RAIRO. INFORMATIQUE THÉORIQUE

JEAN-CLAUDE RAOULT

Finiteness results on rewriting systems

RAIRO. Informatique théorique, tome 15, nº 4 (1981), p. 373-391
<http://www.numdam.org/item?id=ITA_1981__15_4_373_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 15, n° 4, 1981, p. 373 à 391)

FINITENESS RESULTS ON REWRITING SYSTEMS (*)

by Jean-Claude RAOULT (1)

Communicated by M. NIVAT

Résumé. — *Étant donné un système de récriture de termes du premier ordre noetherien et confluent, on considère la relation d'équivalence engendrée, et on prouve que le problème de la finitude d'une classe (ou de toutes les classes) est indécidable, sauf si l'on se restreint aux termes sans variables. En revanche, la finitude du nombre de classes est décidable.*

Abstract. — *Given a rewriting system on terms of first order which is known to be noetherian and confluent, it is proved that deciding the finiteness of the equivalence classes is impossible, unless we restrict attention to variable-free terms. On the other hand, one can decide whether the number of classes is finite.*

I. INTRODUCTION

Term rewriting systems frequently occur in the operational semantics of programming languages. They model ALGOL's copy rule, and in this respect, it is interesting to know whether they satisfy the "Church-Rosser" property. More generally, they model the computation of a program, represented as a term written over a given alphabet; in this case, the computation is hoped to terminate (the rewriting rule is hoped to be noetherian) and this fact is known to be undecidable (*cf.* [3]). So let us suppose now the rewriting rule to be noetherian, and ask if it is decidable that any term computes to a finite number of results only (*cf.* also [5]). The answer to this question is no, as is shown below (*cf.* theorem 1).

From another point of view, grammars over the free monoid generated by a finite alphabet can be generalized into grammars over the free algebra generated by a finite graded alphabet. All questions relevant to the previous case may be asked again, for instance:

— is it decidable, given the rules and an axiom, that the generated language is finite ? The answer is yes (*cf.* theorem 2);

— is it decidable, under the same assumptions that the generated language is rational ? No general answer has been given as yet (to the knowledge of the

(*) Received February 1980, revised November 1980.

(1) Laboratoire de Recherche en Informatique, Université de Paris-Sud, Orsay, France.

author) but a particular case is more tractable: if the number of equivalence classes is finite, then each class is rational. That last condition is decidable for a "Church-Rosser" relation.

II. CONFLUENT AND NŒTHERIAN PRECONGRUENCES

Let $F=F_0+F_1+\ldots+F_k+\ldots$ be a denumerable disjoint union of sets. An *F-algebra* is a set D together with a k-ary function $f_D : D^k \to D$ for each k and $f \in F_k$. A *subalgebra* is a subset closed under the functions f_D. The *product* $D \times D'$ of two F-algebras is again an F-algebra, in which the functions f_D are applied componentwise:

$$f_{D\times D'}((d_1,d'_1),\ldots,(d_k,d'_k))=(f_D(d_1,\ldots,d_k),f_{D'}(d'_1,\ldots,d'_k)).$$

A relation $R \subseteqq D \times D'$ is *compatible* when R is a subalgebra of $D \times D'$:

$$d_i\, R\, d'_i \quad \text{for } 1 \leqq i \leqq k \quad \Rightarrow \quad f_D(d_1,\ldots,d_k)\, R\, f_{D'}(d'_1,\ldots,d'_k).$$

A mapping $\sigma : D \to D'$ between two algebras is a *morphism* when $\{(d, d\sigma); d \in D\}$ is a compatible relation.

Given a set X, the free F-algebra over X is denoted by $M(F,X)$ and its elements are called *terms*. A *subterm* of t is t itself, or if $t=ft_1\ldots t_k$ then a subterm of one of the t_i's. Terms can be considered as labelled trees, and subterms can be addressed, like subtrees, by occurrences: an *occurrence* is a word $u \in N^*$ and the term t/u is defined by induction on t and u. If $u=\varepsilon$ then $t/u=t$, else $u=ku'$ $(k \in N)$ and if $t=ft_1\ldots t_n$ and $1 \leqq k \leqq n$ then $t/u=t_k/u'$; otherwise, t/u does not exist.

DEFINITION 1: A relation $\to$ over $M(F,X)$ is called a *precongruence* when it is reflexive, compatible and invariant under substitution:

(i) $t \to t$ for all t in $M(F,X)$;
(ii) $t_i \to t'_i (1 \leqq i \leqq k) \Rightarrow ft_1\ldots t_k \to ft'_1\ldots t'_k$ for all k and f in F_k;
(iii) $t \to t' \Rightarrow (t\,\sigma) \to (t'\,\sigma)$ for all $\sigma : M(F,X) \to M(F,X)$.

It is easy to check that the intersection of a family of precongruences is again a precongruence, so that.

PROPOSITION 1: *The set of all precongruences over $M(F,X)$ is a complete lattice with respect to set inclusion.*

Beware that the l. u. b. is indeed the intersection, and that the g. l. b. contains the union, but can be strictly greater.

