Revue française d'automatique informatique recherche opérationnelle. Informatique théorique

Pierre Lescanne

# Équivalence entre la famille des ensembles réguliers et la famille des ensembles algébriques

*Revue française d'automatique informatique recherche opérationnelle. Informatique théorique*, tome 10, nº R2 (1976), p. 57-81

<http://www.numdam.org/item?id=ITA_1976__10_2_57_0>

R.A.I.R.O. Informatique Théorique
(vol. 10, n° 8, août 1976, p. 57 à 81).

# ÉQUIVALENCE ENTRE LA FAMILLE DES ENSEMBLES RÉGULIERS ET LA FAMILLE DES ENSEMBLES ALGÉBRIQUES (*)

PIERRE LESCANNE (1)

Communiqué par M. Nivat.

---

Résumé. — *L'une des conséquences du théorème de Kleene* [14] *peut s'énoncer comme l'équivalence entre les langages réguliers et les langages engendrés par des grammaires linéaires à droite. Gruska* [11] *et McWhirter* [17] *ont démontré un théorème similaire affirmant l'équivalence entre les langages définis par des expressions régulières d'un certain type et les langages engendrés par les grammaires à contexte libre. Nous généralisons ces théorèmes aux sous-ensembles d'une algèbre plus générale. Nous définissons les ensembles réguliers et les ensembles algébriques; le théorème principal affirme que les ensembles réguliers et les ensembles algébriques coincident.*

## 1. INTRODUCTION

### 1.1. Trois définitions des langages de type 3

Adoptant la classification de Chomsky [4], nous nous proposons d'examiner à titre d'exemple les langages de type 3. On peut les caractériser de trois manières radicalement différentes.

1.1.1. *Définition par un système d'équations*

$V^*$ désigne l'ensemble des mots sur $V$, $\mathfrak{P}(V^*)$ l'ensemble des parties de $V^*$ et $\Lambda$ le mot vide. Soit le système d'équations :

$$X_1 = \bigcup_{i \in I_1} \alpha_i^1 X_{k(i,1)} \cup \bigcup_{i \in J_1} \beta_i^1,$$

$$\dots\dots\dots\dots\dots\dots$$

$$X_j = \bigcup_{i \in I_j} \alpha_i^j X_{k(i,j)} \cup \bigcup_{i \in J_j} \beta_i^j,$$

$$\dots\dots\dots\dots\dots\dots$$

$$X_n = \bigcup_{i \in I_n} \alpha_i^n X_{k(i,n)} \cup \bigcup_{i \in J_n} \beta_i^n,$$

---

(*) Reçu mai 1975.

(1) Centre National de la Recherche Scientifique, Unité d'Enseignement et de Recherche de Sciences Mathématiques, Université de Nancy I.

où $I_1, \ldots, I_n$ et $J_1, \ldots, J_n$ sont des ensembles finis, $k(i, j) \in \{1, \ldots, n\}$, $\alpha_j$ et $\beta_i^j$ appartiennent à $V^*$.

Un $n$-uple $\mathbf{L} = (L_1, \ldots, L_n)$ de parties de $V^*$ est une solution du système si pour tout $j$ on a :

$$L_j = \bigcup_{i \in I_j} \alpha_i^j L_{k(i,j)} \cup \bigcup_{i \in J_j} \beta_i^j.$$

Considérons l'ordre produit de l'inclusion. Tout système admet une solution minimale pour cet ordre; un langage est de type 3 s'il est première composante de la solution minimale d'un système du type ci-dessus, appelé aussi système linéaire à droite.

*Exemple* 1 : Si $V = \{a, b\}$, la solution minimale du système

$$X_1 = a X_2 \cup X_3 \cup b,$$
$$X_2 = a X_2 \cup b,$$
$$X_3 = ab X_3 \cup \Lambda,$$

est un langage de type 3.

1.1.2. *Définition par un automate fini*

Un ensemble muni d'une loi de composition externe à opérateurs dans un ensemble $V$ et d'un élément distingué $\lambda$ est appelé une algèbre monadique sur $V$. $V^*$ est une algèbre monadique où l'élément distingué est le mot vide $\Lambda$. Si $\mathscr{A}$ est une algèbre monadique sur $V$, il existe une application $\mathscr{I}_{\mathscr{A}}$ unique telle que

$$\mathscr{I}_{\mathscr{A}}(\Lambda) = \lambda,$$
$$\mathscr{I}_{\mathscr{A}}(a\,\alpha) = a \,.\, \mathscr{I}_{\mathscr{A}}(\alpha),$$

c'est pourquoi on désigne parfois $V^*$ sous le nom d'algèbre monadique initiale par référence aux catégories (*cf.* [19]).

Un langage $L$ de $V^*$ est de type 3 s'il existe une algèbre monadique finie $\mathscr{A}$ et une partie $t$ de $\mathscr{A}$ telle que

$$L = \mathscr{I}_{\mathscr{A}}^{-1}(t).$$

Un couple $(\mathscr{A}, t)$ est souvent appelé un automate fini (déterministe).

*Exemple* 2 : La figure 1 schématise un tel automate sur $\{ a, b \}$.

S'il y a un arc étiqueté par $a$ de $i$ vers $j$, cela signifie que $a.i = j$. Le langage reconnu par cet automate est le même que celui de l'exemple 1 si l'on prend $t = \{ 1, 2, 4 \}$ et $\lambda = 1$.

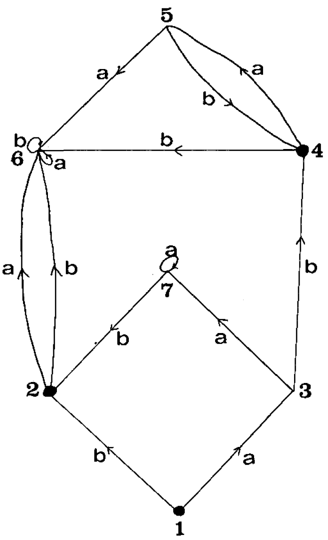


**Figure 1.**
**Un automate.**

1.1.3. *Définition par une expression régulière*

On appelle expression régulière, une expression correctement parenthésée qui utilise uniquement les signes $\cup$, ., * et les éléments de $V$. Par définition, un langage est de type 3 s'il peut être exprimé par une expression régulière de $V^*$ où $\cup$ désigne l'union, . le produit et

$$L^* = \{ \alpha \mid \alpha = \beta_1, \ldots, \beta_n, \beta_i \in L, n \geqq 0 \text{ pour } 1 \leqq i \leqq n \}$$

est l'itéré de $L$.

Autrement dit, les langages de type 3 sont obtenus à partir des langages finis par produit, union et itération; ce résultat est connu sous le nom de théorème de Kleene [14].

*Exemple* 3 : Le langage $L = a^*.b \cup (a.b)^*$ est un langage de type 3, c'est d'ailleurs le même que celui qui a été vu dans les exemples 1 et 2.

**1.2. Deux définitions des langages de type 2 (langages à contexte libre)**

1.2.1. *Définition par un système*

Soit le système d'équations

$$X_1 = \bigcup_{i \in I_1} \alpha_i^1,$$
$$\cdots\cdots\cdots\cdots$$
$$X_j = \bigcup_{i \in I_j} \alpha_i^j,$$
$$\cdots\cdots\cdots\cdots$$
$$X_n = \bigcup_{i \in I_n} \alpha_i^n,$$

où $I_1, \ldots, I_n$ sont des ensembles finis et $\alpha_i^j$ des mots sur $V \cup \{ X_1, \ldots, X_n \}$.

Un $n$-uple $\mathbf{L} = \{ L_1, \ldots, L_n \}$ de parties de $V^*$ est une solution du système si on a :

$$L_j = \bigcup_{i \in I_j} A_i^j \qquad \text{pour} \quad j = 1, \ldots, n,$$

où $A_i^j$ est obtenu en substituant, pour chaque $k$, $L_k$ à la place de $X_k$ à chacune de ses occurrences, dans $\alpha_j^i$.

Un langage est de type 2 s'il est la première composante de la solution minimale d'un tel système.

*Exemple* 4 : $X = a X b \cup \Lambda$ a pour solution minimale $\{ a^n b^n \mid n \geqq 0 \}$.

1.2.2. *Définition par une expression substitutive*

Dans la caractérisation de McWhirter, la substitution et la substitution itérée jouent un rôle prépondérant.

1.2.2.1. *Substitution*

On appelle substitution de $L$ en $a$ dans $L'$ l'opération notée $[a \leftarrow L](L')$ et définie par

$[a \leftarrow L](L') = \{ \alpha_0 \beta_1 \alpha_1 \ldots \beta_n \alpha_n \mid \text{chaque } \beta_i \in L \text{ et } \alpha_0\, a\, \alpha_1, \ldots, a\, \alpha_n \in L'$ et $a$ n'a pas d'occurrence dans $\alpha_i \}$.

