INFORMATIQUE THÉORIQUE ET APPLICATIONS

PIERRE PÉLADEAU

Sur le produit avec compteur modulo un nombre premier

Informatique théorique et applications, tome 26, n° 6 (1992), p. 553-564

<http://www.numdam.org/item?id=ITA_1992__26_6_553_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 26, n° 6, 1992, p. 553 à 564)

SUR LE PRODUIT AVEC COMPTEUR MODULO UN NOMBRE PREMIER (*)

par Pierre PÉLADEAU (1)

Communiqué par J. E. PIN

Résumé. – *Nous montrons que la hiérarchie obtenue à partir d'une variété de langages en itérant le produit avec compteur modulo un nombre premier s'effondre au premier niveau, et ceci quelle que soit la variété de départ. Nous montrons aussi l'équivalence entre le produit avec compteur modulo p et le produit avec compteur modulo p^r pour tout nombre premier p et tout entier $r \geqq 1$.*

Abstract. – *We show that the hierarchy obtained from a variety of languages by iterating the counting modulo a prime number product collapses at the first level, and this whatever the starting variety is. We also show the equivalence between the counting modulo p and counting modulo p^r products for all prime p and integer $r \geqq 1$.*

1. INTRODUCTION

Une part importante de la recherche sur les langages rationnels (et par la correspondance de Eilenberg [2], sur les monoïdes finis) concerne les opérations permettant de construire des langages (ou des monoïdes) complexes à partir d'éléments plus simples. On pense notamment au produit en couronne et à la célèbre théorie de composition et de décomposition des monoïdes de Krohn-Rhodes (*voir* [2]).

Le produit avec compteur est une opération relativement nouvelle [9, 13, 6, 14] qui s'inscrit dans cette lignée. Il tire son nom de sa correspondance avec l'opération sur les langages qui consiste à compter, dans un semi-anneau donné, l'apparition de sous-mots dans un certain contexte. Cette opération

(*) Reçu juin 1991, accepté octobre 1991.
Ce travail a reçu l'appui financier du Conseil de Recherche en Science Naturelle et en Génie (Canada) et du PRC Mathématique et Informatique (France).
(1) École d'Informatique, Université McGill, 3480, rue Université, Montréal, Québec, Canada H3A 2A7.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/92/06 553 12/$3.20/

est une généralisation du produit de Schützenberger [7] qui est le cas spécial lorsque le semi-anneau est celui de Boole.

La chaîne de variétés obtenue en itérant le produit de Schützenberger à partir de la variété triviale donne une hiérarchie infinie appelée la hiérarchie « dot-depth » [1].

Dans ce papier nous étendons un résultat de Eilenberg sur les p-groupes [2, chap. 8, § 10] en montrant que ce résultat sur la hiérarchie dot-depth ne tient plus si on remplace le semi-anneau de Boole par $\mathbb{Z}_{0,p}$, avec p premier, et quelque soit la variété de départ. Nous montrons plus précisément que la clôture de toute variété de monoïdes par le produit avec compteur $\mathbb{Z}_{0,p}$ est obtenue par une seule application de cette opération. Nous montrons aussi que la puissance du produit avec compteur $\mathbb{Z}_{0,p}$ est la même que celle du produit avec compteur $\mathbb{Z}_{0,p^r}$, pour tout $r \geqq 1$.

Les méthodes employées s'inspirent de l'idée de Smolensky [8] qui consiste à utiliser des polynômes pour reconnaître des langages.

2. PRÉLIMINAIRES

Soient K un semi-anneau unitaire et M un monoïde fini. Un *polynôme* est une application $f : M \to K$. Soit $m \in M$, l'élément $f(m) \in K$ est souvent appelé le *coefficient* de m dans f. On utilise alors la notation $f = \sum_{m \in M} f(m)\, m$. L'ensemble des polynômes de M dans K, noté $K\langle M \rangle$, est un monoïde avec la multiplication donnée par :

$$fg = \sum_{m \in M} \Big(\sum_{m = m_1 m_2} f(m_1)\, g(m_2) \Big) m.$$

Soient $M_1, \ldots, M_n$ des monoïdes finis et $M = M_1 \times \ldots \times M_n$. Le produit $K \Diamond_n (M_1, \ldots, M_n)$, introduit par Thérien [13] (sur les congruences), Pin [6] et Weil [14], est le sous-monoïde du monoïde des matrices $n \times n$ à coefficients dans $K\langle M \rangle$, constitué des matrices P vérifiant :

$P_{i,j} = 0$ si $i > j$;

$P_{i,i} = (1, \ldots, 1, m_i, 1, \ldots, 1)$, avec $m_i \in M_i$; et

$P_{i,j} \in K\langle (1 \times \ldots \times 1 \times M_i \times \ldots \times M_j \times 1 \times \ldots \times 1) \rangle$, si $i < j$.