Hence, given a relation S, one can define the precongruence $\underset{S}{\rightarrow}$ (or $\rightarrow$) *generated* by S, and the precongruence *induced* by S, respectively as the smallest precongruence containing S, and the greatest precongruence contained in S. The congruence generated by S is the (reflexive) symmetric and transitive closure of $\underset{S}{\rightarrow}$ and is denoted by $\overset{*}{\underset{S}{\leftrightarrow}}$ (or $\overset{*}{\leftrightarrow}$). One can prove by induction on the structure of the terms (*cf.* [6]) that $t \underset{S}{\rightarrow} t'$ is equivalent to:

$$\exists c \in M(F,X), x_1, \ldots, x_n \in X, \quad g_1 \rightarrow d_1, \ldots, g_n \rightarrow d_n \in S,$$

$\sigma_1, \ldots, \sigma_n$ substitutions, such that:

$$t = c[g_1 \sigma_1/x_1, \ldots, g_n \sigma_n/x_n]$$

and:

$$t' = c[d_1 \sigma_1/x_1, \ldots, d_n \sigma_n/x_n].$$

Thus $t \underset{S}{\rightarrow} t'$ means that t rewrites in t' in one step of n simultaneous and disjoint applications of the rules of S. When $n=1$, we say that $t \underset{S}{\rightarrow} t'$ is a single rewriting. Of course the single rewritings and the whole precongruence have the same reflexive and transitive closure.

DEFINITION 2: Given a relation $\rightarrow$ over $M(F,X)$ and a subset E of $M(F,X)$, a term t of E is *extremal* in E when $t \overset{*}{\rightarrow} t'$ & $t' \in E$ imply $t' = t$.

PROPOSITION 2: *The following assertions are equivalent:*

(i) *every infinite chain* $t_0 \overset{*}{\rightarrow} t_1 \overset{*}{\rightarrow} \ldots \overset{*}{\rightarrow} t_n \overset{*}{\rightarrow} \ldots$ *is eventually constant;*

(ii) *every non-empty set E contains an element extremal in E.*

A relation satisfying these assertions is called a *noetherian* relation [1].

Proof: (i) $\Rightarrow$ (ii), suppose that the non-empty set E contains no extremal element, and construct by induction a chain:

$$t_0 \rightarrow t_1 \rightarrow \ldots \rightarrow t_n \rightarrow \ldots$$

Indeed, since t_n is not extremal, there exists in E an element $t_{n+1} \neq t_n$ such that $t_n \rightarrow t_{n+1}$. The chain got in this way is not eventually constant.

(ii) $\Rightarrow$ (i) is clear.

DEFINITION 3: A relation $\rightarrow$ is said to be *confluent* when for all t_1, t_2, t_3:

$$(t_1 \overset{*}{\rightarrow} t_2 \text{ and } t_1 \overset{*}{\rightarrow} t_3) \text{ implies } \exists t_4, (t_2 \overset{*}{\rightarrow} t_4 \text{ and } t_3 \overset{*}{\rightarrow} t_4).$$

PROPOSITION 3: *Let S be a relation over $M(F, X)$. If $\underset{S}{\rightarrow}$ is noetherian, the following assertions are equivalent:*

(i) $\underset{S}{\rightarrow}$ *is confluent;*

(ii) $\forall\, t_1, t_2, t_3, (t_1 \xrightarrow{*} t_2 \;\&\, t_1 \xrightarrow{*} t_3) \Rightarrow \exists\, t_4, (t_2 \xrightarrow{*} t_4 \;\&\, t_3 \xrightarrow{*} t_4)$;

(iii) *every term t rewrites into a unique extremal $\bar{t}$ called the* irreducible (*or* normal) form *of t*

Proof: (i) $\Rightarrow$ (ii) is clear.

(ii) $\Rightarrow$ (iii): since $\underset{S}{\rightarrow}$ is noetherian, every term admits at least one irreducible form. Let M denote the set of those which admit more than one, and t an element of M. Then t admits at least two irreducible forms $\bar{t}_1$ and $\bar{t}_2$ and we have:

$$\begin{tikzcd}
 & t_1 \arrow[r, "*"] \arrow[dr, "*"'] & \bar{t}_1 & \\
t \arrow[ur, "*"] \arrow[dr, "*"'] & & u \arrow[r, "*"] & \bar{u} \\
 & t_2 \arrow[r, "*"] \arrow[ur, "*"] & \bar{t}_2 &
\end{tikzcd}$$

From (ii), we deduce the existence of u and its irreducible form $\bar{u}$. Since t is extremal in M, t_1 is not in M, hence $\bar{t}_1 = \bar{u}$ Similarly, t_2 is not in M, hence $\bar{t}_2 = \bar{u}$ .Thus t admits a unique irreducible form: t is not in M .Hence $M = \emptyset$

(iii) $\Rightarrow$ (i): take $\bar{t}_1$ for t_4 in definition 3.

See [2] for another proof.

