnée à la précédente $s = b_0\, b_1 \dots b_n \dots$ où $b_0 = f_p$ pour un certain $p \in \mathbb{N}$ et où par conséquent $\bar{m} = m$.

Comme $b_{n+1} \in E'_u\, X^*\, E_u$, par construction, nous avons :

(i) $\bar{u} = \bar{u}^2 \in u\, M \cap M\, u$.

Introduisons alors l'hypothèse $s \notin \omega(K_u)$. Comme s a une infinité de facteurs dans $\bar{u}\, \bar{\varphi}'$, on a $s \in \omega(X^*\, E'_{\bar{u}})$ et, par conséquent, $\bar{u} \notin W_u$, c'est à dire :

(ii) $u = u^2 \in M\, \bar{u}\, M$.

Comme M est fini, les deux relations : $\bar{u} \in u\, M \cap M\, u$ et $u \in M\, \bar{u}\, M$ entrainent que u et $\bar{u}$ appartiennent à la même $\mathcal{H}$ classe de M, donc qu'ils soient égaux puisque $u = u^2$, $\bar{u} = \bar{u}^2$. Ceci achève la preuve de $s \in A$.

<u>COROLLAIRE</u>. Le monôme CB^{ω} appartient à Rec^{ω}.

<u>PREUVE</u>. Ceci résulte immédiatement des propriétés 1. et 3.

Q.E.D.

3. - FIN DE LA DEMONSTRATION

THEOREME DE BUCHI. La famille $\overset{\omega}{\mathrm{Rat}}$ est fermée par rapport aux opérations booléennes.

PREUVE - Comme X^ω appartient à $\overset{\omega}{\mathrm{Rat}}$, et comme cette famille est fermée par union, il suffit de montrer qu'elle contient $D = X^\omega \setminus C\,B^\omega$, avec $C\,B^\omega$ comme dans la section précédente. Or ceci est trivial d'après le théorème de Ramsey-Büchi et le corollaire 4 puisque celui-ci montre que D est l'ensemble des $s \in X^\omega$ tels que $U(s) \cap V = \emptyset$ ou, de façon équivalente, $U(s) \not\subset V$.

Q.E.D.

THEOREME DE MC NAUGHTON - Les familles $R' = \overset{\omega}{\mathrm{Rat}}$ et $R = \overset{\omega}{\mathrm{Rec}}$ sont identiques.

PREUVE - L'inclusion de R' dans R résulte immédiatement de la Propriété 3 et des définitions de R et de R' puisque F et K_u sont certainement des parties reconnaissables de X^* .

Comme R' est fermée par les opérations booléennes d'après le théorème précédent, il suffit pour établir l'inclusion opposée de considérer un élément m d'un monoïde fini M et un morphisme $\varphi : X^* \to M$ et de prouver $A \in \overset{\omega}{\mathrm{Rat}}$ où $A = \{s \in X^\omega : s \in \omega(m\,\varphi^{-1})\}$.

Or de nouveau ceci est trivial puisque l'on peut écrire $A = m\,\varphi^{-1} .\, B^+$ où $B = \{f \in X^+ : m.\, f\,\varphi = m\}$.

Q.E.D.

OBSERVATION. Pour tout morphisme de semi groupe $\varphi : X^+ \to M$ notons $\bar{\varphi}^{-1}$ l'application envoyant chaque $(m, u) \in M \times M$ sur $m\varphi^{-1} (u\varphi^{-1})^\omega \in X^\omega$ et $\bar{\varphi}$ l'application réciproque telle que pour chaque $s \in X^\omega$ on ait $(m, u) \in s\bar{\varphi}$ ssi $s \in (m, u)\bar{\varphi}^{-1}$.

On dira que φ reconnaît une partie A de X^ω ssi $A = A\bar{\varphi}\bar{\varphi}^{-1}$

(donc $V\bar{\varphi}^{-1}\bar{\varphi} = V$ où $V = A\bar{\varphi}$).

D'autre part appelons semi-groupe syntactique de la partie A de X^ω le semi groupe quotient $S = X^+\sigma$, où pout tout $f, f' \in X^+$ on pose comme dans le cas fini habituel :

$f\sigma = f'\sigma$ ssi

$gfs, gf's \in A$ ou $gfs, gf's \notin A$ pour chaque $(g, s) \in X^* \times X^\omega$.

Ces notations permettent de formuler de la façon suivante le Théorème de Buchi.

PROPRIETE. Le monoïde syntactique S de A est fini ssi $A \in \overset{\omega}{\text{Rat}}$. De plus dans ce cas :

le morphisme σ reconnaît A et S est image homomorphe de tout monoïde $X^+\varphi$ où le morphisme φ reconnaît A.

PREUVE. Supposons S fini et $(m, u) \in A\bar{\sigma}$. Il existe des mots $a_j \in X^+$ tels que $a_o\sigma = m$; $a_{j+1}\sigma = u$ $(j \in \mathbb{N})$ et $s = a_0 a_1 \ldots a_n \ldots \in A$.
Soit $s' \in (m, u)\bar{\sigma}^{-1}$, c'est-à-dire $s' = b_0 b_1 \ldots b_n \ldots$ où $b_j\sigma = a_j\sigma$ identiquement. D'après la définition de σ on a $h_0 h_1 \ldots h_n a_{n+1} \ldots a_{n+h} \ldots \in A$ pour tout $n \in \mathbb{N}$, donc $s' \in A$.

Ceci montre que quand S est fini, le morphisme σ reconnaît A et que par conséquent $A \in \overset{\omega}{\text{Rat}}$.

Supposons maintenant $A \in \overset{\omega}{\mathrm{Rat}}$. On déduit facilement de la Propriété 2 l'existence d'un semi-groupe fini M et d'un morphisme surjectif $\varphi : X^+ \to M$ qui reconnaît A. Pour prouver que S est image homomorphe de M, et par conséquent que S est fini, il suffit de considérer deux mots f, $f' \in X^+$ tels que $f\sigma \neq f'\sigma$ et de montrer $f\varphi \neq f'\varphi$.

L'hypothèse implique qu'il existe $(g, s) \in X^* \times X^\omega$ tels que par exemple $g\,f\,s \in A$ et $g\,f'\,s \notin A$. De plus comme M est fini, on a $s \in (m, u)\,\bar{\varphi}^{-1}$ pour au moins une paire $(m, u) \in M \times M$. Maintenant comme φ reconnaît A, on a $(g\,f\,\varphi\,m, u) \in A\,\bar{\varphi}$ et $(g\,f'\varphi\,m, u) \notin A\,\bar{\varphi}$, donc $f\,\varphi \neq \varphi'\varphi$ Q.E.D.

REFERENCES

[1] BUCHI, J.R. (1962) - On a decision Methode ...
Proc. 1960 Int. Congress. Logic Methodology and Phil. of Science.
p. 1 - 11.

[2] R. Mc. NAUGHTON (1966) - Testing and generating Infinite sequences by finite automata.
Inf. and Control 9 - P. 521 - 530.