Lorsque $K = \mathbb{Z}_{t,q}$, ce produit est appelé *produit avec compteur* (seuil t, modulo q). Ce produit est une généralisation du *produit de Schützenberger* (où $K = \mathbb{Z}_{1,1}$) introduit par Schützenberger [7] pour le cas $n = 2$, et Straubing [10] pour le cas général.

Rappelons qu'une *variété de monoïdes finis* est une classe fermée par produit direct et par division (image homomorphe d'un sous-monoïde). Cette opération sur les monoïdes s'étend alors à une opération sur les variétés en prenant pour toute variété $\mathbf{V}$, $K \Diamond \mathbf{V}$ la variété engendrée par les monoïdes de la forme $K \Diamond M$ avec $M \in \mathbf{V}$.

Soit A un alphabet fini, on notera A^* le monoïde libre engendré par A. Une partie L de A^* est appelée *langage*. Un langage $L \subseteq A^*$ est *reconnu* par un monoïde fini M si et seulement si il existe un morphisme $\varphi : A^* \to M$ tel que $L\varphi\varphi^{-1} = L$. Un tel langage est dit *reconnaissable*.

Le *quotient* (ou *résiduel*) *à gauche* (resp. *à droite*) d'un langage $L \subseteq A^*$ par un mot $u \in A^*$ est le langage $u^{-1}L = \{ v \mid uv \in L \}$ (resp. $Lu^{-1} = \{ v \mid vu \in L \}$).

Une *variété de langages* est une classe de langages reconnaissables (définie pour chaque alphabet fini) fermée par les opérations de Boole $\cup$ et $\setminus$, par morphismes inverses entre monoïdes libres et par les quotients à gauche et à droite par des mots. Il existe une bijection entre les variétés de monoïdes et les variétés de langages [2].

Soient $\mathscr{V}$ une variété de langages et A un alphabet fini, on notera $A^*\mathscr{V}$ l'ensemble des langages $L \subseteq A^*$ appartenant à $\mathscr{V}$. Si $\mathbf{V}$ est la variété de monoïdes correspondant (par le théorème de Eilenberg [2, chap. 7, § 3]) à la variété des langages $L \subseteq A^*$ reconnus par les monoïdes de $\mathbf{V}$.

Soient $L_0, \ldots, L_n \subseteq A^*$, et $a_1, \ldots, a_n \in A$, $t \geq 0$, $q \geq 1$ et $0 \leq c < t+q$. On note $(L_0 a_1 L_1 \ldots a_n L_n)_{c,t,q}$ le langage composé des mots $w \in A^*$ dont le nombre de factorisations $w = u_0 a_1 u_1 \ldots a_n u_n$, avec $u_i \in L_i$ pour $i = 1, \ldots, n$, est congru à c seuil t, modulo q. Cette opération sur les langages correspond à l'opération du produit avec compteur sur les monoïdes. C'est-à-dire : pour toute variété de monoïde $\mathbf{V}$ et pour tout $t \geq 0$ et $q \geq 1$, la variété de langages correspondant à $\mathbb{Z}_{t,q} \Diamond \mathbf{V}$ est l'algèbre de Boole engendrée par les langages de la forme $(L_0 a_1 L_1 \ldots a_n L_n)_{c,t,q}$, avec $n \geq 1$, $0 \leq c < t+q$ et L_i reconnu par un monoïde de $\mathbf{V}$ pour $i = 0, \ldots, n$ [9, 13, 6, 14]. Par extension de la notation sur les monoïdes, nous noterons cette variété de langages $\mathbb{Z}_{t,q} \Diamond \mathscr{V}$.

3. UNE ALGÈBRE

Soit A un alphabet fini et soit $\mathscr{F}$ l'ensemble des vecteurs de la forme $[L_0, a_1, L_1, \ldots, a_k, L_k]$, avec $k \geq 0$, chaque $a_i \in A$ et chaque L_i reconnaissable.

De façon canonique, un élément $f = [L_0, a_1, L_1, \ldots, a_k, L_k]$ de $\mathscr{F}$ définit une fonction $f : A^* \to \mathbb{N}$, où $f(w)$ est le nombre de factorisation $w = u_0 a_1 u_1 \ldots a_k u_k$, avec $u_i \in L_i$, pour $i = 1, \ldots, k$.