III. THE FINITENESS OF THE CLASSES

DEFINITION 4: A term s overlaps a term t if there exist substitutions σ and τ, and a subterm u of t (u not a variable) such that:

$$u\,\sigma = s.\tau.$$

Given a relation S over $M(F, X)$ one can prove that a sufficient condition for $\underset{S}{\rightarrow}$ to be confluent is that the left-hand sides of S do not overlap one another (*see* for instance [4, 2, 6]) but this condition is by no means necessary as is shown by the simple example:

$$S = \{fa \rightarrow b, fb \rightarrow b, a \rightarrow b\}.$$

THEOREM 1: *The problem of determining, given a finite* $S \subset M(F,X)^2$ *and* $t \in M(F,X)$, *whether the congruence class* $[t]_S$ *of* t *modulo* $\overset{*}{\underset{S}{\leftrightarrow}}$ *is finite is undecidable, even if* $\underset{S}{\rightarrow}$ *is noetherian and the left-hand sides of* S *cannot overlap (and in particular,* $\overset{*}{\underset{S}{\rightarrow}}$ *is confluent). It is also undecidable whether all the classes are finite.*

The proof uses the two following lemmas.

LEMMA 1: *Let* S *be a finite relation over* $M(F,X)$ *with* $\underset{S}{\rightarrow}$ *noetherian and confluent. Then* $[t]_S$ *infinite* $\Leftrightarrow$ *there exists a co-chain* $\ldots \rightarrow t_n \rightarrow \ldots \rightarrow t_1 \rightarrow \bar{t}$ *with distinct* t_i*'s.*

$\Leftarrow$: clear.

$\Rightarrow$: note that:

(1) Since S is finite, only a finite number of terms s satisfy $s \underset{S}{\rightarrow} t$,

(2) $s \in [t] \Leftrightarrow s \overset{*}{\rightarrow} \bar{t}$ [from proposition 3 (iii)].

Apply Koenig's lemma to the relation $s\,R\,t$ iff $t \rightarrow s$ & $t \neq s$, and get an infinite co-chain $\ldots \rightarrow t_n \rightarrow \ldots \rightarrow \bar{t}$. No two t_i's can be equal because $\underset{S}{\rightarrow}$ is acyclic, hence the result.

Recall that a Turing machine is defined by a finite set Q of states, the position of a head on an input-output tape, a finite tape alphabet A and a finite set of quintuples:

$$(q, a, q', a', e) \in Q \times A \times Q \times A \times \{-1, +1\},$$

meaning: the machine in state q reading symbol a goes in state q', overprints a' and moves its head left or right if $e = -1$ or $+1$.

LEMME 2: *A Turing machine can be simulated by a rewriting system* S *such that* $\underset{S}{\rightarrow}^{-1}$ *is noetherian and the right-hand sides of* S *do not overlap (hence* $\underset{S}{\rightarrow}^{-1}$ *is confluent). Furthermore all the terms in* S *contain at most one occurrence of each variable.*

Proof: We begin by coding the machine in much the same way as in [3]. The tape of the TM is assumed to be filled with blanks except for a finite portion.

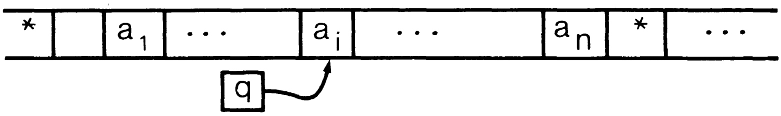

Figure 1

Take $F'_0 = d$, where $d \notin A$, $F_1 = Q + A + \bar{A} + \{g\}$ where $g \notin A$ is meant to be a left marker, and $\bar{A} = \{\bar{a};\, a \in A\}$.

The symbol $b \in A$ denotes the blank. A configuration c such as the one pictured in figure 1 can be represented by the set $T(c)$ of terms of the form (parentheses are omitted for easier reading):

$$gbb \ldots ba_1 \ldots q\bar{a}_i \ldots \bar{a}_n \bar{b} \ldots \bar{b}d$$

(the barred symbols indicate that the head is on their left).

Each quintuple is represented by a finite number of rewriting rules according to the following algorithm. Call R the set of rewriting rules and:

– initialize R to the empty set;

– for all $(q, a, q', a', 1)$ add to R the rule $q\bar{a}x \to a'q'x$ and if $a = b$ add also $qd \to a'q'd$, extending the workspace on the right;

– for all $(q, a, q', a', -1)$ add to R the finite set $\{cq\bar{a}x \to q'\overline{ca}'x;\, c \in A\} + \{gq\bar{a}x \to gq'\overline{ba}'x\}$ that last rule extending the workspace on the left; if $a = b$ the head of the Turing machine may be on a square corresponding with d, so add to R also the set $\{cqd \to q'\overline{ca}'d;\, c \in A\} + \{gqd \to gq'\bar{a}'d\}$.

Now we define the rewriting system S, by adding one argument to the function q, which will indicate the rule in S which has just been applied. Let n be the number of rules of R and set:

$$F'_0 = \{d, 0\}, \qquad F'_1 = A + A + \{g, 1, \ldots, n\}, \qquad F'_2 = Q.$$

With rule number i of R, of the form $uqv \to u'q'v'$ associate the rule of S, written in a tree-like form:

$$\begin{array}{ccc} u-q-v & \to & u'-q'-v'. \\ \;\;| & & \;\;| \\ \;\;y & & \;\;i \\ & & \;\;| \\ & & \;\;y \end{array}$$

Notice that the length of the first argument of q is incremented by 1 each time a rule of S is applied; hence $\underset{S}{\to}^{-1}$ is noetherian. The first argument of q behaves like a write-only stack, and the top symbol indicates the last rule which has been applied. The symbols on the right of q are barred but those on the left are not, so that no overlapping is possible. Finally, variables x and y occur only once in each term of S.

