

MAURICE BOFFA

Une remarque sur les systèmes complets d'identités rationnelles

Informatique théorique et applications, tome 24, n° 4 (1990), p. 419-423.

http://www.numdam.org/item?id=ITA_1990__24_4_419_0

© AFCET, 1990, 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 REMARQUE SUR LES SYSTÈMES COMPLETS D'IDENTITÉS RATIONNELLES (*)

par Maurice BOFFA (1)

Communiqué par J.-E. PIN

Résumé. – Une règle déductive très simple permet de relier des problèmes de complétude soulevés par Conway et Salomaa.

Abstract. – Completeness questions of Conway and Salomaa are linked by means of a very simple deductive rule.

1. NOTATIONS

Nous utiliserons les lettres minuscules a, b, c, \dots comme variables (parcourant les langages) et les lettres majuscules A, B, C, \dots comme termes que l'on peut construire à partir des variables, des constantes 0, 1 et des opérations rationnelles $+, \cdot, *$. Une *identité rationnelle* est une égalité $A = B$ qui est vraie quelles que soient les valeurs prises par les variables figurant dans les termes A et B . Chaque terme A représente un langage canonique $L(A)$ obtenu en donnant aux variables a, b, c, \dots les valeurs $\{a\}, \{b\}, \{c\}, \dots$. On peut montrer que $A = B$ est une identité rationnelle si et seulement si $L(A) = L(B)$. La partie constante d'un terme A , c'est-à-dire sa valeur pour $a, b, c, \dots = 0$, sera notée $c(A)$. On a $c(A) = 1$ ou 0 suivant que le mot vide appartient ou n'appartient pas à $L(A)$.

(*) Reçu octobre 1988, révisé en mai 1989.

(1) Faculté des Sciences, 15, avenue Maistriau, B-7000 Mons, Belgique.

2. LE SYSTÈME DE SALOMAA [4]

Appelons S l'ensemble des identités rationnelles S1-S12 suivantes (axiomes de Salomaa) :

$$\begin{array}{ll}
 \text{S1 } a+0=a, & \text{S7 } 1 \cdot a=a \\
 \text{S2 } a+b=b+a, & \text{S8 } a(b+c)=ab+ac \\
 \text{S3 } (a+b)+c=a+(b+c), & \text{S9 } (b+c)a=ba+ca \\
 \text{S4 } a \cdot 0=0, & \text{S10 } (ab)c=a(bc) \\
 \text{S5 } 0 \cdot a=0, & \text{S11 } (1+a)^*=a^* \\
 \text{S6 } a \cdot 1=a, & \text{S12 } a^*=1+a^*a.
 \end{array}$$

De ces axiomes, on déduit facilement les identités $0^*=1^*=1$, $1=1+1$, $a=a+a$. Notons S^+ le système de Salomaa obtenu en adjoignant à S la règle déductive suivante :

$$\frac{E=EF+G}{E=GF^*} \quad [\text{si } c(F)=0].$$

Dans [4], Salomaa prouve que S^+ est complet (c'est-à-dire que toutes les identités rationnelles y sont déductibles à l'aide de la logique équationnelle) et pose le problème suivant : le système $S^+((E=EF+1)/(E=F^*))(c(F)=0)$ est-il complet?

3. LE SYSTÈME DE CONWAY [2]

Appelons C l'ensemble des identités rationnelles C1-C14 suivantes (axiomes classiques de Conway) :

$$\begin{array}{l}
 \text{C1-C10 qui coïncident avec S1-S10} \\
 \text{C11 } (a+b)^*=(a^*b)^*a^* \\
 \text{C12 } (ab)^*=1+a(ba)^*b \\
 \text{C13 } a^{**}=a^* \\
 \text{C14 } a^*=(a^n)^*(1+a+\dots+a^{n-1}) \quad (n > 0).
 \end{array}$$

Notons C^+ le système de Conway obtenu en adjoignant à C la règle déductive suivante :

$$\frac{E_g E_h \leq E_{gh} \text{ et } (E_{g,g})^*=E_{g,g} \text{ (pour tout } g, h \in M)}{(\sum E_g)^*=(\sum E_g)}$$

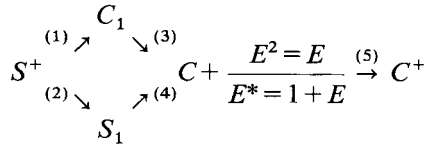
où M est un monoïde fini quelconque, \sum désigne la sommation sur M , $E_{g,h} = \sum_{gk=h} E_k$ et $A \leq B$ signifie $A + B = B$.

Dans [2], Conway conjecture que C^+ est complet (p. 116) et affirme (sans donner de preuve) que $C + ((E = EF)/(E = EF^*))$ l'est également (p. 108).

4. LA RÈGLE $(E^2 = E)/(E^* = 1 + E)$

Cette règle semble intéressante pour l'étude des systèmes complets, car on a le résultat suivant :

THÉORÈME : *On a*



où

$$C_1 = C + \frac{E = EF}{E = EF^*}, \quad S_1 = S + \frac{E = EF + 1}{E = F^*} (c(F) = 0)$$

et chaque \rightarrow désigne une inclusion (\supset). La conjecture de Conway implique donc que tous les systèmes figurant dans le diagramme précédent sont complets.