On appellera les éléments de $\mathscr{F}$ des *monômes*. Le *degré* d'un monôme $f \in \mathscr{F}$ (noté $\deg(f)$) est le nombre de lettres dans le vecteur représentant f. Par exemple, si $f=[L_0, a_1, L_1, \ldots, a_k, L_k]$, alors $\deg(f)=k$.

Soit $\mathscr{F}_\Sigma$ l'ensemble des sommes finies d'éléments de $\mathscr{F}$. Par extension de la notation employée pour $\mathscr{F}$, les éléments de $\mathscr{F}_\Sigma$ seront appelés des *polynômes* et $\deg\left(\sum_{i=1}^{m} f_i\right)=\max\{\deg(f_i) \mid i \in [m]\}$. Les éléments de $\mathscr{F}_\Sigma$ définissent aussi naturellement des fonctions de A^* dans $\mathbb{N}$

$$\left[i.e.\left(\sum_{i=1}^{m} f_i\right)(w)=\sum_{i=1}^{m} f_i(w)\right].$$

On définit, par récurrence sur le degré, un produit entre monômes :

$$[K].[L]=[K \cap L]; \tag{1}$$

$$[K_0, a, K_1].[L]=\sum[K_0 \cap L(av)^{-1}, a, K_1 \cap (ua)^{-1}L]; \tag{2}$$

$$\begin{aligned}[K_0, a, K_1].[L_0, b. L_1] &= \sum[K_0 \cap L_0(av)^{-1}, a, K_1(bw)^{-1} \cap (ua)^{-1}L_0, b, (vb)^{-1}K_1 \cap L_1] \\ &+ \sum[K_0(bv)^{-1} \cap L_0, b, (ub)^{-1}K_0 \cap L_1(aw)^{-1}, a, K_1 \cap (va)^{-1}L_1] \\ &+ \delta_{a=b}[K_0 \cap L_0, a, K_1 \cap L_1]. \end{aligned} \tag{3}$$

où

$$\delta_{a=b}=\begin{cases} 0 & \text{si } a \neq b, \\ 1 & \text{si } a=b. \end{cases}$$

En (3), la première (resp. seconde) sommation est prise sur les triplets $(u, v, w) \in (A^*)^3$ donnant des triplets $(K_0 \cap L_0(av)^{-1}, K_1(bw)^{-1} \cap (ua)^{-1}L_0, (vb)^{-1}K_1 \cap L_1)$ (resp. $(K_0(bv)^{-1} \cap L_0, (ub)^{-1}K_0 \cap L_1(aw)^{-1}, K_1 \cap (va)^{-1}L_1)$) distincts. Puisque les langages K_0, K_1, L_0 et L_1 sont reconnaissables, ils n'ont chacun qu'un nombre fini de quotients. Par conséquent, ces sommations ne sont prises que sur un nombre fini de triplets $(u, v, w) \in (A^*)^3$. De même pour (2).

L'ensemble $\mathscr{F}_\Sigma$ devient alors un anneau avec $0=[\varnothing]$, $1=[A^*]$ et le produit défini par

$$\left(\sum_{i=1}^{m} f_i\right).\left(\sum_{j=1}^{n} g_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n} f_i.g_j.$$

Soient $f, g \in \mathscr{F}_\Sigma$, on remarque que $\deg(f.g)=\deg(f)+\deg(g)$ et pour tout $w \in A^*$, $f(w).g(w)=(f.g)(w)$.

Soit K un corps fini, on note $K[\mathscr{F}_\Sigma]$ l'algèbre des polynômes avec variables dans $\mathscr{F}_\Sigma$ et coefficients dans K. L'algèbre quotient de $K[\mathscr{F}_\Sigma]$ obtenue en identifiant $1(f+g)$ à $1(f)+1(g)$, pour tout $f, g \in \mathscr{F}_\Sigma$, s'identifie aux polynômes de la forme $\sum_{i=1}^{m} c_i f_i$, avec $c_i \in K$ et $f_i \in \mathscr{F}$. On notera ce quotient $K[\mathscr{F}]$.

Un élément $f = \sum_{i=1}^{m} c_i f_i$ de $K[\mathscr{F}]$ définit une fonction $f: A^* \to K$, par $f(w) = \sum_{i=1}^{m} c_i f_i(w)$.