1.2.2.2. *Substitution itérée*

C'est l'opération notée $L^{*a}$ et définie par

$$L^{*a} = \bigcup_{n \geqq 0} (L)_n,$$

où

$$(L)_0 = \{ a \} \qquad \text{et} \qquad (L)_{n+1} = (L)_n \cup L[a \leftarrow (L)_n].$$

Une expression substitutive sur $V$ et $W$ est une expression correctement parenthésée qui utilise uniquement les signes $\cup$, $[a \leftarrow]$, $*^a$ pour $a \in W$, les éléments de $V$ et de $W$ et le signe $\Lambda$.

McWhirter [17] a démontré que pour qu'un langage soit de type 2, il faut et il suffit qu'il puisse être exprimé par une expression substitutive.

*Exemple* 5 : $\{ a^n b^n \mid n \geqq 0 \} = [c \leftarrow \Lambda] (\{ a c b \}^{*c})$.

1.2.3. *Les langages de type* 2 *ne sont pas reconnus par les monoïdes finis*

Les systèmes d'équations que nous avons définis sont liés à la structure de monoïdes de $V^*$. La question que l'on peut se poser est de savoir si tout langage de type 2 est l'image réciproque d'une partie finie d'un monoïde fini. En fait, il n'en est rien, on obtient seulement ainsi les langages de type 3 (*cf.* [7], p. 62) qui forment une famille strictement plus petite.

### 1.3. Plan

Dans la suite, nous allons faire quelques rappels d'algèbre universelle (partie 2) pour définir correctement les notions générales :

– d'ensemble algébrique (partie 3.3), c'est-à-dire solution minimale d'un système d'équations;

– d'ensemble reconnaissable (partie 3.4), c'est-à-dire image inverse d'une partie finie d'une algèbre finie;

– d'ensemble régulier (partie 4), c'est-à-dire obtenu à partir des ensembles finis par substitution et substitution itérée.

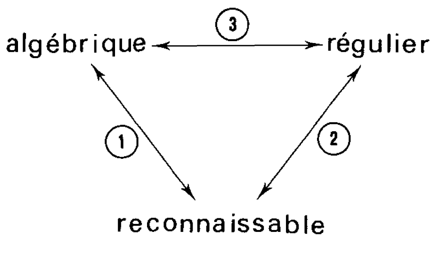


**Figure 2.**
**Trois équivalences.**

Notre but est de montrer un théorème qui généralise le théorème de McWhirter et le théorème de Kleene et affirme l'équivalence entre ensembles algébriques et ensembles réguliers (partie 5), c'est-à-dire l'équivalence (3) de la figure 2. Dans cette figure, les équivalences (1) et (2) qui ne sont vraies que pour les théories libres de base finie ont été démontrées par Mezei et Wright [18] pour (1) et Thatcher et Wright [21] pour (2). Nous allons, quant à nous, montrer l'équivalence (3) dans le cas des théories conformes; dans ce cas plus général, c'est la seule équivalence qui reste valable comme le montre l'examen de la théorie des monoïdes. Nous allons, par le fait, généraliser le théorème de Gruska [11] et de McWhirter [17].

La définition de la notion d'ensemble algébrique suppose que l'on puisse munir l'ensemble des parties d'une structure identique à celle de l'algèbre elle-même, ce n'est pas toujours le cas, c'est pourquoi nous introduisons la notion de théorie conforme (partie 2.2); un contre-exemple simple est celui des groupes; envisageons le groupe $\mathbf{Z}/2\,\mathbf{Z}$, on a :

$$\{0, 1\} + \{0\} = \{0, 1\} = \{0, 1\} + \{1\}.$$

Par conséquent, l'ensemble de ses parties muni du prolongement naturel de l'opération $+$ n'est pas conforme. Cette classification des théories algébriques entre conforme et non conforme est nouvelle et plus commode que la classification entre théorie libre et non libre, en effet, la plupart des théories algébriques que l'on rencontre quand on étudie les langages sont conformes sans être libres (ce qui est le cas pour les monoïdes). Le théorème que nous donnons est une illustration de l'utilité de cette notion : il généralise agréablement des résultats connus sur les théories libres. Ce qu'il faut bien voir, c'est que hors du cadre des théories conformes, on ne peut pas parler d'ensemble algébrique, c'est pourquoi nous reprendrons l'introduction de ce concept dans ce nouveau cadre.

## 2. THÉORIES ALGÉBRIQUES CONFORMES

Nous reprendrons les notations et les concepts d'Eilenberg et Wright [8] à quelques exceptions près cependant : ce que nous appellerons théorie est la catégorie opposée à celle que ces auteurs définissent sous ce nom (*cf.* [19], chap. 3); ainsi les foncteurs contravariants deviennent covariants et les notations postfixées deviennent préfixées. De façon classique, $\mathbf{N}^0$ est la catégorie opposée de $\mathbf{N}$, c'est une sous-catégorie de chaque théorie. Nous ne ferons pas de différences entre l'entier $n$ et l'ensemble $\{1, 2, \ldots, n\}$ de la catégorie $\mathbf{N}$, $n$ est la somme directe de $n$ fois 1 dans $\mathbf{N}$, donc le produit de $n$ fois 1 dans $\mathbf{N}^0$. Les morphismes d'une théorie sont appelés « schémas d'opération » ou « opération »; l'opération $p \to 1$ qui correspond à la $i$-ième projection sera notée $x_i$; c'est un morphisme de la catégorie $\mathbf{N}^0$. De manière assez systématique, nous utiliserons la notation $\mathbf{x}$ pour les $n$-uplets $(x_1, \ldots, x_n)$.

### 2.1. Multiplicité

Si $\mathbf{N}^0[\Omega]$ est une théorie libre sur $\Omega$, on définit pour chaque entier $i$, une fonction de l'ensemble des morphismes de $\mathbf{N}^0[\Omega]$ vers les entiers, notée $m_i$ et appelée multiplicité de $x_i$, elle vérifie les axiomes :

$$MUL\,1 \qquad m_i(x_i) = 1 \qquad \text{où} \quad x_i : p \to 1,$$

$$MUL\,2 \quad m_i(x_k) = 0 \qquad \text{où} \quad x_k : p \to 1 \quad \text{et} \quad k \neq i,$$

$$MUL\,3 \qquad m_i(\varphi) = m_i(x_1\varphi) + \ldots + m_i(x_n\varphi),$$

$$MUL\,4 \qquad \text{si} \quad \omega \in \Omega_n \quad \text{alors} \ m_i(\omega\varphi) = m_i(\varphi).$$

Intuitivement, la multiplicité $m_i(\varphi)$ désigne le nombre d'occurrences de $x_i$ dans $\varphi$.

*Exemple* 6 : Si $\varphi = \pi(x_2, \pi(x_2, x_1))$, $m_1(\varphi) = 1$, $m_2(\varphi) = 2$, $m_3(\varphi) = 0$.

### 2.2. Théorie conforme

Une théorie algébrique est habituellement définie comme le quotient d'une théorie libre $\mathbf{N}^0[\Omega]$ et d'une congruence $Q$ sur cette théorie; la congruence $Q$ elle-même est définie comme la plus petite des congruences qui contienne une famille $\Gamma = \{\Gamma_n/n \text{ entier}\}$ de relations binaires [$\Gamma_n$ est une relation sur $\mathbf{N}^0[\Omega](n, 1)$]. Le couple $(\Omega, \Gamma)$ est appelé une *présentation* de la théorie.

Une présentation est *conforme* si elle vérifie

$$\boxed{\begin{array}{l} CONF \qquad \{\forall n, i \in \mathbf{N}\}, \{\forall \alpha, \beta \in \mathbf{N}^0[\Omega](n, 1)\}, \\ \qquad \{\alpha\Gamma_n\beta \Rightarrow m_i(\alpha) = m_i(\beta) \wedge [m_i(\alpha) = 0 \vee m_i(\alpha) = 1]\}. \end{array}}$$

C'est-à-dire que pour chaque couple relié de $\Gamma_n$, toutes les multiplicités coïncident de part et d'autre et valent un ou zéro. Une théorie est dite conforme si elle admet une présentation conforme.

*Exemple* 7 : La théorie $\mathbf{M}$ des monoïdes est conforme.

