INFORMATIQUE THÉORIQUE ET APPLICATIONS

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>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 24, n° 4, 1990, p. 419 à 423)

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 $a, b, c, \ldots$ comme variables (parcourant les langages) et les lettres majuscules $A, B, C, \ldots$ comme termes que l'on peut construire à partir des variables, des constantes 0, 1 et des opérations rationnelles $+, ., *$. 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 $a, b, c, \ldots$ les valeurs $\{a\}, \{b\}, \{c\}, \ldots$. 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 $a, b, c, \ldots = 0$, 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.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/90/04 419 05/$2.50/

2. LE SYSTÈME DE SALOMAA [4]

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

S1 $a+0=a$,	S7 $1.a=a$
S2 $a+b=b+a$,	S8 $a(b+c)=ab+ac$
S3 $(a+b)+c=a+(b+c)$,	S9 $(b+c)a=ba+ca$
S4 $a.0=0$,	S10 $(ab)c=a(bc)$
S5 $0.a=0$,	S11 $(1+a)^*=a^*$
S6 $a.1=a$,	S12 $a^*=1+a^*a$.

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 :

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

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) :

C1-C10 qui coïncident avec S1-S10

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

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

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

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

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

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

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

$$\begin{array}{ccccc} & & C_1 & & \\ & \overset{(1)}{\nearrow} & & \overset{(3)}{\searrow} & \\ S^+ & & & & C+\dfrac{E^2=E}{E^*=1+E} \overset{(5)}{\to} C^+ \\ & \underset{(2)}{\searrow} & & \underset{(4)}{\nearrow} & \\ & & S_1 & & \end{array}$$

où

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

et chaque $\to$ *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^+ :

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

(2) est trivial.

(3) s'obtient par la déduction suivante :

$E^2=E$, $E=EE^*$, $E^*=1+EE^*=1+E$ (par C12 avec $a=$ E 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 :

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

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

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

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

$E^2 = E$ 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

$$E^2=E, \qquad 1+E'=(1+E')^2=1+E'+E'E'=(1+E')E'+1,$$
$$1+E=(1+E)E'+1 \quad (\text{car } 1+E=1+E'), \qquad 1+E=(E')^*=E^*.$$

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

si $E_g E_h \leqq E_{gh}$ 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, *Two Complete Axiom Systems for the Algebra of Regular Events*, J.A.C.M., vol. 13, 1966, p. 158-169.