

M. BOFFA

## **Une condition impliquant toutes les identités rationnelles**

*Informatique théorique et applications*, tome 29, n° 6 (1995), p. 515-518.

[http://www.numdam.org/item?id=ITA\\_1995\\_\\_29\\_6\\_515\\_0](http://www.numdam.org/item?id=ITA_1995__29_6_515_0)

© AFCET, 1995, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## UNE CONDITION IMPLIQUANT TOUTES LES IDENTITÉS RATIONNELLES (\*)

par M. BOFFA <sup>(1)</sup>

Communiqué par Christian CHOFRUT

---

Résumé. – Nous montrons que la condition affirmant que  $a^*$  est le plus petit idempotent  $\geq 1 + a$  implique toutes les identités rationnelles.

Abstract. – We show that the condition saying that  $a^*$  is the smallest idempotent  $\geq 1 + a$  implies all rational identities.

Dans un article précédent [1] (auquel nous renvoyons le lecteur pour la terminologie et les notations) nous avons établi (modulo une conjecture de Conway [2], p. 116, aujourd'hui démontrée par Krob [5]) la complétude du système d'identités rationnelles C1-C14 auquel on a ajouté la règle déductive suivante :

$$(R) \frac{E^2 = E}{E^* = 1 + E}.$$

Les identités C1-C10 caractérisent les opérations et constantes  $+$ ,  $\cdot$ ,  $0$ ,  $1$  de semi-anneau, et les suivantes sont :

$$(a + b)^* = (a^* b)^* a^* \quad C11$$

$$(ab)^* = 1 + a (ba)^* b \quad C12$$

$$a^{**} = a^* \quad C13$$

$$a^* = (a^n)^* (1 + a + \dots + a^{n-1}) \quad (n > 0). \quad C14$$

---

(\*) Reçu en mars 1995; accepté en octobre 1995.

(<sup>1</sup>) Université de Mons-Hainaut, Institut de Mathématique et Informatique, Avenue Maistriau, 15, B-7000 Mons, Belgique.

Si on ajoute l'idempotence de l'addition

$$a + a = a, \quad \text{C0}$$

alors en appliquant (R) pour  $E = 1$ , on voit qu'on peut éliminer C13, qui est déductible de C1-C12 et  $1^* = 1$  (voir [2], p. 35), donc de C0-C12 et  $1^* = 1 + 1$ . En l'appliquant pour  $E$  égal au second membre de C14, on parvient aussi à éliminer C14. Le système C0-C12 avec (R) est donc complet, ce qui implique que si un semi-anneau additivement idempotent  $(S, +, \cdot, 0, 1)$  est muni d'une opération  $*$  telle que (pour tout  $a, b, e \in S$ )  $(a + b)^* = (a^* b)^* a^*$ ,  $(ab)^* = 1 + a(ba)^* b$  et  $e^2 = e \rightarrow e^* = 1 + e$ , alors  $(S, +, \cdot, *, 0, 1)$  vérifie toutes les identités rationnelles.

Dans ce résultat, on peut évidemment remplacer la condition  $e^2 = e \rightarrow e^* = 1 + e$  par une condition qui l'implique, par exemple  $ab = b \rightarrow a^* b = b$ , qui redonne un théorème de Conway énoncé sans démonstration dans [2], p. 108.

Mais ici, il va nous servir à établir le

**THÉORÈME:** Si pour chaque élément  $a$  d'un semi-anneau additivement idempotent  $(S, +, \cdot, 0, 1)$  il existe un plus petit idempotent (multiplicatif)  $\geq 1 + a$  que l'on note  $a^*$ , alors  $(S, +, \cdot, *, 0, 1)$  vérifie toutes les identités rationnelles.

*Démonstration:* Dans  $(S, +, \cdot, *, 0, 1)$  on a par hypothèse :

$$1 + a \leq a^*, \quad a^* a^* = a^* \quad \text{et} \quad 1 + a \leq e = e^2 \rightarrow a^* \leq e.$$

On en déduit facilement que  $e^2 = e \rightarrow (1 + e)^2 = 1 + e \rightarrow e^* = 1 + e$ , donc il nous suffit de montrer que  $(a + b)^* = (a^* b)^* a^*$  et  $(ab)^* = 1 + a(ba)^* b$ .

Nous le ferons en plusieurs étapes, en utilisant certaines conséquences immédiates de nos hypothèses :  $a \leq b \rightarrow a^* \leq b^*$ ,  $a^{**} = a^*$ .

$$1) (ab)^* \leq 1 + a(ba)^* b.$$

En effet, posons  $e = 1 + a(ba)^* b$ .

$$\text{On a } e^2 = 1 + a(ba)^* b + a(ba)^* ba(ba)^* b.$$

Mais le dernier terme disparaît, car il est  $\leq a(ba)^* (ba)^* (ba)^* b = a(ba)^* b$ .