With a configuration c is now associated a set of terms of the form:

$$g-b-\ldots-a_1-\ldots-a_{i-1}-\underset{\displaystyle s}{\underset{|}{q}}-\bar{a}_i-\ldots-\bar{a}_n-\bar{b}-\ldots\bar{b}-d,$$

where $s \in M(\{0, 1, \ldots, n\}, \emptyset)$.

CLAIM: *Given a configuration c and a term t in $T(c)$, there is a one-to-one correspondence between the transitions $c \to c'$ of the Turing machine and the single rewritings $t \underset{S}{\to} t'$, with $t' \in T(c')$.*

The proof is an easy but tedious argument by cases on the quintuple.

To prove the theorem, consider a Turing machine starting in state q on an initial configuration $c=a_1 \ldots a_n$ with its head pointing on the square a_i. Associate with it the rewriting system S as in lemma 2, and the term:

$$t=g-a_1-\ldots-a_{i-1}-\underset{\displaystyle 0}{\underset{|}{q}}-\bar{a}_i-\ldots-\bar{a}_n-d.$$

Then $[t]_S$ is finite if and only if there is no infinite chain:

$$\bar{t} \underset{S}{\to}^{-1} t_1 \underset{S}{\to}^{-1} t_2 \ldots \underset{S}{\to}^{-1} t_n \underset{S}{\to}^{-1} \ldots$$

Since $\underset{S}{\to}^{-1}$ is noetherian and confluent, $\bar{t}$ can be computed in a finite amount of time, so that deciding whether there exists such an infinite chain is equivalent to deciding whether the Turing machine halts on input c; this is impossible. This proves the first assertion of the theorem.

As for the second, we shall show that all the equivalence classes under $\overset{*}{\underset{S}{\leftrightarrow}}$ are finite if and only if the Turing machine halts on every initial configuration c. The "only if" part is clear since shall be finite in particular the classes of the terms representing the initial configurations of the machine. To prove the converse, we prove that if there exists one term the class of which is infinite, then the Turing machine does not halt on some initial configuration. Associate with each term t the set $OC(t)$ of all occurences of binary symbols q.

LEMMA 3: *For two terms t and t' such that $t \underset{S}{\to} t'$, the sets $OC(t)$ and $OC(t')$ are isomorphic.*

Proof: Either the occurrence u of q has not been rewritten, and $u \mapsto u$; or the occurrence has been rewritten by a rule simulating a right move of the head, and $u \mapsto u\,1$; or again, the occurrence has been rewritten by a rule simulating a left move, hence $u = u'\,1$, and $u \mapsto u'$.

If we identify the corresponding occurrences and since there is only a finite number of them, the term t admits an infinite number of rewritings if and only if one of the occurrences in $OC(t)$ is rewritten an infinite number of times This occurrence can be associated with a subterm of t of the form:

$$\begin{array}{rcl} a_1 - \ldots - a_{i-1} - & q & - a_i - \ldots - a_n - x, \\ & | & \\ & k_1 & \\ & | & \\ & \vdots & \\ & | & \\ & k_m & \\ & | & \\ & y & \end{array}$$

where x and y are subterms of t, and n and m are maximal. Then the term:

$$\begin{array}{rcl} g - a_1 - \ldots - a_{i-1} - & q & - \bar{a}_i - \ldots - \bar{a}_n - d, \\ & | & \\ & k_1 & \\ & | & \\ & \vdots & \\ & | & \\ & 0 & \end{array}$$

represents a configuration of the Turing machine, and is rewritten infinitely often. This concludes the proof of theorem 1.

The situation is different if S contains only ground terms, i.e. terms which contain no variable, or equivalently if no substitution is allowed.

LEMMA 4: *Given a relation $\rightarrow$ with finite image (i.e. $\{s; t \rightarrow s\}$ is finite for all t), and a term t, there exists an infinite number of elements s such that $t \overset{*}{\rightarrow} s$ if and only if there exists an infinite chain:*

$$t \rightarrow t_1 \rightarrow \ldots \rightarrow t_n \rightarrow \ldots$$

with distinct t_i's.

Proof: Construct the tree of all sequences $t \rightarrow t_1 \rightarrow \ldots \rightarrow t_m$ such that the father of the sequence above is the sequence $t \rightarrow t_1 \rightarrow \ldots \rightarrow t_{m-1}$. The tree is finitely branching. Prune all subtrees whose root occurs already somewhere in the tree either less deep or at the same depth but on the left. The remaining tree contains an infinite number of distinct nodes, hence has a branch of infinite length (Koenig's lemma).

Q.E.D.