*Contre-exemple :* La théorie $\mathbf{G}$ des groupes est habituellement présentée ainsi :

$$\Omega_0 = \{e\} \ \Omega_1 = \{inv\} \ \Omega_2 = \{\pi\} \qquad \text{et} \qquad \Omega_k = \varnothing \quad \text{pour } k > 2,$$

$$\Gamma_1 = \{\pi(x_1, inv(x_1)) \sim e; \pi(x_1, e) \sim x_1\},$$

$$\Gamma_2 = \{\pi(\pi(x_1, x_2), x_3) \sim \pi(x_1, \pi(x_2, x_3))\}$$

et

$$\Gamma_0 = \Gamma_k = \varnothing \quad \text{pour} \quad k > 2.$$

août 1976.

Cette présentation n'est pas conforme, en effet :

$$m_1(\pi(x_1, inv(x_1)) = 2 \neq m_1(e) = 0.$$

REMARQUE : Le cas de $\mathbf{Z}/2\,\mathbf{Z}$ et le théorème de Gautam permettent d'affirmer que $\mathbf{G}$ n'admet aucune présentation conforme.

### 2.3. Théorème de Gautam

Gautam [10] a démontré qu'une théorie $\mathbf{T}$ admet une présentation conforme si et seulement si pour toute $\mathbf{T}$-algèbre $A$, le prolongement des opérations à $\hat{A}$ (ensemble des parties de $A$) est possible et munit $\hat{A}$ d'une structure de $\mathbf{T}$-algèbre. Les théories algébriques que l'on rencontre habituellement dans l'étude des langages formels sont conformes : c'est le cas des théories libres, entre autres celles des algèbres monadiques et c'est le cas de la théorie des monoïdes.

## 3. ENSEMBLES ALGÉBRIQUES ET ENSEMBLES RECONNAISSABLES

A partir de maintenant, nous nous plaçons dans une théorie conforme $\mathbf{T}$ à laquelle nous faisons implicitement référence.

Dans cette partie, nous introduisons la notion d'ensemble algébrique, comme plus petite solution d'un système d'équations. Pour cela, nous définissons ce qu'est une application polynômiale, c'est-à-dire une application de $\mathfrak{P}(A)^k$ vers $\mathfrak{P}(A)^n$ induite par un « polynôme ».

Considérons le cas des monoïdes de base $\{a, b\}$, c'est-à-dire les monoïdes qui ont en plus de l'élément neutre $e$, deux points distingués $a$ et $b$.

$P : (X, Y) \mapsto (a X, Y a X, Y b)$ est un polynôme et

$$Q : \quad (X, Y) \mapsto (a\, Y \cup e, X b)$$

est aussi un polynôme, si

$$L_1 = \{a^n b^n \mid n \geqq 0\},$$
$$L_2 = \{a^n b^{n+1} \mid n \geqq 0\},$$

on a

$$(L_1, L_2) = (a\, L_2 \cup \Lambda, L_1 b),$$

c'est-à-dire que $(L_1, L_2)$ est un point fixe de $Q$, c'est d'ailleurs le seul, donc le plus petit. Sa première composante $L_1$ est alors un ensemble algébrique.

### 3.1. Polynômes

3.1.1. Un polynôme $k \mapsto n$ est un $n$-uple $\mathbf{P} = (P_1, \ldots, P_n)$ où $P_i$ est un sous-ensemble fini de $\mathbf{T}(k, 1)$. Les éléments de $P_i$ sont appelés les constituants de $\mathbf{P}$. Si chaque $P_i$ est réduit à un seul élément, $\mathbf{P}$ est dit monomial.

3.1.2. *Application associée à un polynôme*

Si $A$ est une algèbre, si $\mathbf{X} = (X_1, \ldots, X_k) \in \mathfrak{P}(A)^k$, nous définissons

$$P_i\mathbf{X} = \bigcup_{\varphi \in P_i} \varphi(X_1, \ldots, X_k),$$

$$\mathbf{PX} = (P_1\mathbf{X}, \ldots, P_n\mathbf{X}).$$

Alors $\mathbf{P}$ induit une application $\mathbf{P}_A : \mathfrak{P}(A)^k \to \mathfrak{P}(A^n)$.

$\mathfrak{P}(A)^k$ est muni de la structure de treillis produit, c'est-à-dire :

$$\mathbf{X} \subset \mathbf{Y} \quad \text{si} \quad X_i \subset Y_i \quad \text{pour tout } 1 \leqq i \leqq n,$$

$$\mathbf{X} \cup \mathbf{Y} = (X_1 \cup Y_1, \ldots, X_n \cup Y_n).$$

3.1.3. $\mathbf{P}_A$ *est une application continue, c'est-à-dire :*

Proposition 1 : *Si* $\mathbf{X}^0 \subset \mathbf{X}^1 \subset \ldots \subset \mathbf{X}^m \subset \ldots$ *est une chaîne (c'est-à-dire une suite dénombrable croissante d'ensembles), alors* $\mathbf{P}_A(\bigcup_m \mathbf{X}^m) = \bigcup_m \mathbf{P}_A(\mathbf{X}^m)$. ∎

### 3.2. Point fixe et polynômes

3.2.1. *Théorème du point fixe*

Si $\mathbf{P}$ est un polynôme $n \to n$, le théorème du point fixe [2] affirme que $\mathbf{P}_A$ admet un plus petit point fixe noté $\mathbf{P}_A = (P_{A,1}, \ldots, P_{A,n})$ et que celui-ci est donné par :

$$\mathbf{P}_A = \bigcup_k \mathbf{P}_A^k \varnothing \qquad \text{où} \quad \varnothing = (\varnothing, \ldots, \varnothing) \in \mathfrak{P}(A)^n$$

et

$$\mathbf{P}_A^k = \mathbf{P}_A \circ \mathbf{P}_A \circ \ldots \circ \mathbf{P}_A \; k \text{ fois}.$$

3.2.2. *Transfert du point fixe*

Dans le cas particulier où l'on a affaire à l'algèbre initiale notée $A_0$, nous écrirons $\mathbf{P}$ au lieu de $\mathbf{P}_{A_0}$. La proposition suivante montre le rôle très important joué par l'ensemble $\mathbf{P}$. Si $\xi_A : A_0 \to A$ est l'unique morphisme de $A_0$ vers $A$, nous notons par le même signe $\xi_A$ l'unique morphisme de $\mathfrak{P}(A_0)^n$ vers $\mathfrak{P}(A)^n$ prolongeant $\xi_A$. On a alors :

PROPOSITION 2 : $\bar{\mathbf{P}}_A = \xi_A \bar{\mathbf{P}}$.

La démonstration provient du diagramme commutatif ci-dessous

$$\begin{tikzcd} \mathfrak{P}(A_0)^n \arrow[r, "\mathbf{P}_{A_0}"] \arrow[d, "\xi_A"'] & \mathfrak{P}(A_0)^n \arrow[d, "\xi_A"] \\ \mathfrak{P}(A)^n \arrow[r, "\mathbf{P}_A"'] & \mathfrak{P}(A)^n \end{tikzcd}$$

### 3.3. Ensembles algébriques

Une partie $X$ d'une algèbre $A$ initiale est dite algébrique s'il existe un entier $n$ et un polynôme $\mathbf{P} : n \to n$ tels que $X = \bar{\mathbf{P}}_{A,1}$, c'est-à-dire que $X$ est la première coordonnée de la plus petite solution $\bar{\mathbf{P}}_A$ de l'équation $\mathbf{PX} = \mathbf{X}$. On a les propriétés suivantes :

1) Un singleton est algébrique.

2) L'ensemble vide est algébrique.

3) Si $X_1$ et $X_2$ sont algébriques, il en est de même de $X_1 \cup X_2$.

4) Si $\varphi \in (n, 1)$ et si $X_1, \ldots, X_n$ sont algébriques, alors $(X_1, \ldots, X_n)$ l'est aussi.

### 3.4. Ensembles reconnaissables

Un sous-ensemble $X$ de $A_0$ est reconnaissable s'il existe une algèbre finie $A$ et une partie $t$ de $A$ telles que $X = \xi_A^{-1}\, t$. Mezei et Wright ([18], *voir* aussi [8]) ont montré :

THÉORÈME 1 : *Si $A_0$ est l'algèbre initiale d'une théorie libre finement engendrée (c'est-à-dire que $\bigcup_k \Omega_k$ est finie), les ensembles reconnaissables et algébriques coïncident.* ■

Ce théorème ne s'étend pas aux théories libres engendrées par une famille infinie; par exemple, si $V^*$ est l'algèbre monadique initiale sur un ensemble $V = \{ a_1, \ldots, a_n, \ldots \}$ infini, $V^*$ est reconnaissable [reconnu par exemple par $(\{ \lambda \}, \{ \lambda \})$], mais n'est pas algébrique car un polynôme n '« utilise » qu'une famille $V'$ finie d'éléments de $V$ et admet toujours comme plus petite solution un $n$-uplet de parties de $V'^*$.