Soit L un langage de A^* et f un polynôme de $K[\mathscr{F}]$, on dira que *f reconnaît* L s'il existe $P \subseteqq K$ tel que $L = f^{-1}(P)$. On appellera *polynôme caractéristique* de L tout polynôme $f \in K[\mathscr{F}]$ tel que

$$f(w) = \begin{cases} 1 & \text{si } w \in L, \\ 0 & \text{si } w \notin L. \end{cases}$$

Un langage reconnaissable peut avoir et possède en général plusieurs polynômes caractéristiques.

Exemple 1 : Soit $L = (A^* a A^*)_{0,0,2}$ et $K = \mathbb{Z}_{0,2}$, alors $[L]$ et $1+[A^*, a, A^*]$ sont tous les deux des polynômes caractéristiques de L. □

On remarque dans cet exemple que le degré du second polynôme caractéristique est plus élevé que le premier, par contre les langages utilisés dans sa construction sont plus « simples ».

Soit $\mathscr{V}$ une variété de langages, on notera $\mathscr{F}(\mathscr{V})$ l'ensemble des vecteurs de la forme $[L_0, a_1, L_1, \ldots, a_k, L_k]$, avec $k \geqq 0$, chaque $a_i \in A$ et chaque $L_i \in A^* \mathscr{V}$. $K[\mathscr{F}(\mathscr{V})]$ notera la restriction évidente de $K[\mathscr{F}]$.

Nous terminons cette section avec quelques propriétés élémentaires.

LEMME 1 : *Soit K un corps fini, soit $\mathscr{V}$ une variété de langages, et soit un langage $L \in A^* \mathscr{V}$. Alors L possède un polynôme caractéristique dans $K[\mathscr{F}(\mathscr{V})]$.*

Preuve : $[L] \in K[\mathscr{F}(\mathscr{V})]$ est un polynôme caractéristique de L. ■

LEMME 2 : *Soit $\mathscr{V}$ une variété de langages et soient $L_0, L_1 \subseteqq A^*$ des langages ayant chacun des polynômes caractéristiques dans $K[\mathscr{F}(\mathscr{V})]$. Alors les langages $A^* \setminus L_0$, $L_0 \cap L_1$ et $L_0 \cup L_1$ ont aussi des polynômes caractéristiques dans $K[\mathscr{F}(\mathscr{V})]$.*

Preuve : Soient $\mathrm{car}(L_0), \mathrm{car}(L_1) \in K[\mathscr{F}(\mathscr{V})]$ des polynômes caractéristiques de L_0 et L_1. Alors

- $1 - \mathrm{car}(L_0)$ est un polynôme caractéristique de $A^* \setminus L_0$,

• car (L_0).car (L_1) est un polynôme caractéristique de $L_0 \cap L_1$, et

• car (L_0)+car (L_1)−car (L_0).car (L_1) est un polynôme caractéristique de $L_0 \cup L_1$. ■

4. APPLICATION AU PRODUIT AVEC COMPTEUR

Nous utilisons les polynômes de $\mathbb{Z}_{0,p}[\mathscr{F}]$ afin d'étudier les produits de langages avec compteurs mod p, pour p premier. Nous montrerons

THÉORÈME 3 : *Soient $\mathscr{V}$ une variété de langages et p un nombre premier. Alors $\mathbb{Z}_{0,p} \Diamond (\mathbb{Z}_{0,p} \Diamond \mathscr{V}) = \mathbb{Z}_{0,p} \Diamond \mathscr{V}$.*

La démonstration de ce théorème repose sur quelques propriétés de la reconnaissance de langages avec les polynômes de $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$.

LEMME 4 : *Soit A un alphabet fini et soit K un corps fini. Si un langage $L \subseteqq A^*$ est reconnu par un polynôme dans $K[\mathscr{F}(\mathscr{V})]$, alors L a un polynôme caractéristique dans $K[\mathscr{F}(\mathscr{V})]$.*

Preuve : Supposons K de caractéristique p. Soit $f \in K[\mathscr{F}(\mathscr{V})]$ et $c \in K$, alors un polynôme caractéristique du langage $f^{-1}(c)$ est $1-(f-c)^{p-1}$. La démonstration résulte alors du lemme 2. ■

La démonstration du théorème 3 découle des deux propositions suivantes.