LEMMA 5: *Let $\rightarrow$ be a precongruence generated by a finite system $S=\{g_1 \rightarrow d_1, \ldots, g_n \rightarrow d_n\}$ of ground terms. There exists an infinite number of terms s such that $t \overset{*}{\rightarrow} s$ if and only if there exist two terms t_1 and t_2, two occurrences u, $v \in \mathbb{N}^*$, $v \neq \varepsilon$, and a rule $g_i \rightarrow d_i$ such that:*

$$t \overset{*}{\rightarrow} t_1 \overset{*}{\rightarrow} t_2 \qquad \textit{and} \qquad t_1/u=d_i \;\&\; t_2/uv=g_i.$$

Proof: The sufficiency is clear. The converse is proved by induction on the cardinality n of S. It is trivially true for $n=0$. If $n\neq 0$, there exists an infinite sequence of single rewritings:

$$t=t_0 \rightarrow t_1 \rightarrow \ldots$$

with distinct t_i's.

We shall prove the intermediate result that there exists an occurrence u and a subsequence of single rewritings such that the image of the subsequence under the occurrence u is of the form:

$$d_i \rightarrow \ldots \rightarrow t_h \rightarrow \ldots$$

Indeed, either $t_k=d_i$ for some k and i, and the result is true for $u=\varepsilon$ and the subsequence starting at t ; or else $t=ft_1 \ldots t_n$ and one t_j admits an infinite sequence of rewritings. By induction on $|t|$ there exists a subsequence of infinite rewritings, and an occurrence u of t_j such that the image of the subsequence under the occurrence u is:

$$d_i \rightarrow \ldots \rightarrow t_m \rightarrow \ldots$$

This is also the image of the same subsequence of rewritings of t under the occurrence ju. So is proved the intermediate result.

If the precongruence generated by $S-\{g_i \to d_i\}$ has a reflexive and transitive closure of infinite image, the result is true by induction on n. Otherwise, since the sequence contains an infinite number of distinct terms, the rule $g_i \to d_i$ must be applied. If an all instances $t_k \to t_{k+1}$ of this rule, $t_k = g_i$, the subsequence contains only a finite number of distinct terms. Therefore:

$$\exists k, v, \quad t_k/v = g_i \;\&\; v \neq \varepsilon.$$

THEOREM 2: *Given a finite rewriting system S of ground terms, and the generated congruence, one can decide whether the congruence class of a term t is finite. It is also decidable whether all classes are finite.*

Proof: From lemma 5, the class $[t]=\{s;\, t \overset{*}{\underset{S}{\leftrightarrow}} s\}$ is infinite if and only if there exist two terms t_1 and t_2, two occurrences u and $v(v \neq \varepsilon)$ and a rule $g_i \to d_i \in S \cup S^{-1}$ such that:

$$t \xrightarrow[S \cup S^{-1}]{*} t_1 \xrightarrow[S \cup S^{-1}]{*} t_2 \;\&\; t_1/u = d_i \;\&\; t_2/uv = g_i.$$

The algorithm consists of finding the terms t_1 and t_2 (if they exist) in the following way. Generate the tree of single rewritings of t for $S \cup S^{-1}$ by successive depths When a term is encountered which has already been seen, it is omitted together with the whole subtree of which it is the root. If $[t]$ is finite, the algorithm terminates. With each node of the tree is associated the pair (u, i) of the occurrence u and the number i of the rule of S which has just been applied, and it is compared to the pairs which have already been computed on the same branch. If $[t]$ is infinite, there must exist two pairs (u_1, i) and (u_2, i) with:

$$u_2 = u_1 v \qquad (v \neq \varepsilon)$$

and the algorithm terminates also in this case.

To prove the second assertion, notice that if there exists an infinite congruence class $[t]$, there exist two terms t_1 and t_2, two occurrences $u, v \in \mathbb{N}^* (v \neq \varepsilon)$ and a rule $g_i \to d_i \in S \cup S^{-1}$ such that:

$$t \xrightarrow[S \cup S^{-1}]{*} t_1 \xrightarrow[S \cup S^{-1}]{*} t_2 \;\&\; t_1/u = d_i \;\&\; t_2/uv = g_i.$$

Applying the same lemma to $t'_1 = t_1/u = d_i$, $t'_2 = t_2/u$, $u' = \varepsilon$ and $v' = v$ we see that the class $[d_i]$ is infinite. Hence it suffices to run the algorithm above on the terms $d_1, \ldots, d_n$.

IV. A REVIEW ON RATIONAL FORESTS

As is the case with languages in a free monoid, the rational forests can be characterized by accepting devices (finite automata), generating devices (linear grammars), or by purely algebraic means (finite index congruences). In this section, these three possibilities are defined and proved equivalent.

DEFINITION 4: A *finite ascending F-automaton* is a finite F-algebra Q of *states* together with a subset $P \subseteq Q$ of *final states*.

Since $T(F)$ is a free F-algebra, there exists a unique morphism $\mu : T(F) \to Q$. A term t is *accepted* by the automaton Q when $t\mu$ is a final state.

DEFINITION 5: A *finite descending F-automaton* is a finite set Q of *states* together with a relation $f_Q \subseteq Q \times Q^n$ for all $f \in F$, where n is the arity of f.