Ce théorème ne s'étend pas non plus aux théories conformes puisqu'il est faux dans le cas de la théorie des monoïdes : en effet, dans ce cas, les ensembles algébriques sont les langages à contexte libre ou de type 2 (dans la classification de Chomsky) et leur famille contient strictement celle des ensembles reconnaissables qui sont les langages de type 3.

## 4. ENSEMBLES RÉGULIERS

Avant de définir les ensembles réguliers et de les utiliser, nous allons préciser quelques notions relatives aux algèbres libres.

### 4.1. Algèbres libres

4.1.1. *Introduction*

Dans [8] et dans [19], on trouve introduite la notion d'algèbre libre sur un ensemble fini [en l'occurrence l'intervalle $\{1, \ldots, k\}$ des entiers pour tout $k$; il s'agit de $\mathbf{T}(k, 1)$]; il n'est guère plus difficile de définir une algèbre libre sur $V$ pour tout ensemble fini $V$; nous la noterons $\mathbf{T}(V)$. Nous considérons dorénavant $\mathbf{T}(\{x_1, \ldots, x_k\})$ et $\mathbf{T}(k, 1)$ comme la même algèbre.

*Exemple* 8 :

1) Une algèbre monadique sur $V$ libre sur $\Sigma$ est par exemple l'ensemble $V^*(\Sigma \cup \{\lambda\})$ des mots composés d'une suite finie d'éléments de $V$ terminée par $\lambda$ ou par un élément de $\Sigma$.

2) Une algèbre libre sur $V$ de la théorie $\mathbf{M}$ des monoïdes, c'est-à-dire un monoïde libre sur $V$ est l'ensemble $V^*$ des mots sur $V$.

4.1.2. *Les algèbres libres comme algèbre initiale d'une théorie*

Considérons la théorie $\mathbf{T}$ présentée par $(\Omega, R)$, on peut construire une théorie, notée $\mathbf{T}[V]$ et présentée par $(\Omega', R')$ de la manière suivante : $\Omega'_0 = \Omega_0 \cup V$ (on suppose $V$ disjoint de $\Omega_0$), $\Omega'_i = \Omega_i$ pour $i \geqq 1$ et $R_i = R'_i$ pour tout $i$; la théorie $\mathbf{T}[V]$ est dite obtenue à partir de la théorie $\mathbf{T}$ par adjonction d'une famille $V$ de constantes.

La catégorie des $\mathbf{T}[V]$-algèbres est une sous-catégorie de la catégorie des $\mathbf{T}$-algèbres; elle est formée des $\mathbf{T}$-algèbres dans lesquelles on a distingué les images des éléments de $V$, les $\mathbf{T}[V]$ morphismes sont ceux qui conservent ces images. Une $\mathbf{T}[V]$-algèbre initiale est alors une $\mathbf{T}$-algèbre libre sur $V$.

4.1.3. *Preuves par récurrence dans les algèbres libres*

Pour prouver qu'une propriété Prop $(x)$ est vraie pour tout $x$ d'une algèbre libre sur $V$, il suffit de prouver :

$$(REC\,1) \qquad \mathrm{Prop}(a) \text{ pour tout } a \in V,$$

et

$$(REC\,2) \qquad \mathrm{Prop}(x_1) \wedge \ldots \wedge \mathrm{Prop}(x_n) \wedge \varphi \in \mathbf{T}(n, 1) \Rightarrow \mathrm{Prop}(\varphi(x_1), \ldots, \varphi(x_n)).$$

On peut justifier cela de la manière suivante : supposons que $P$ est une application de $\mathbf{T}(V)$ vers $\{ vrai, faux \}$; si l'on considère l'algèbre à un seul élément $\{ \alpha \}$, l'algèbre de ses parties $\{ \emptyset, \{ \alpha \} \}$ est une algèbre à deux éléments où l'on fait correspondre $\{ \alpha \}$ à *vrai* et $\emptyset$ à *faux*.

On voit alors que $\{ vrai \}$ est une sous-algèbre et que Prop est un morphisme de $\mathbf{T}(V)$ vers cette algèbre; c'est aussi le seul, de $\mathbf{T}(V)$, vers $\{ vrai, faux \}$, qui vérifie (REC 1), donc Prop est identiquement vraie.

### 4.2. Substitution

4.2.1. *Définition de la substitution*

Soient $a \in V$ et $L$ un sous-ensemble de $\mathbf{T}(V)$. Considérons l'application sb $\{ a, L \}$ de $V$ vers $\mathfrak{P}(\mathbf{T}(V))$ définie par :

$$\mathrm{sb}\{a, L\}(a) = L,$$

$$\mathrm{sb}\{a, L\}(b) = \{b\} \qquad \text{si} \quad b \neq a,$$

puisque $\mathbf{T}$ est conforme, $\mathfrak{P}(\mathbf{T}(V))$ est une $\mathbf{T}$-algèbre, donc sb $\{ a, L \}$ se prolonge de manière unique par un morphisme $[a \leftarrow L]$ :

$$\mathbf{T}(\mathrm{V}) \to \mathfrak{P}(\mathbf{T}(V)).$$

L'image d'un élément $r$ par ce morphisme est notée $[a \leftarrow L](r)$.

Notons que si $r \in \mathbf{T}(V - \{ a \})$, alors $[a \leftarrow L](r) = r$.

*Exemple* 9 : Soit $V = \{ a, b, c \}$. Plaçons-nous dans le monoïde libre $V^*$ si $L = \{ ac, b \}$ :

$$[a \leftarrow L](aa) = \{acac, acb, bac, b^2\},$$

$$[a \leftarrow L](bcb) = [a \leftarrow \emptyset](bcb) = bcb.$$

4.2.2. *Substitution d'un ensemble dans un autre*

Le morphisme $[a \leftarrow L]$ s'étend de manière unique en un morphisme toujours noté $[a \leftarrow L]$ de $\mathfrak{P}(\mathbf{T}(V))$ vers $\mathfrak{P}(\mathbf{T}(V))$; il est ainsi défini :

$$[a \leftarrow L](L') = \bigcup_{x \in L'} [a \leftarrow L](x).$$

4.2.2.1. *Une propriété de la substitution*

Soit $\mathbf{P} = (P_1, \ldots, P_m)$ un polynôme $k \to m$ de la théorie $\mathbf{T}[V]$; si $a \in V$, on peut aussi lui associer un polynôme $\mathbf{Q} = (Q_1, \ldots, Q_m) : k+1 \to m$ de la théorie $\mathbf{T}[V - \{ a \}]$ de la manière suivante : « on remplace toute occurrence de $a$ dans $\mathbf{P}$ par $x_{k+1}$ », ce qui s'énonce plus formellement ainsi : $\mathbf{T}[V](k, 1)$ est une $\mathbf{T}$-algèbre libre sur $V \cup k$, par conséquent, l'application

$$f : \quad V \cup k \to (V - \{a\}) \cup k+1,$$

où $(V-\{a\}) \cup k+1$ est considéré comme un sous-ensemble de

$$\mathbf{T}[V-\{a\}](k+1, 1)$$

et où

$$f(b) = b \qquad \text{si} \quad b \in V-\{a\},$$
$$f(a) = x_{k+1},$$
$$f(x_i) = x_i \qquad \text{si} \quad 1 \leqq i \leqq k,$$

se prolonge de manière unique en un morphisme

$$\bar{f}: \mathbf{T} \quad [\mathrm{V}](k, 1) \rightarrow \quad [\mathbf{T}-\{a\}](k+1, 1),$$

ce morphisme est d'ailleurs un isomorphisme.

NOTATION : Dans la proposition qui suit, nous adopterons les notations

$$P_i = \bigcup_j \varphi_{ij}, \qquad \bar{\varphi} = \bar{f}(\varphi), \qquad Q_i = \bigcup_j \bar{\varphi}_{ij}.$$

Avec ces notations, on a

LEMME : *Si* $\varphi \in \mathbf{T}[V](k+1)$, *alors*

$$[a \leftarrow L](\varphi(\mathbf{r})) = \bar{\varphi}([a \leftarrow L](r_1), \ldots, [a \leftarrow L](r_k), L).$$

Considérons la propriété

$$\operatorname{Prop}(\varphi): \quad [a \leftarrow L](\varphi(\mathbf{r})) = \bar{\varphi}([a \leftarrow L](r_1), \ldots, [a \leftarrow L](r_k), L).$$

Cette propriété va être montrée par récurrence pour tous les éléments de la $\mathbf{T}$-algèbre libre sur $V \cup k$ :

si $\varphi = b \in V$ et $b \neq a$, on a $\bar{\varphi} = b$ et Prop $(\varphi)$ tient

pour $\varphi = a$, on a $\varphi(\mathbf{r}) = a$ et $[a \leftarrow L](a) = L$,

par conséquent, $\bar{\varphi} = x_{k+1}$ et $\bar{\varphi}(\ldots, L) = L$, donc on a encore Prop $(\varphi)$ :

pour $\varphi = x_i$, on a $\varphi = \bar{\varphi} = x_i$ :

$$[a \leftarrow L](\varphi(\mathbf{r})) = [a \leftarrow L](r_i) = \bar{\varphi}(\ldots, [a \leftarrow L](r_i), \ldots, [a \leftarrow L](x_k), L).$$

Soient

$$\psi \in \mathbf{T}(n, 1) \qquad \text{et} \qquad \varphi_1, \ldots, \varphi_n \in \mathbf{T}[V](k, 1)$$

tels que Prop $(\varphi_1), \ldots,$ Prop $(\varphi_n)$.