Démonstration :

(1) résulte de la complétude de S^+ , mais peut être établi directement : on prouve d'abord C11-C14 dans S^+ [voir (4) plus bas] puis on y établit $(E = EF)/(E = EF^*)$ comme suit :

si $c(F) = 0$, on a successivement $E = EF$, $E = EF + E$, $E = EF^*$;

si $c(F) = 1$, alors (par induction sur F), il existe un terme F' tel que $c(F') = 0$ et $F = 1 + F'$ dans S , ce qui permet de faire la déduction suivante dans S^+ :

$$E = EF, \quad E = EF' + E, \quad E = E(F')^*, \quad E = EF^*.$$

(2) est trivial.

(3) s'obtient par la déduction suivante :

$$E^2 = E, \quad E = EE^*, \quad E^* = 1 + EE^* = 1 + E \quad (\text{par C12 avec } a = E \text{ et } b = 1).$$

(4) s'obtient en prouvant d'abord C11-C14 dans S_1 :

C11 : il suffit d'établir $E = EF + 1$ pour $E = (a^* b)^* a^*$ et $F = a + b$:

$$\begin{aligned}
 EF + 1 &= (a^* b)^* a^* (a + b) + 1 \\
 &= (a^* b)^* a^* a + (a^* b)^* a^* b + 1 \\
 &= (a^* b)^* a^* a + (a^* b)^* \\
 &= (a^* b)^* (a^* a + 1) \\
 &= (a^* b)^* a^* = E.
 \end{aligned}$$

C12 : idem pour $E = 1 + a(ba)^* b$ et $F = ab$:

$$\begin{aligned}
 EF + 1 &= (1 + a(ba)^* b) ab + 1 \\
 &= ab + a(ba)^* bab + 1 \\
 &= a(1 + (ba)^* ba) b + 1 \\
 &= a(ba)^* b + 1 = E.
 \end{aligned}$$

C13 :

$$\begin{aligned}
 a^* &= 1 + a^* a \\
 &= 1 + 1 + a^* a \\
 &= 1 \dagger a^* \\
 &= 1 + (a + 1)^* \\
 &= 1 + a^{**} a^* \text{ (par C11 avec } b = 1) \\
 &= a^{**}
 \end{aligned}$$

C14 : si $E = (a^n)^* (1 + a + \dots + a^{n-1})$ et $F = a$, alors :

$$\begin{aligned}
 EF + 1 &= (a^n)^* (a + \dots + a^n) + 1 \\
 &= (a^n)^* (a + \dots + a^{n-1}) + (a^n)^* a^n + 1 \\
 &= (a^n)^* (a + \dots + a^{n-1}) + (a^n)^* \\
 &= (a^n)^* (1 + a + \dots + a^{n-1}) = E.
 \end{aligned}$$

Pour établir $((E^2 = E)/(E^* = 1 + E))$ dans S_1 , on commence par le cas où $c(E) = 0$:

$$E^2 = E \text{ donne successivement } 1 + E = (1 + E)E + 1, \quad 1 + E = E^*.$$

Et si $c(E) = 1$, alors $E = 1 + E'$ avec $c(E') = 0$, d'où successivement

$$E^2 = E, \quad 1 + E' = (1 + E')^2 = 1 + E' + E' E' = (1 + E') E' + 1,$$

$$1 + E = (1 + E) E' + 1 \quad (\text{car } 1 + E = 1 + E'), \quad 1 + E = (E')^* = E^*.$$

(5) s'obtient en raisonnant comme suit dans $C + ((E^2 = E)/(E^* = 1 + E))$:

si $E_g E_h \leq E_{gh}$ et $(E_{g,g})^* = E_{g,g}$, alors $E_1^* = E_1$ (car $E_1 = E_{1,1}$, où 1 désigne ici l'élément neutre du monoïde) d'où

$$\sum E_g = 1 + \sum E_g,$$

d'où

$$(\sum E_g)^2 = (1 + \sum E_g)^2 = 1 + \sum E_g + \sum E_g E_h = 1 + \sum E_g = \sum E_g,$$

d'où

$$(\sum E_g)^* = 1 + \sum E_g = \sum E_g.$$

Note : La conjecture de Conway reste à établir, mais l'utilisation des séries formelles (cf. [1]) a permis d'analyser les problèmes de complétude dans le cadre plus général des identités rationnelles définies sur un semi-anneau quelconque (cf. [3]).

BIBLIOGRAPHIE

- [1] J. BERSTEL et C. REUTENAUER, *Les séries rationnelles et leurs langages*, Collection E.R.I., Masson, Paris, 1984.
- [2] J. H. CONWAY, *Regular Algebra and Finite Machines*, Chapman & Hall, 1971.
- [3] D. KROB, *Expressions K-rationnelles*, Thèse d'Université, Université Paris-VII, 1988 (Rapport L.I.T.P. 88-23).
- [4] A. SALOMAA, *Twø Complete Axiom Systems for the Algebra of Regular Events*, J.A.C.M., vol. 13, 1966, p. 158-169.