PROPOSITION 5 : *Soient A un alphabet fini, $\mathscr{V}$ une variété de langages et p un nombre premier. Alors un langage appartient à $A^* \mathbb{Z}_{0,p} \Diamond \mathscr{V}$ si et seulement si il a un polynôme caractéristique dans $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$.*

PROPOSITION 6 : *Soient A un alphabet fini, $\mathscr{V}$ une variété de langages et p un nombre premier. Alors tout langage de $A^* \mathbb{Z}_{0,p} \Diamond (\mathbb{Z}_{0,p} \Diamond \mathscr{V})$ a un polynôme caractéristique dans $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$.*

Preuve de la proposition 5 : Tout langage de $A^* \mathbb{Z}_{0,p} \Diamond \mathscr{V}$ est combinaison booléenne finie de langages de la forme $(L_0 a_1 L_1 \ldots a_k L_k)_{c,0,p}$, avec $0 \leqq c < p$, chaque $a_i \in A$ et chaque $L_i \in A^* \mathscr{V}$. Le langage $(L_0 a_1 L_1 \ldots a_k L_k)_{c,0,p}$ est reconnu par le polynôme $[L_0, a_1, L_1, \ldots, a_k, L_k] \in \mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$, en choisissant $\{c\}$ comme ensemble reconnaissant. La démonstration de la première implication découle alors des lemmes 2 et 4.

Réciproquement, soit $L \subseteqq A^*$ avec comme polynôme caractéristique

$$\operatorname{car}(L) = \sum_{i=1}^{m} c_i [L_{i,0}, a_{i,1}, L_{i,1}, \ldots, a_{i,k_i}, L_{i,k_i}] \in \mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})].$$

Alors

$$L = \bigcup \bigcap_{i=1}^{m} (L_{i,0}\, a_{i,1}\, L_{i,1} \ldots a_{i,k_i} L_{i,k_i})_{d_i,0,p},$$

où l'union est prise sur tous les m-uplets $(d_1, \ldots, d_m) \in \{0, \ldots, p-1\}^m$ tels que $\sum_{i=1}^{m} c_i d_i = 1$. ■

Preuve de la proposition 6. Soient $K, L \in A^* \mathbb{Z}_{0,p} \Diamond \mathscr{V}$, $a \in A$ et $0 \leqq c < p$. On démontre comment obtenir un polynôme caractéristique dans $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$ pour le langage $(K a L)_{c,0,p}$. La construction donnée se généralise facilement pour un produit plus long et la démonstration de la proposition résulte alors du lemme 2.

Par la proposition 5, K et L ont tous les deux des polynômes caractéristiques dans $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$. Soient

$$\operatorname{car}(K) = \sum_{i=1}^{m} c_i [K_{i,0}, a_{i,1}, K_{i,1}, \ldots, a_{i,k_i}, K_{i,k_i}]$$

et

$$\operatorname{car}(L) = \sum_{j=1}^{n} d_i [L_{j,0}, b_{j,1}, L_{j,1}, \ldots, b_{j,l_j}, L_{j,l_j}].$$

deux de ces polynômes caractéristiques pour K et L respectivement.

Soit $w \in A^*$. Le nombre de factorisations $w = uav$, avec $u \in K$ et $v \in L$ est donné par

$$\sum_{w=uav} \operatorname{car}(K)(u) . \operatorname{car}(L)(v).$$

Il s'ensuit que $(K a L)_{c,0,p}$ est reconnu par le polynôme

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_i d_j [K_{i,0}, a_{i,1}, K_{i,1}, \ldots, a_{i,k_i}, K_{i,k_i}, a, L_{j,0}, b_{j,1}, L_{j,1}, \ldots, b_{j,l_j}, L_{j,l_j}]$$

appartenant à $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$, en choisissant $\{c\}$ comme ensemble reconnaissant. La démonstration découle alors du lemme 4. ■

THÉORÈME 7 : *Soit $\mathscr{V}$ une variété de langages et soient p un nombre premier et $r \geqq 1$. Alors $\mathbb{Z}_{0,p^r} \Diamond \mathscr{V} = \mathbb{Z}_{0,p} \Diamond \mathscr{V}$.*

Les deux lemmes suivants seront utiles dans la démonstration du théorème 7. Ces lemmes peuvent être déduits d'un résultat ancien en théorie

des nombres (*voir* [3, p. 417]). Nous en donnons la démonstration ici pour rendre ce travail complet.