On sait que

$$\overline{\psi(\varphi_1, \ldots, \varphi_n)} = \psi(\bar{\varphi}_1, \ldots, \bar{\varphi}_n),$$

$$\begin{aligned}
&[a \leftarrow L](\psi(\varphi_1(\mathbf{r}), \ldots, \varphi_n(\mathbf{r}))\\
&\quad = \psi(\ldots, [a \leftarrow L](\varphi_i(\mathbf{r})), \ldots)\\
&\quad = \psi(\ldots, \bar{\varphi}_i([a \leftarrow L](r_1), \ldots, [a \leftarrow L](r_k), L)\ldots)\\
&\quad = \overline{\psi(\varphi_1, \ldots, \varphi_n)}([a \leftarrow L](r_1), \ldots, [a \leftarrow L](r_k), L). \quad \blacksquare
\end{aligned}$$

PROPOSITION 3 : *Avec les notations ci-dessus, on a*

$$[a \leftarrow L'](P_j(\mathbf{L})) = Q_j([a \leftarrow L'](L_1), \ldots, [a \leftarrow L'](L_k), L').$$

Sans nuire à la généralité, on peut supposer $P$ monomial, autrement dit,

$$[a \leftarrow L'](P_j(\mathbf{L})) = [a \leftarrow L'](\varphi_j(\mathbf{L})) = \bigcup_{\mathbf{r} \in \mathbf{L}} [a \leftarrow L']\varphi_j(\mathbf{r})$$

où $\varphi_j$ est l'unique élément de $P_j$.

Le résultat découle alors du lemme et des propriétés de la substitution. ■

4.2.3. *Substitution itérée d'un ensemble*

4.2.3.1. *Définition*

La substitution itérée transforme un sous-ensemble $L$ de $\mathbf{T}(V)$ en un sous-ensemble noté $L^{*a}$ de $\mathbf{T}(V - \{a\})$. Elle est définie par $L^{*a} = \bigcup_{p \geqq 0} L^{pa}$ où

$$L^{0a} = \emptyset \qquad \text{et} \qquad L^{pa} = [a \leftarrow L^{(p-1)a}](L).$$

$L^{*a}$ est la plus petite solution de $X = [a \leftarrow X](L)$.

4.2.3.2. *Comparaison avec les autres définitions*

La substitution itérée que nous proposons, diffère de celle proposée habituellement, par le fait que $L^{0a} = \emptyset$, alors que les autres auteurs (sauf Engelfriet [24]) proposent $L^{0a} = L$ (Gruska, [11]) ou $L^{0a} = \{a\}$ (McWhirter, [17], Thatcher et Wright, [21]).

Nous l'avons choisie ainsi pour deux raisons :

1) La substitution itérée effectuée, il semble préférable que la « variable » par rapport à laquelle on l'a effectuée ait disparu.

2) La présentation que nous faisons s'intègre agréablement dans le cadre de la théorie du point fixe, en effet, $L^{*a}$ est la plus petite solution de l'équation simple

$$X = [a \leftarrow X](L).$$

*Exemple de substitution itérée :* Si $\{a, b, c\}^*$ est le monoïde libre sur $\{a, b, c\}$ et si $L = \{bab, c\}$ :

$$L^{1a} = \{c\},\ L^{2a} = \{bcb, c\},\ L^{3a} = \{b^2cb^2, bcb, c\}$$

et

$$L^{*a} = \{b^n cb^n \mid n \geqq 0\}.$$

4.2.3.3. *Des propriétés de la substitution itérée*

Nous donnons ici quelques propriétés de la substitution itérée qui interviendront dans la suite.

Soit $\mathbf{P} = (P_1, \ldots, P_m)$ un polynôme $k \to m$ de la théorie $\mathbf{T}[V]$; si $a \in V$, on peut lui associer un polynôme $\mathbf{R} = (R_1, \ldots, R_m)$ de la théorie $\mathbf{T}[V - \{a\}]$ de la manière suivante : « on remplace toute occurrence de $a$ dans $\mathbf{P}$ par $x_1$ ».

NOTATION : Dans les propositions qui suivent, nous adopterons les notations

$$P_i = \bigcup_j \varphi_{ij}, \qquad R_i = \bigcup_{ij} \tilde{\varphi}_{ij}.$$

PROPOSITION 4 : *Si $L_1$ n'a pas d'occurrence de $a$, c'est-à-dire si*

$$L_1 \subset \mathbf{T}(V - \{a\}) :$$

$$[a \leftarrow L_1]\, P_j(L_1, L_2, \ldots, L_m) = R_j(L_1, [a \leftarrow L_1](L_2), \ldots, [a \leftarrow L_1](L_m)).$$

Donnons-en tout de suite le corollaire qui nous servira.

COROLLAIRE : *Si $L \subset \mathbf{T}[V]$, alors*

$$\begin{aligned}&[a \leftarrow L^{*a}]\, P_j(L^{*a}, L_2, \ldots, L_m)\\ &\quad = R_j(L^{*a}, [a \leftarrow L^{*a}](L_2), \ldots, [a \leftarrow L^{*a}](L_m)).\end{aligned}$$

Ici aussi nous pouvons supposer $P_j$ monomial, il nous faut alors montrer que

$$[a \leftarrow L_1]\, \varphi(L_1, L_2, \ldots, L_m) = \tilde{\varphi}(L_1, \ldots, [a \leftarrow L_1](L_j), \ldots).$$

Nous le ferons par récurrence :

si $\varphi = b \neq a$ ou $\varphi = x_i\ (i \neq 1)$, le résultat est immédiat;

si $\varphi = a$, alors $\tilde{\varphi} = x_1$ et $\tilde{\varphi}(L_1, \ldots, L_m) = L_1$ et

$$[a \leftarrow L_1]\, \varphi(L_1, \ldots, L_m) = L_1 = \varphi(L_1, \ldots);$$

si $\varphi = x_1$, alors $\tilde{\varphi} = x_1$ :

$$[a \leftarrow L_1]\, \varphi(L_1, \ldots, L_m) = [a \leftarrow L_1](L_1) = L_1 = \varphi(L_1, \ldots, L_m).$$

Supposons que $\varphi_1, \ldots, \varphi_n$ vérifie la propriété et soit $\psi \in \mathbf{T}(n, 1)$, on a alors

$$\widetilde{\psi(\varphi_1, \ldots, \varphi_n)} = \psi(\tilde{\varphi}_1, \ldots, \tilde{\varphi}_n)$$

et

$$\begin{aligned}
&[a \leftarrow L_1](\psi(\varphi_1(\mathbf{L}), \ldots) \\
&\quad = \psi(\ldots, [a \leftarrow L_1]\varphi_i(\mathbf{L}), \ldots) \\
&\quad = \psi(\ldots, \tilde{\varphi}_i(L_1, \ldots, [a \leftarrow L_1](L_k), \ldots) \\
&\quad = \widetilde{\psi(\varphi_1, \ldots, \varphi_n)}(L_1, \ldots, [a \leftarrow L_1](L_k), \ldots). \quad \blacksquare
\end{aligned}$$

Cette proposition a deux variantes.