Donc  $e^2 = e$ , donc  $e^* = 1 + e = e$ .

Mais  $ab \leq e$ , donc  $(ab)^* \leq e^* = e$ .

$$2) 1 + a(ba)^* b \leq (ab)^*.$$

En effet, en échangeant  $a$  et  $b$  dans le résultat précédent, il vient  $(ba)^* \leq 1 + b(ab)^* a$ , d'où  $1 + a(ba)^* b \leq 1 + ab + ab(ab)^* ab \leq (ab)^*$ .

$$3) (ab)^* a = a(ba)^*.$$

En effet, nous savons maintenant que  $(ab)^* = 1 + a(ba)^* b$  (et en particulier que  $a^* = 1 + aa^*$ ,  $b^* = 1 + b^* b$ ), d'où

$$(ab)^* a = a + a(ba)^* ba = a(1 + (ba)^* ba) = a(ba)^*.$$

$$4) (a + b)^* \leq (a^* b)^* a^*.$$

En effet, posons  $e = (a^* b)^* a^*$ .

On a

$$\begin{aligned} e^2 &= (a^* b)^* a^* (a^* b)^* a^* \\ &= (a^* b)^* a^* a^* (ba^*)^* \\ &= (a^* b)^* a^* (ba^*)^* \\ &= (a^* b)^* (a^* b)^* a^* \\ &= (a^* b)^* a^* \\ &= e. \end{aligned}$$

Donc  $e^* = 1 + e = e$ .

Mais  $a \leq a^* \leq e$  et  $b \leq (a^* b)^* \leq e$ , donc  $a + b \leq e$ , donc  $(a + b)^* \leq e^* = e$ .

$$5) (a^* b)^* a^* \leq (a + b)^*.$$

En effet,

$$\begin{aligned} (a^* b)^* a^* &\leq ((a + b)^* (a + b)^*)^* (a + b)^* = (a + b)^{**} (a + b)^* \\ &= (a + b)^* (a + b)^* = (a + b)^*. \end{aligned}$$

#### APPLICATION

Kozen [3] appelle algèbre de Kleene tout semi-anneau additivement idempotent muni d'une opération  $*$  telle que

$$1 + aa^* \leq a^* \tag{1}$$

$$1 + a^* a \leq a^* \tag{2}$$

$$ab \leq b \rightarrow a^* b \leq b \tag{3}$$

$$ba \leq b \rightarrow ba^* \leq b. \tag{4}$$

Il montre dans [4] qu'une algèbre de Kleene doit vérifier toutes les identités rationnelles. Nous allons voir que cela peut se déduire du théorème précédent.

Kozen parle aussi d'algèbre de Kleene à droite ou à gauche, lorsqu'on ne retient que les conditions (1), (2), (3) ou (1), (2), (4), et il montre que ces notions ne sont pas équivalentes. On voit facilement que les conditions (1), (3) [resp. (2), (4)] impliquent déjà la condition (2) [resp. (1)]. Plus généralement, montrons que les conditions (1), (3) [resp. (2), (4)] impliquent que  $a^*$  est le plus petit idempotent (multiplicatif)  $\geq 1 + a$ , et impliquent donc (par le théorème précédent) toutes les identités rationnelles.

En effet, en supposant (1), (3), il vient :

- i)  $1 \leq a^*$ , d'où  $a^* \leq a^* a^*$ .
- ii)  $aa^* \leq a^*$ , d'où  $a^* a^* \leq a^*$ .
- iii)  $1 + a \leq 1 + aa^* \leq a^*$ .
- iv) si  $1 + a \leq e = e^2$ , alors  $a \leq e$ , d'où  $ae \leq e$ , d'où  $a^* e \leq e$ , d'où  $a^* \leq a^* e \leq e$ .

On a une preuve similaire pour (2), (4).

En conclusion : dans une algèbre de Kleene à droite (ou à gauche)  $a^*$  est le plus petit idempotent (multiplicatif)  $\geq 1 + a$ , et c'est la raison pour laquelle une telle algèbre doit vérifier toutes les identités rationnelles.

#### RÉFÉRENCES

1. M. BOFFA, Une remarque sur les systèmes complets d'identités rationnelles, *Informatique théorique et Applications/Theoretical Informatics and Applications*, 1990, 24, p. 419-423.
2. J. H. CONWAY, *Regular Algebra and Finite Machines*, Chapman & Hall, 1971.
3. D. C. KOZEN, On Kleene Algebras and Closed Semirings, *Springer Lecture Notes in Computer Science*, 1990, 452, p. 26-47.
4. D. C. KOZEN, A completeness theorem for Kleene algebras and the algebra of regular events, *Proc. 6th Symp. Logic in Computer Science (IEEE)*, 1991, p. 214-225.
5. D. KROB, Complete systems of  $\mathcal{B}$ -rational identities, *Theoretical Computer Science*, 1991, 89, p. 207-343.