LEMME 8 : *Soient p un nombre premier et $m \geqq 1$ un entier multiple de p. Alors pour tout $k \geqq 1$: p divise $\binom{m/p}{k}$ si et seulement si p divise $\binom{m}{pk}$.*

Preuve : Supposons p divise

$$\binom{m/p}{k} = \frac{(m/p)(m/p-1)\ldots(m/p-(k-1))}{k(k-1)\ldots 1}$$

Alors p divise

$$\frac{m(m-p)\ldots(m-(k-1)p)}{pkp(k-1)\ldots p}.$$

Puisque p ne divise pas $pa-b$ pour tout $a \geqq 1$ et $1 \leqq b < p$, on déduit que p divise

$$\frac{m(m-1)\ldots(m-(pk-1))}{pk(pk-1)\ldots 1} = \binom{m}{pk}.$$

Supposons maintenant p divise

$$\binom{m}{pk} = \frac{m(m-1)\ldots(m-(pk-1))}{pk(pk-1)\ldots 1} = \frac{m(m-p)\ldots(m-(k-1)p)}{pkp(k-1)\ldots p} \cdot a$$

pour

$$a = \frac{(m-1)\ldots(m-(p-1))\ldots(m-(pk-(p-1)))\ldots(m-(pk-1))}{(pk-1)\ldots(pk-(p-1))\ldots(p-1)\ldots 1}$$

Alors p divise

$$\frac{m/p(m/p-1)\ldots(m/p-(k-1))}{k(k-1)\ldots 1} \cdot a = \binom{m/p}{k} \cdot a.$$

Puisque p divise m, on déduit que p ne divise pas a et donc p divise $\binom{m/p}{k}$. ■

LEMME 9 : *Soient p un nombre premier et $m, r \geqq 1$ des entiers avec m un multiple de p. Alors p^r divise m si et seulement si p divise $\binom{m}{p^i}$ pour* $i=0, \ldots, r-1$.

Preuve : Par récurrence sur r. Si $r=1$, il n'y a rien à démontrer.

Supposons p^r divise m. Alors p^{r-1} divise m/p et par récurrence p divise $\binom{m/p}{p^i}$ pour $i=0, \ldots, r-2$. Puisque p divise m, par le lemme 8, nous avons p divise $\binom{m}{p^i}$ pour $i=0, \ldots, r-1$.

Supposons maintenant p divise $\binom{m}{p^i}$ pour $i=0, \ldots, r-1$. Alors par le lemme 8, nous avons p divise $\binom{m/p}{p^i}$ pour $i=0, \ldots, r-2$ et par récurrence p^{r-1} divise m/p, ce qui implique p^r divise m. ■

Preuve du théorème 7 : L'inclusion dans un sens est triviale. Par la proposition 5, il suffit de montrer que tout langage $L \in A^* \mathbb{Z}_{0,p^r} \Diamond \mathscr{V}$ a un polynôme caractéristique dans $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$.

On peut supposer par exemple $L=(L_0 a L_1 b L_2)_{c,0,p^r}$ avec $a, b \in A$, L_0, L_1, $L_2 \in A^* \mathscr{V}$ et $0 \leqq c < p^r$. Soit $w \in A^*$ et supposons $[L_0, a, L_1, b, L_2](w)=m$. On remarque que $m \equiv c \pmod{p^r}$ si et seulement si p^r divise $m+(p^r-c)$. Par le lemme 9, p^r divise $m+(p^r-c)$ si et seulement si p divise $\binom{m+(p^r-c)}{p^i}$ pour $i=0, \ldots, r-1$. De l'identité

$$\binom{m+(p^r-c)}{p^i}=\binom{m}{p^i}\binom{p^r-c}{0}+\binom{m}{p^i-1}\binom{p^r-c}{1}+\ldots+\binom{m}{0}\binom{p^r-c}{p^i}$$

$\left[\text{notez que } \binom{x}{y}=0 \text{ lorsque } x<y\right]$, on déduit que pour vérifier $m \equiv c \pmod{p^r}$, il suffit de calculer mod p les nombres $\binom{m}{k}$ pour $k=0, \ldots, p^{r-1}$. Supposons par exemple $k=2$. Puisque m est le nombre de factorisations $w=u_0 a u_1 b u_2$ avec $u_i \in L_i$, $i=1, 2, 3$, on déduit que $\binom{m}{2}$ est donné par le nombre de factorisations

(1) $w = u_0 a u_1 b u_2 b u_3$ avec $u_0 \in L_0$, $u_1 \in L_1$, $u_2 b u_3 \in L_2$, $u_1 b u_2 \in L_1$, et $u_3 \in L_2$, ou

(2) $w = u_0 a u_1 a u_2 b u_3$ avec $u_0 \in L_0$, $u_1 a u_2 \in L_1$, $u_3 \in L_2$, $u_0 a u_1 \in L_0$, et $u_2 \in L_1$ ou