PROPOSITION 5 : *Si $L \subset \mathbf{T}(V)$, alors*

$$[a \leftarrow L]\,P_j(L_1, \ldots, L_m) \subset R_j(L \cup [a \leftarrow L](L_1), L_2, \ldots, L_m).$$

Nous ne donnerons pas la démonstration complète qui se fait par récurrence comme celle de la proposition 4; examinons le point clé, c'est-à-dire les cas $\varphi = a$ et $\varphi = x_1$;

si $\varphi = a$, alors $\tilde{\varphi} = x_1$ et

$$\begin{aligned}
[a \leftarrow L]\,\varphi(L_1, \ldots, L_m) &= [a \leftarrow L](a) = L \\
&\subset \tilde{\varphi}(L \cup [a \leftarrow L](L_1), \ldots, L_m) = L \cup [a \leftarrow L](L_1);
\end{aligned}$$

si $\varphi = x_1$, alors $\tilde{\varphi} = x_1$ et

$$\begin{aligned}
[a \leftarrow L]\,\varphi(L_1, \ldots, L_m) &= [a \leftarrow L](L_1) \\
&\subset \tilde{\varphi}(L \cup [a \leftarrow L](L_1), \ldots, L_m) = L \cup [a \leftarrow L](L_1).
\end{aligned}$$

PROPOSITION 6 :

$$[a \leftarrow L^{*a}]\,P_j(L, L_2, \ldots, L_m) = R_j(L^{*a}, [a \leftarrow L^{*a}](L_2), \ldots, [a \leftarrow L^{*a}](L_m)).$$

### 4.3. Ensembles réguliers

Un sous-ensemble d'une $\mathbf{T}$-algèbre libre $\mathbf{T}(W)$ sera dit $\mathbf{T}$-régulier (ou simplement régulier s'il n'y a pas d'ambiguïté) s'il est obtenu à partir des ensembles finis d'une $\mathbf{T}$-algèbre libre $\mathbf{T}(V)$ (où $V \supset W$) par un nombre fini de substitutions ou substitutions itérées. Cette définition généralise la notion de langage régulier au sens du théorème de Kleene (*cf.* 1.1.3), c'est-à-dire engendré par une expression régulière. Notons que nous n'utilisons pas la réunion dans la définition, car celle-ci peut être obtenue par substitution; en effet, si $L_1$ et $L_2$ sont des sous-ensembles de $\mathbf{T}(V)$ et si $L_3 = \{a, b\}$ où $a$ et $b$ n'appartiennent pas à $V$ :

$$L_1 \cup L_2 = [b \leftarrow L_1][a \leftarrow L_2](L_3).$$

On aurait pu utiliser la réunion dans la définition et on aurait alors remplacé « ensembles finis » par « singletons ».

*Exemple d'ensembles réguliers :* Dans le cas de $\{a, b, c\}^*$ monoïde libre sur $\{a, b, c\}$ on a vu que $\{b^n cb^n \mid n \geqq 0\} = \{bab, c\}^{*a}$, donc c'est un ensemble $\mathbf{M}$-régulier.

## 5. ÉQUIVALENCE ENTRE LA FAMILLE DES ENSEMBLES RÉGULIERS ET LA FAMILLE DES ENSEMBLES ALGÉBRIQUES

### 5.1. Énoncé du théorème

*Dans l'algèbre initiale, un ensemble est régulier si et seulement si il est algébrique.*

NOTATON : Si $\mathbf{P} = (P_1, \ldots, P_m)$ est un polynôme, nous allons poser :

$$p_j^0 = \varnothing,$$

$$p_j^k = P_j(p_1^{k-1}, \ldots, p_m^{k-1}) \quad \text{pour tout } j \text{ compris entre 1 et } m.$$

### 5.2. Stabilité de la famille des ensembles algébriques par substitution

PROPOSITION 7 : *La famille des ensembles algébriques est stable par substitution.*

Soient $L = \overline{P}_1$ où $\mathbf{P} = (P_1, \ldots, P_m)$ et $L' = \overline{Q}_1$ où $\mathbf{Q} = (Q_1, \ldots, Q_m)$, deux ensembles algébriques.

Montrons que $[a \leftarrow L'](L)$ est solution minimale du polynôme $\mathbf{R} = (R_1, \ldots, R_{n+m})$, construit ainsi :

★ si $1 \leqq j \leqq m$, $R_j$ est obtenu en substituant $x_{m+1}$ à $a$ dans $P_j$ (*cf.* 4.2.2.1);

★ si $1 \leqq j \leqq n$, $R_{j+m}$ est obtenu en « décalant » de $m$ les indices des variables qui figuraient dans $Q_j$, autrement dit en substituant $x_{j+m}$ à $x_j$ dans $Q_j$.

Remarquons que si $1 \leqq j \leqq n$ :

$$R_{j+m}(\varnothing, \ldots, \varnothing, X_1, \ldots, X_m) = Q_j(X_1, \ldots, X_m),$$

car $R_{j+m}$ ne contient pas de variables $x_i$ pour $1 \leqq i \leqq m$; donc $\overline{R}_{m+1} = \overline{Q}_1 = L'$.

Considérons la suite d'ensembles définie par

$$\tilde{r}_j^{k+1} = R_j(\tilde{r}_1^k, \ldots, \tilde{r}_{m+n}^k)$$

et

$$\tilde{r}_j^0 = \emptyset \qquad \text{si} \quad 1 \leqq j \leqq m,$$

$$\tilde{r}_j^0 = \bar{R}_j \qquad \text{si} \quad m < j \leqq m+n.$$

On voit facilement que pour tout $k$, $r_j^k \subset \tilde{r}_j^k \subset \bar{R}_j$, en particulier $\tilde{r}_j^k = \bar{R}_j$ si $j > m$. Par conséquent, $\bigcup_{k \geqq 0} \tilde{r}_j^k = \bar{R}_j$. Montrons que pour $j = 1 \ldots m$ :

$$\tilde{r}_j^k = [a \leftarrow L'](p_j^k).$$

C'est immédiat si $k = 0$; supposons le résultat vrai pour $k-1$ :

$$\begin{aligned}
\tilde{r}_j^k &\overset{(1)}{=} R_j(r_1^{k-1}, \ldots, r_m^{k-1}, \bar{R}_{m+1}, \ldots, R_{m+n}),\\
&\overset{(2)}{=} R_j([a \leftarrow L'](p_1^{k-1}), \ldots, [a \leftarrow L'](p_m^{k-1}), L', \bar{R}_{m+2}, \ldots, \bar{R}_{m+n}),\\
&\overset{(3)}{=} [a \leftarrow L'](P_j(p_1^{k-1}, \ldots, p_m^{k-1})),\\
&\overset{(4)}{=} [a \leftarrow L'](p_j^k).
\end{aligned}$$

(1) est la définition de $r_j^k$;

(2) par hypothèse de récurrence;

(3) d'après la définition de $R_j$ pour $1 \leqq j \leqq m$ et d'après la proposition 3;

(4) d'après la définition de $p_j^k$.

De ce résultat, on tire :

$$\begin{aligned}
\bar{R}_j = \bigcup_{k \geqq 0} \tilde{r}_j^k &= \bigcup_{k \geqq 0} [a \leftarrow L'](p_j^k) = [a \leftarrow L'](\bigcup_{k \geqq 0} p_j^k)\\
&= [a \leftarrow L'](\bar{P}_j),
\end{aligned}$$

en particulier $[a \leftarrow L'](L) = \bar{R}_1$. ■

### 5.3. Stabilité de la famille des ensembles algébriques par substitution itérée

PROPOSITION 8 : *La famille des ensembles algébriques est stable par substitution itérée.*

En définissant **R** comme dans le paragraphe 4.2.3.3, nous allons montrer que $\bar{P}_1^{*a} = \bar{R}_1$.

*Exemple* 10 : Considérons dans $\{a, b, c\}^*$ le polynôme

$$P_1 = ax_2 \cup c \cup \Lambda,$$

$$P_2 = x_1 b.$$

Sa solution minimale est le couple $(L_1, L_2)$ où

$$L_1 = \{a^n cb^n \mid n \geqq 0\} \cup \{a^n b^n \mid n \geqq 0\}$$

$$L_2 = \{a^n cb^{n+1} \mid n \geqq 0\} \cup \{a^n b^{n+1} \mid n \geqq 0\}.$$

On voit que $L_1^{*c} = \{a^k b^k \mid k \geqq 0\}$ et que cet ensemble est première composante de la solution minimale du polynôme obtenu en remplaçant toute occurrence de $c$ par $x_1$, c'est-à-dire

$$x_1 = ax_2 \cup x_1 \cup \Lambda,$$

$$x_2 = x_1 b.$$

LEMME 1 : *Si* $L \subset \overline{R}_1$, *alors* $[a \leftarrow L](p_j^{k-1}) \subset \overline{R}_j$.

Pour $k = 0$, on a $[a \leftarrow K](\varnothing) = \varnothing \subset \overline{R}_j$.