We shall note $qf(q_1, \ldots, q_n)$ instead of $(q, q_1, \ldots, q_n) \in f_Q$. It is also possible to write $(q_1, \ldots, q_n) \in f_Q(q)$, and then f_Q is considered as a function $Q \to 2^Q$. There may exist several n-tuples $(q_1, \ldots, q_n)$. But if for all state q there is a unique n-tuple $(q_1, \ldots, q_n)$ such that $qf(q_2, \ldots, q_n)$ the automaton is *deterministic*.

If $a \in F_Q$, $a_Q \subseteq Q$ is merely a subset of Q: the domain of a_Q. If $q \in a_Q$ ones writes $qa_Q 1$, and says that a *erases* q. This definition is extended inductively: the term $t = ft_1 \ldots t_n$ *erases* the state q when there exists $qf(q_1, \ldots, q_n)$ and t_i erases q_i $(1 \leqq i \leqq n)$. A set L of terms is *accepted* by the descending automaton starting at a (finite) subset P of initial states if and only if L is the set of terms which erase at least one state of P.

DEFINITION 6: A rational grammar is a finite subset $G \subseteq X \times M(F, X)$ in which X is a finite set of nullary constants called *non-terminals*.

If a term t contains a non-terminal x, then this term will be rewritten into a term t' obtained from t by replacing x by one of its corresponding right-hand sides in G. The relation generated in this way is a left-precongruence, according to the following definition.

DEFINITION 7: A relation $\rightarrow$ over $M(F, X)$ is a *left-precongruence* when it is reflexive and compatible:

(i) $t \rightarrow t$ for all $t \in M(F, X)$;

(ii) $t_i \rightarrow t'_i (1 \leqq i \leqq n) \Rightarrow ft_1 \ldots t_n \rightarrow ft'_1 \ldots t'_n$, for all n and all $f \in F_n$.

A *left-congruence* is a left-precongruence which is also an equivalence relation. Thus if $\rightarrow$ denotes the left-precongruence generated by G over $M(F, X)$, then the language $L(G, Y)$ generated by G from the set of axioms $Y \subseteq X$ is the set of terms $t \in M(F)$ such that $x \overset{*}{\underset{G}{\rightarrow}} t$ for some $x \in Y$ (the star denotes the transitive closure).

One can check, by adding a suitable number of new non-terminals (in fact one for each subterm of the right-hand sides of G), that one can define a new grammar G' of the following type:

$$G' \begin{cases} \ldots, & \\ x \rightarrow f y_1 \ldots y_n, & x, y_i \in X, \quad f \in F_n, \\ \ldots, & z \in X, \quad a \in F_\varphi, \\ z \rightarrow a & \end{cases}$$

This simpler grammar generates nevertheless the same language from the same set of starting axioms.

Example:

$$G \begin{cases} x \rightarrow f(g(x, x), y) + b, \\ \quad y \rightarrow g(a, x) + b, \end{cases} \qquad G' \begin{cases} x \rightarrow f(z, y) + b, \\ y \rightarrow g(u, x) + b, \\ z \rightarrow g(x, x), \\ u \rightarrow a. \end{cases}$$

PROPOSITION 4: *Let L be a subset of $M(F)$. The following assertions are equivalent:*

(i) *$L = L(G, Y)$ for some rational grammar G;*

(ii) *L is accepted by a finite descending F-automaton;*

(iii) *L is accepted by a finite ascending F-automaton;*

(iv) *L is a union of equivalence classes for a left-congruence of finite index.*

We prove (iv) $\Leftrightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) $\Rightarrow$ (iii).

(iv) $\Leftrightarrow$ (iii): let $\sim$ denote the left-congruence, and:

$$\mu : \quad M(F) \rightarrow M(F)/\sim$$

be the projection onto the finite quotient. In order to define a finite automaton accepting L, set $Q = M(F)/\sim$. The assumption that L is a union of equivalence classes for $\sim$ implies that there exists a (finite) subset $P \subseteq Q$ such that $L = P\mu^{-1}$, or $t \in L \Leftrightarrow t\mu \in P$.

Conversely, any finite ascending F-automaton $\mu : M(F) \to Q$ defines a left-precongruence over $M(F) : t \sim t'$ iff $t\mu = t'\mu$. The accepted set L of terms is $P\mu^{-1} = \bigcup_{q \in P} q\mu^{-1}$, i.e. a finite union of equivalence classes.

(iii) $\Rightarrow$ (ii): simple duality transforms an ascending automaton into a descending one: the sets of states are isomorphic, the set of initial states of the descending automaton corresponds to the set of final states of the ascending automaton. For the transitions of the descending automaton, set:

$$q f_Q(q_1, \ldots, q_n) \quad \text{iff} \quad q = f_Q(q_1, \ldots, q_n),$$

in the ascending automaton.

Clearly t erases q in the descending automaton if and only if t is accepted (with final state q) by the ascending automaton.

(ii) $\Rightarrow$ (i) by a classical argument: let X be a set of non-terminals isomorphic with Q, and x_q be the non-terminal associated with q. Define the following grammar:

$$(x_q \to f x_{q_1} \ldots x_{q_n}) \in G \quad \Leftrightarrow \quad q f_Q(q_1, \ldots, q_n),$$

for all n-ary symbols f, and all $n > 0$. If $a \in F_0$, then:

$(x_q \to a) \in G \Leftrightarrow a$ erases q in the finite automaton.