(3) $w = u_0 a u_1 b u_2 a u_3 b u_4$ avec $u_0 \in L_0$, $u_1 \in L_1$, $u_2 a u_3 b u_4 \in L_2$, $u_0 a u_1 b u_2 \in L_0$, $u_3 \in L_1$ et $u_4 \in L_2$, ou

(4) $w = u_0 a u_1 a u_2 b u_3 b u_4$ avec $u_0 \in L_0$, $u_1 a u_2 \in L_1$, $u_3 b u_4 \in L_2$, $u_0 a u_1 \in L_0$, $u_2 a u_3 \in L_1$ et $u_4 \in L_2$, ou

(5) $w = u_0 a u_1 a u_2 b u_3 b u_4$ avec $u_0 \in L_0$, $u_1 a u_2 b u_3 \in L_1$, $u_4 \in L_2$, $u_0 a u_1 \in L_0$, $u_2 \in L_1$ et $u_3 b u_4 \in L_2$.

Il s'ensuit que

$$\binom{m}{2} = \sum [L_0, a, L_1 \cap L_1 (bu_2)^{-1}, b, (u_1 b)^{-1} L_1 \cap L_2 (bu_3)^{-1}, b, (u_2 b)^{-1} L_2 \cap L_2](w)$$
$$+ \sum [L_0 \cap L_0 (au_1)^{-1}, a, L_1 (au_2)^{-1} \cap (u_0 a)^{-1} L_0, a, (u_1 a)^{-1} L_1 \cap L_1, b, L_2](w)$$
$$\text{cas (3)} + \text{cas (4)} + \text{cas (5)}$$

où ces sommations sont prises sur les quadruplets $(u_0, u_1, u_2, u_3) \in (A^*)^4$ donnant des résiduels distincts. Il n'y a qu'un nombre fini de tels quadruplets et chacun des résiduels appartient à $A^* \mathscr{V}$. On en déduit que L est reconnu par un polynôme de $\mathbb{Z}_{0,p}[\mathscr{F}(\mathscr{V})]$ et l'on conclut grâce au lemme 4.

Les autres cas sont traités de la même façon. ■

COROLLAIRE 10 : *Soient $\mathscr{V}$ une variété de langages, p un nombre premier, $r \geqq 1$ et $s \geqq 1$. Alors $\mathbb{Z}_{0,p^r} \Diamond (\mathbb{Z}_{0,p^s} \Diamond \mathscr{V}) = \mathbb{Z}_{0,p} \Diamond \mathscr{V}$.*

5. QUELQUES CONSÉQUENCES

La clôture de variété par le produit avec compteur a été étudié d'un point de vue algébrique et dans toute sa généralité par Weil [5]. Dans cette section nous examinons les conséquences de notre résultat d'effondrement sur les caractérisations des clôtures de variétés par le produit avec compteur données par Weil. Pour ce faire il nous faut d'abord introduire un peu de notation.

Soient M et N deux monoïdes finis, une relation $\tau : M \to N$ est un *morphisme relationnel* si $m\tau \neq \varnothing$ et $(m\tau)(n\tau) \subseteqq (mn)\tau$ pour tout $m, n \in M$. Soit **V** une variété de monoïdes finis, un morphisme relationnel $\tau : M \to N$ est un

V-*morphisme relationnel* si $N'\tau^{-1} \in \mathbf{V}$ pour chaque sous-monoïde N' de N appartenant à **V**. Soit **W** une variété de monoïdes finis, la classe de tous les monoïdes M tels qu'il existe un **V**-morphisme relationnel de M dans un élément N de **W** est une variété que l'on note $\mathbf{V}^{-1}\mathbf{W}$ [2, 5].

Weil démontre que la clôture d'une variété **V** par le produit avec compteur modulo un nombre premier p nous est donnée par la variété $\mathbf{LG}_p^{-1}\mathbf{V}$. Le théorème 3 nous permet alors de conclure

COROLLAIRE 11 : $\mathbf{LG}_p^{-1}\mathbf{V} = \mathbb{Z}_{0,p} \Diamond \mathbf{V}$ *pour toute variété de monoïdes* **V** *et tout nombre premier* p.

Weil étudie aussi quelques cas particuliers et montre notamment que $\mathbf{DS}_p = \mathbf{LG}_p^{-1}\mathbf{J}_1$. $\mathbf{DS}_p$ est la variété des semigroupes dont chaque D-classe régulière forme un semigroupe et dont tous les sous-groupes sont des p-groupes.

On déduit alors du théorème 3.