Si la propriété est vraie pour $k-1$, on a alors $[a \leftarrow L](p_j^{k-1}) \subset \overline{R}_j$ pour tout $j$ et donc

$$\begin{aligned}[a \leftarrow L](p_j^k) &= [a \leftarrow L](P_j(p_1^{k-1}, \ldots, p_m^{k-1})) \\ &\subset R_j(L \cup [a \leftarrow L](p_1^{k-1}), \ldots, [a \leftarrow L](p_j^{k-1}), \ldots) \\ &\subset R_j(\overline{R}_1, \ldots, \overline{R}_m) = \overline{R}_j.\end{aligned}$$

La première inclusion provient de la proposition 5 du paragraphe 4.2.3.3, la seconde de l'hypothèse de récurrence et de la croissance de **R**. ∎

Comme $\overline{P}_j = \bigcup_{k \geqq 0} p_j^k$, on obtient donc

$$[a \leftarrow L](\overline{P}_j) = [a \leftarrow L](\bigcup_{k \geqq 0} p_j^k) = \bigcup_{k \geqq 0} [a \leftarrow L](p_j^k) \subset \overline{R}j.$$

En particulier, si $L \subset \overline{R}_1$, on a $[a \leftarrow L](\overline{P}_1) \subset \overline{R}_1$, ce qui va nous servir à démontrer le lemme suivant :

LEMME 2 : $\overline{P}_1^{*a} \subset \overline{R}_1$.

Il est immédiat que $\overline{P}_1^{0a} = \varnothing \subset \overline{R}_1$.

Supposons $\overline{P}_1^{(n-1)a} \subset \overline{R}_1$ et alors, d'après ce qui précède

$$\overline{P}_1^{na} \subset [a \leftarrow \overline{P}_1^{(n-1)a}](\overline{P}_1) \subset \overline{R}_1,$$

ainsi

$$\bar{P}_1^{*a} = \bigcup_{n \geqq 0} \bar{P}_1^{na} \subset \bar{R}_1. \quad \blacksquare$$

Réciproquement, montrons que $\bar{R}_1 \subset \bar{P}_1^{*a}$ ; pour cela, montrons que $\bar{P}_1^{*a}$ est la première composante d'une solution du polynôme **R**. Choisissons-la ainsi :

$$L_1 = \bar{P}_1^{*a},$$

$$L_j = [a \leftarrow \bar{P}_1^{*a}](\bar{P}_j).$$

On a alors d'après la proposition 6 :

$$R_j(L_1, \ldots, L_{n+m}) = [a \leftarrow \bar{P}_1^{*a}]\, P_j(\bar{P}_1, \bar{P}_2, \ldots, \bar{P}_n)$$
$$= [a \leftarrow \bar{P}_1^{*a}](\bar{P}_j) = L_j. \quad \blacksquare$$

PROPOSITION 9 : *Tout ensemble régulier est algébrique.*

Vue les deux propositions précédentes et vu le fait que les ensembles finis sont algébriques, ce résultat est immédiat.

### 5.4. Inclusion de la famille des algébriques dans celle des réguliers

PROPOSITION 10 : *Tout ensemble algébrique est régulier.*

*Remarques préliminaires :* On a vu que $L_1 \cup L_2$ est obtenu par substitution. D'autre part, si $L_1, \ldots, L_n$ sont des ensembles et $\varphi \in \mathbf{T}(n, 1)$,

$$L = \varphi(L_1, \ldots, L_n)$$

est obtenu par substitution; en effet, si $L' = \{ \varphi(a_1, \ldots, a_n) \}$ :

$$L = [a_n \leftarrow L_n]([a_{n-1} \leftarrow L_{n-1}](\ldots([a_1 \leftarrow L_1](L'))\ldots)).$$

*Démonstration de la proposition :* Soient $L$ un ensemble algébrique et $\mathbf{P} = (P_1, \ldots, P_n)$ un polynôme dont « $L$ est solution »; par commodité, nous supposerons sans nuire à la généralité qu'ici $L = \bar{P}_n$.

Nous allons raisonner par récurrence sur $n$.

5.4.1. *Cas* $n = 1$

$P = \bigcup_{i=1}^{n} \varphi_i$ où $\varphi_i \in \mathbf{T}(1,1)$, alors $\bar{P} = P^{*x_1}$, ici $P$ est vu comme sous-ensemble fini de l'algèbre $\mathbf{T}(1,1)$ libre sur $\{ x_1 \}$. Cela provient immédiatement des définitions

$$\bar{P}_1 = \bigcup_{k \geqq 0} p_1^k = \bigcup_{k \geqq 0} P_1^{kx} = P^{*x_1}.$$

5.4.2. *Cas général*

Avant de démontrer le cas général, posons quelques notations :

– $\mathbf{P} = (P_1, \ldots, P_n)$ est un polynôme à $n$ variables;

– $\mathbf{Q} = (Q_1, \ldots, Q_{n-1})$ est un polynôme à $n-1$ variables, déduit de $\mathbf{P}$ en supprimant $P_n$ et en considérant $x_n$ comme constante.

La solution minimale $\overline{\mathbf{Q}}$ est un $n$-uplet de sous-ensembles de l'algèbre initiale $\mathbf{T}(\{x_n\})$ et par hypothèse de récurrence $\overline{Q}_i$ est régulier.

Nous noterons $Q_n$ le sous-ensemble fini de $\mathbf{T}(\{x_n\})(n-1,1)$ déduit de $P_n$ en supposant $x_n$ constant. L'ensemble $M = Q_n(\overline{Q}_1, \ldots, Q_{n-1})$ est régulier.

Posons $L_n = M^{*x_n}$ et $L_j = [x_n \leftarrow L_n](\overline{Q}_j)$ pour $1 \leqq j \leqq n-1$. $L_n$ est régulier ainsi que $L_j$. Il reste à montrer que $L_n = \overline{P}_n$.

*Première étape :* $\overline{P}_n \subset L_n$.

Pour cela, il suffit de montrer que

$$\mathbf{P}(L_1, \ldots, L_n) = (L_1, \ldots, L_n).$$

Or

$$P_j(L_1, \ldots, L_{n-1}, L_n) = P_j([x_n \leftarrow L_n](\overline{Q}_1), \ldots, [x_n \leftarrow L_n](\overline{Q}_{n-1}), L_n).$$

On applique la proposition 3 (en intervertissant les rôles de $P$ et $Q$ et en remplaçant $a$ par $x_n$) :

$$P_j(L_1, \ldots, L_n) = [x_n \leftarrow L_n](Q_j(\overline{Q}_1, \ldots, \overline{Q}_{n-1});$$

si $1 \leqq j \leqq n-1$ :

$$= [x_n \leftarrow L_n](\overline{Q}_j) = L_j;$$

si $j = n$ :

$$= [x_n \leftarrow L_n](M) = [x_n \leftarrow M^{*x_n}](M)$$
$$= L_n.$$

*Deuxième étape :* $L_n \subset \overline{P}_n$.

Nous avons besoin de plusieurs lemmes.

LEMME 1 : *Pour tout* $k \geqq 0$, *tout* $i\,(1 \leqq i \leqq n-1)$, $L \subset \overline{P}_n$ *implique* $[x_n \leftarrow L](q_i^k) \subset \overline{P}_i$.

On démontre cela par récurrence sur $k$. Si $k = 0$ :

$$[x_n \leftarrow L](\varnothing) = \varnothing \subset \overline{P}_i.$$

Si la propriété est vraie pour $k-1$, d'après la proposition 3 :

$$[x_n \leftarrow L](q_i^k) = P_i([x_n \leftarrow L](q_1^{k-1}), \ldots, [x_n \leftarrow L](q_{n-1}^{k-1}), L).$$

Or chaque ensemble qui intervient est inclus dans $\overline{P}_i$, donc :

$$[x_n \leftarrow L](q_i^k) \subset \overline{P}_i. \quad \blacksquare$$

Lemme 2 : *Si* $L \subset \overline{P}_n$, *alors* $[x_n \leftarrow L](\overline{Q}_i) \subset \overline{P}_i$. $\blacksquare$

Lemme 3 : *Si* $L \subset \overline{P}_n$, *alors* $[x_n \leftarrow L](M) \subset \overline{P}_n$.
En effet

$$\begin{aligned}[x_n \leftarrow L](M) &= [x_n \leftarrow L](P_n(\overline{Q}_1, \ldots, \overline{Q}_{n-1}, x_n)) \\ &= P_n([x_n \leftarrow L](\overline{Q}_1), \ldots, [x_n \leftarrow L](\overline{Q}_{n-1}), L).\end{aligned}$$

Or d'après le lemme 2, chaque terme de ce $n$-uplet est inclus dans $\overline{P}_i$. $\blacksquare$

Lemme 4 : *Pour tout* $k \geqq 0$, $M^{kx_n} \subset \overline{P}_n$ :
si $k = 0$, c'est évident en appliquant le lemme 3 pour $L = \emptyset$;

si $k \geqq 1$ et si le résultat est vrai pour $k-1$, on obtient alors :

$$M^{kx_n} = [x_n \leftarrow M^{(k-1)x_n}](M)$$

et on applique le lemme 3 et l'hypothèse de récurrence.