It is easily checked by induction on the structure of t that t erases q if and only if $t \in L(G, x_q)$; so that if $Y \subseteq X$ is the set of non-terminals associated with the initial states of Q, then:

$$L = L(G, Y).$$

(i) $\Rightarrow$ (iii): Let the grammar G be of the simple form:

$$G \begin{cases} \ldots, & \\ x \to f y_1 \ldots y_n, & x, y_i \in X, \quad f \in F_n, \\ z \to a. & z \in X, \quad a \in F_0, \end{cases}$$

where X is the finite set of non-terminals.

Define a finite F-algebra Q, the elements of which are all subsets $q \subseteq X$, endowed with the following operations:

$$a_Q = \{ x \in X ; x \to a \text{ is in } G \} \quad \text{for all } a \in F_\varphi,$$

and:

$$f_Q(q_1, \ldots, q_n) = \{x \in X; \exists y_1 \in q_1, \ldots, \exists y_n \in q_n, x \to f y_1 \ldots y_n \text{ is in } G\},$$

for all $f \in F_n$. There exists a unique morphism $\mu : M(F) \to Q$. Let us check by induction on the structure of t that $x \in t\,\mu$ if and only if $x \overset{*}{\underset{G}{\to}} t$. In fact, it is the definition of t_Q if $t \in F_0$, and if $t = f t_1 \ldots t_n$, then:

$$\begin{aligned} x \in t\,\mu \quad &\Leftrightarrow \quad x \in f_Q(t_1\,\mu, \ldots, t_n\,\mu), \text{ because } \mu \text{ is a morphism.} \\ &\Leftrightarrow (x \to f y_1 \ldots y_n) \in G \;\&\; y_i \in t_i\,\mu \quad \text{for all } i, \text{ by definition of } f_Q. \\ &\Leftrightarrow \quad (x \to f y_1 \ldots y_n) \in G \;\&\; y_i \overset{*}{\underset{G}{\to}} t_i, \text{ by induction hypothesis.} \\ &\Leftrightarrow \quad x \overset{*}{\underset{G}{\to}} t. \end{aligned}$$

Therefore Q accepts the set $L(G, Y)$ if the set of final states is Y. ■

Note that the finite F-algebra Q defined above is also a $(F+X)$-algebra in which:

$$x_Q = \{x\} \quad \text{for all } x \in X.$$

Therefore μ can be extended into a morphism $M(F, X) \to Q$ which is again denoted by μ. The relation $t\,\mu = t'\,\mu$ is a left-congruence over $M(F, X)$ which has a finite index, and L is invariant under its restriction to $M(F)$:

$$\forall \; t, t' \in M(F), \qquad (t \in L \;\&\; t\,\mu = t'\,\mu) \;\Rightarrow\; t' \in L.$$

As is the case with monoids, there is a coarsest such left-congruence:

PROPOSITION 5: *Let L be a subset of $M(F)$. Then L is rational if and only if the following left-congruence has a finite index:*

$$t \sim t' \quad \textit{iff} \;\; \forall \; c \in M(F, X), \; \forall \; x \in X, \quad c[t/x] \in L \;\Leftrightarrow\; c[t'/x] \in L.$$

Furthermore the quotient $M(F)/\sim$ is the smallest F-automaton accepting L.

Proof: Let S denote the set of all left-congruence over $M(F,X)$ such that L is invariant under their restriction to $M(F)$. Then $\sim\ \in S$ (take $c=x$), and any left-congruence $\equiv$ in S is contained in $\sim$: $\equiv \in S \Rightarrow \equiv \subseteq \sim$. Thus there is a unique surjective morphism $M(F)/\equiv\ \to M(F)/\sim$ such that the following triangle commutes:

$$\begin{array}{ccc} & \nearrow & M(F)/\equiv \\ M(F) & & \\ & \searrow & M(F)/\sim \end{array}$$

This proves the last assertion of the proposition. The first one follows immediately since $M(F)/\sim$ is finite if $M(F)/\equiv$ is finite. ■

If one wishes to consider congruences instead of left-congruences, the situation is nearly the same.

PROPOSITION 6: *Let $\sim$ be a left-congruence over $M(F,X)$, and $\simeq$ be the induced congruence. Then $\sim$ has a finite index if $\simeq$ has a finite index. The converse is true when X is finite.*

Proof: Since $t\simeq t' \Rightarrow t\sim t'$, the direct assertion is clear. Conversely consider the mapping:

$$M(F,X)\times M(F,X)^X \to M(F,X) \to M(F,X)/\sim,$$
$$(t,\sigma)\mapsto t\,\sigma \mapsto [t\,\sigma]_\sim .$$

If $t\simeq t'$, then $t\,\sigma\simeq t'\,\sigma$, hence $t\,\sigma\sim t'\,\sigma$, hence $[t\,\sigma]_\sim=[t'\,\sigma]_\sim$. And if for all $x\in X$, $x\,\sigma\sim x\,\sigma'$ (shortly $\sigma\sim\sigma'$) then $t\,\sigma\sim t\,\sigma'$ because $\sim$ is a left congruence. So that the above mapping factors through:

$$(M(F,X)/\simeq)\times(M(F/x)/\sim)^X \to M(F,X)/\sim .$$

Each class of congruence in $M(F,X)/\simeq$ thus appears as a function:

$$[t]_\simeq : (M(F,X)/\sim)^X \to M(F,X)/\sim,$$

which is easily checked to be injective. If X is finite, the set of functions $(T(F,X)/\sim)^X \to T(F,X)/\sim$ is finite, hence the result. ■