COROLLAIRE 12 : *Soit* $\mathscr{V}$ *la variété de langages associée à la variété de semigroupes* $\mathbf{DS}_p$. *Alors pour tout alphabet fini* A, $A^*\mathscr{V}$ *est l'algèbre de Boole des langages de la forme* $(L_0 a_1 L_1 \ldots a_k L_k)_{c,0,p}$ avec $a_i \in A$, $0 \leqq c < p$ *et chaque* $L_i \subseteqq A^*$ *dans la clôture booléenne des langages de la forme* $A^* a A^*$ *avec* $a \in A$.

6. CONCLUSION

Nous avons montré que pour obtenir la clôture d'une variété par le produit avec compteur modulo un nombre premier p, il suffit d'une seule application de cette opération. Nous avons aussi montré l'équivalence entre la puissance du produit avec compteur mod p^r et du produit avec compteur mod p^s pour tout $r, s \geqq 1$.

Ces résultats nous permettent de donner une image complète de l'arbre infini (décrivant les variétés de monoïdes résolubles) obtenu à partir de la variété triviale par des applications des produits avec compteurs de la forme $\mathbb{Z}_{t,q}$ avec $t \geqq 0$ et $q \geqq 1$. En effet le nombre de fois que le produit avec compteur modulo un nombre composé, ou une alternance de nombres premiers, est utilisé dans la construction d'un groupe correspond à la longueur de Fitting (ou longueur de nilpotence) du groupe, et donne une hiérachie stricte (*voir* [12, p. 89-93]). Ceci avec l'infinitude de la hiérarchie « dot-depth » implique que pour toute variété $\mathscr{V}$ obtenue à partir de la variété triviale par l'application d'une suite de produits avec compteurs de la forme $\mathbb{Z}_{t,q}$ avec $t \geqq 0$ et

$q \geqq 1$: $\mathbb{Z}_{r,m} \diamond \mathbb{Z}_{s,n} \diamond \mathscr{V} = \mathbb{Z}_{s,n} \diamond \mathscr{V}$ si et seulement si $r = s = 0$, $m = p^i$ et $n = p^j$ pour un nombre premier p et $i, j \geqq 1$.

REMERCIEMENTS

J'aimerais remercier Pascal Weil et le rapporteur anonyme pour plusieurs commentaires utiles, en particulier en ce qui a trait à la Section 5. J'aimerais aussi remercier Jacques Desarménien pour m'avoir indiqué la référence [3].

BIBLIOGRAPHIE

1. J. A. Brzozowski et R. Knast, The Dot-Depth Hierarchy of Star-Free Languages is Infinite, *J. Computer and System Sci.*, 1978, *16*, p. 35-55.
2. S. Eilenberg, Automata, Languages and Machines, *Academic Press*, 1976, *B*.
3. E. Luca, La Théorie des nombres, tome 1, 1961.
4. P. Péladeau, Classes de circuits booléens et variétés de langages, *Thèse de Doctorat*, Université Paris-VI, 1990.
5. J. E. Pin, Variétés de langage formels, *Masson*, Paris, 1984.
6. J.-E. Pin, Topologies for the Free Monoid, Rapport LITP 88.17, *J. of Algebra* (à paraître).
7. M. P. Schützenberger, On Finite Monoids Having Only Trivial Subgroups, *Inform. and Control*, 1965, *8*, p. 190-194.
8. R. Smolensky, Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity, *Proc. 19th ACM STOC*, 1987, p. 77-82.
9. H. Straubing, Families of Recognizable Sets Corresponding to Certain Varieties of Finite Monoids, *J. Pure Appl. Algebra*, 1979, *15*, p. 319-327.
10. H. Straubing, A Generalization of the Schützenberger Product of Finite Monoids, *Theoret. Comput. Sci.*, 1981, *13*, p. 137-150.
11. H. Straubing, D. Thérien and W. Thomas, Regular Languages Defined with Generalized Quantifiers, *Automata, Languages and Programming; Proc. 15th ICALP*, Springer, Lectures Notes in Comput. Sci., 1988.
12. D. Thérien, Classification of Regular Languages by Congruences, *Ph. D. Thesis*, Univ. of Waterloo, 1980.
13. D. Thérien, Classification of Finite Monoids: the Language Approach, *Theoret. Comput. Sci.*, 1981, *14*, p. 195-208.
14. P. Weil, Products of Languages with Counter, *Theoret. Comput. Sci.*, 1990, *76*, p. 251-260.
15. P. Weil, Closure of Varieties of Languages Under Products with Counter, *Rapport LITP*, p. 89-129.