*Démonstration de la deuxième étape :* Elle nous est donnée par le lemme 5.

Lemme 5 : $M^{*x_n} \subset \overline{P}_n$.
$M^{*x_n} = \bigcup_{k \geqq 0} M^{kx_n}$, or chaque $M^{kx_n}$ est inclus dans $\overline{P}_n$ d'après le lemme 4, donc $M^{*x_n} \subset \overline{P}_n$. $\blacksquare$

## 6. CONSÉQUENCES ET APPLICATIONS

### 6.1. Applications aux algèbres monadiques

Si nous reprenons à la lumière du théorème les exemples du paragraphe 1.1, nous sommes amenés à distinguer deux cas : suivant que $A$ est fini ou infini; si $A$ est fini, les théorèmes de Thatcher et Wright [21] et de Mezei et Wright ([18] et [8]) s'appliquent et donnent en définitive le théorème de Kleene ([14]). En effet, il est très facile de montrer dans ce cas précis, l'équivalence entre les reconnaissables et les algébriques (*voir*, par exemple, [13], p. 33). Si $A$ est infini, le résultat est plus significatif puisqu'alors on sort du domaine d'application des théorèmes de Thatcher et Wright et de Mezei et Wright.

6.1.1. *Cas où $A$ est fini*

Ici les ensembles algébriques sont les langages de $A^*$, solutions minimales des systèmes linéaires à droite (*cf.* [7], 1.1). Le théorème de Kleene est équivalent à l'énoncé suivant : « un langage est solution minimale d'un système linéaire à droite si et seulement si il est obtenu à partir des langages finis par un nombre fini de réunions, de produits et de produits itérés ».

Cet énoncé sera une conséquence de notre théorème : il suffit d'exprimer le produit à partir de la substitution, d'exprimer le produit itéré à partir de la substitution itérée et réciproquement. La réunion est, on le sait, un cas particulier de la substitution.

6.1.1.1. *Expression de l'itération en terme de produit*

Si $L$ est un langage de $A^* V$ et si $a \in V$, associons à $L$ trois langages : ($V$ et $A$ sont disjoints);

$L_1 = L \cap A^*.(V - \{ a \})$ qui est l'ensemble des mots ne se terminant pas par $a$;

$L_2 = L - L_1$ qui est l'ensemble des mots de $L$ se terminant par $a$; et le langage $L_3$ de $A^*$ tel que

$L_2 = L_3.a$, $L_3 = L_2.a^{-1}$ (suivant la notation d'Eilenberg dans [7]).

On a alors

$$[a \leftarrow L'](L) = L_1 \cup L_3 . L'$$

et

$$L^{*a} = L_3^* \, L_1,$$

où $L_3^*$ est le produit itéré au sens habituel.

6.1.1.2. *Expression du produit en terme d'itération*

Il est immédiat que

$$L^* = (L.a \cup L)^{*a},$$

$$L.L' = [a \leftarrow L'](L.a).$$

6.1.2. *Cas où $A$ est infini*

Comme nous l'avons dit au paragraphe 3.4, les reconnaissables ne coïncident pas avec les algébriques, pourtant, les réguliers sont les algébriques et eux seuls.

### 6.2. Applications à la théorie des monoïdes

Ici, les langages algébriques sont les langages à contexte libre; la substitution est celle que l'on connaît sous ce nom dans le monoïde libre, comme on l'a vu dans les différents exemples. On retrouve le théorème de McWhirter [19] lui-même très proche du théorème de Gruska [11].

août 1976.

On trouvera dans [16] des applications de ce résultat à d'autres structures algébriques.

## 7. TRAVAUX RELIÉS AUX NÔTRES

### 7.1. Extensions possibles

Turner ([22]) a généralisé le théorème de Mezei-Wright aux théories algébriques hétérogènes, c'est-à-dire aux théories où les algèbres ont plusieurs types d'objets. En généralisant le concept de théorie conforme à ce cas, on doit pouvoir étendre notre théorème aux théories hétérogènes.

### 7.2. Travaux voisins

Parmi les travaux qui sont très proches, il faut citer Wand ([23]) qui, en terme de $\mu$-clan, énonce un théorème similaire, mais il n'est pas traductible directement car une telle théorie met côte à côte des aspects purement algébriques et des aspects qui relèvent spécifiquement des treillis, ce que nous avons voulu distinguer nettement en introduisant les théories conformes. On doit aussi rapprocher cela des travaux sur le « point fixe » en théorie de la programmation, en particulier de ce que Scott et De Bakker appellent itération ([20] et [6]) et Hitchcock et Park l' « élimination des points fixes multiples » ([12]).

## REMERCIEMENTS

Je remercie le Professeur Claude Pair qui m'a guidé dans cette recherche et Jean-Luc Remy et Alain Quere qui m'ont fait de nombreuses suggestions, ainsi que M$^{me}$ Chaunac qui s'est chargée de la frappe de mon texte.

## BIBLIOGRAPHIE

1. H. Bekic, *Definable Operations in General Algebras and the Theory of Automata and Flowcharts*, I.B.M., Vienna, 1969.
2. G. Birkhoff, *Lattice Theory*, American Math. Soc., Coll., vol. 25, 3$^e$ édition, 1967.
3. P. M. Cohn, *Universal Algebra*, Van Nostrand, Princeton, 1965.
4. N. Chomsky, *On Certain Formal Properties of Grammars*, Inf. and Control, 2, 1959, p. 137-167.
5. J. W. De bakker, *Fixed Points in Programming Theory* in Foundations of Computer Science (J. W. De bakker ed.), Mathematical Center Tracts, 63, Mathematisch Centrum Amsterdam, 1974, p. 1-49.

6. W. P. DE ROEVER, *Recursion and Parameters Mechanisms, Axiomatic Approach* in Automata, Languages and Programming (J. LOECKX ed.), Lectures Notes in Computer Sciences, vol. 14, Springer Verlag, Berlin 1974, p. 34-65.
7. S. EILENBERG, *Automata, Languages and Machines*, vol. A, Academic Press (1974).
8. S. EILENBERG et J. B. WRIGHT, *Automata in General Algebras*, Inf. and Control, 11, 1967, p. 452-470.
9. N. D. GAUTAM, *The Validity of Equations of Complex Algebras*, Arch. Math. Logik Grundlagenforsch, 3, 1957, p. 117-127.
10. G. GRATZER, *Universal Algebra*, Van Nostrand, 1968.
11. J. GRUSKA, *A Characterization of Context Free Languages*, J. Comput System Sc., 5, 1971, p. 353-364.
12. P. HITCHCOCK et D. PARK, *Induction Rules and Termination Proofs* in Automata, Languages and Programming (M. NIVAT ed.), North-Holland, 1972, p. 225-251.
13. J. E. HOPCROFT et J. D. ULLMANN, *Formal Languages and Their Relation to Automata*, Addison Wesley, 1969.
14. S. G. KLEENE, *Representations of Events in Nerves Nets and Finite Automata in Automata Studies* (C. E. SHANNON and J. MCCARTHY eds.), Princeton Univ. Press, Princeton, New Jersey, 1956, p. 3-42.
15. F. W. LAWVERE, *Functorial Semantics of Algebraic Theories*, Proc. Math. Acad. Sc. U.S.A., 50, 1963, p. 869-872.
16. P. LESCANNE, *Étude de quelques théories des langages et généralisation du théorème de Kleene*, Thèse de 3e Cycle, Université de Nancy, 1971.
17. I. P. MC WHIRTER, *Substitution Expressions*, J. Comput Systems Sc., 5, 1971, p. 629-637.
18. J. MEZEI et J. B. WRIGHT, *Algebraic Automata and Context-Free Sets*, Inf. and Control, 11, 1967, p. 3-29.
19. B. PAREIGIS, *Categories and Functors*, Academic Press, 1970.
20. D. SCOTT et J. W. DE BAKKER, *A Theory of Programs*, unpublished notes I.B.M. Seminar, Vienna, 1969.
21. J. W. THATCHER et J. B. WRIGHT, *Generalized Automata Theory with an Appli, cation to a Decision Problem of Second Order Logic*, Math. Systems Theory-2, 1968, p. 57-81.
22. R. TURNER, *An Infinite Hiérarchy of Terms Languages and Approach to Mathematical Complexity* in Automata, Languages and Programming (M. NIVAT ed.), North Holland, 1972, p. 593-608.
23. M. WAND, *A Concrete Approach to Abstract Recursive Definitions* in Automata, Languages and Programming (M. NIVAT ed.), North Holland, 1972, p. 331-341.
24. J. ENGELFRIET, *Simple Program Schemes and Formal Languages*, Lecture Notes in Computer Science, 20, Springer Verlag, 1974.

août 1976.