COROLLARY: *Let $L \in M(F,X)$ where X is a finite set of variables. Then L is rational if and only if either of the following equivalences has a finite index:*

(i) $t \sim t'$ *iff* $\forall c \in M(F, X), \forall\ x \in X,\ c[t/x] \in L \Leftrightarrow c[t'/x] \in L;$

(ii) $t \simeq t'$ *iff* $\forall c \in M(F, X), \forall\ x \in X, \forall\ \sigma$ *substitution*,

$$c[t\,\sigma/x] \in L \Leftrightarrow c[t'\,\sigma/x] \in L.$$

The congruence (ii) corresponds, for trees, to the syntactic congruence in the monoids.

V. THE FINITENESS OF THE NUMBER OF CLASSES

The aim of the present section is to prove the following theorem.

THEOREM 3: *Given a finite relation S over $M(F, X)$ such that $\underset{S}{\rightarrow}$ is noetherian and confluent, one can decide whether the congruence $\overset{*}{\underset{S}{\leftrightarrow}}$ has a finite index, if in the left-hand sides of S, each variable occurs at most once.*

Proof: Since $\underset{S}{\rightarrow}$ is noetherian and confluent, each class contains a unique extremal term t such that:

$$s \overset{*}{\rightarrow} t \Leftrightarrow s \overset{*}{\rightarrow} t \quad (cf.\ \text{prop. } 3).$$

The problem is now reduced to deciding whether there is a finite number of extremal terms. Turning things around, a term t is not extremal when there exists a term c containing a variable x, a substitution σ and a left-hand side g of S such that:

$$t = c[g\,\sigma/x].$$

This is the classical problem of recognizing the "pattern" g in the text t, and can be done with the help of a finite automaton (as in [7]).

For our purpose we shall use the following $(F+X)$-automaton. Define:

$$E = \{\ t \in M(F, X);\ t \text{ is a subterm of a left-hand side of } S\};$$

$Q = 2^E$, the set of subsets of E.

Since S is finite, E – hence Q – are also finite. Give Q the structure of a $(F+X)$-algebra: for all $f \in F+X$:

– if $f \in F_0 + X$, then $f_Q = E \cap \{f\}$;

– else $f_Q(q_1, \ldots, q_n) = \{ft_1 \ldots t_n \in E;\ (\forall i)\ t_i \in q_i \cup X\} \cup \bigcup_i (q_i \cap G)$,

where G is the set of all left-hand sides of S.

PROPOSITION 7: *The image $t\,\mu$ of a term $t \in M(F, X)$ in the $(F+X)$-algebra Q defined above is the set:*

$$t\,\mu=\{s \in E; \exists\,\sigma,\ t=s\,\sigma\} \cup \{q \in G; \exists\,c,\ \sigma,\ t=c[g\,\sigma/x]\}.$$

Proof by induction on the structure of t: if $t \in F_0+X$, then $t_Q=\{t\}$ or $\emptyset$ according as t belongs to E or not, and the proposition holds. If $t=ft_1 \ldots t_n$, then $t\,\mu=f_Q(t_1\,\mu, \ldots, t_n\,\mu)$ and the definition of f_Q yields:

$$t\,\mu=\{fs_1 \ldots s_n \in E; (\forall i)\ s_i \in t_i\,\mu \cup X\} \cup \bigcup t_i\,\mu \cap G.$$

Thus $s \in t\,\mu$ if and only if one of the following conditions is met:

(1) $s \in t_i\,\mu \cap G$ for some i. In that case $\exists\, c_i,\ \sigma_i \in t_i=c_i[s\,\sigma_i/x]$ by induction, and the variable x may be chosen so that it does not appear in any t_j for $j \neq i$. Then $t=c[s\,\sigma_i/x]$ with $c=ft_1 \ldots t_{i-1}\,c_i\,t_{i+1} \ldots t$;

(2) $s=fs_1 \ldots s_n$ and for all i, $s_i \in t_i\,\mu$ or $s_i \in X$, i.e.:

$$\forall\ i, \quad \exists\,\sigma_i, \qquad t_i=s_i\,\sigma_i$$

(if $s_i \in X$, then σ_i is defined by $t_i=s_i\,\sigma_i$). Since the term $s \in E$ is a subterm of a term in G, each variable $x \in X$ occurs in at most one s_i. Define the substitution σ by:

$x\,\sigma=x\,\sigma_i$ for all x occurring in s.

$x\,\sigma=x$ otherwise.

Then $t=s\,\sigma$. ■

Choose, for final states in P all subsets of E which do not contain any $g \in G$:

$$P=\{q \subseteq E; q \cap G=\emptyset\}.$$

Then $t\,\mu \in P$ if, and only if, t is irreducible. The following proposition concludes the proof of theorem 3.

PROPOSITION 8: *A finite automaton with n states accepts an infinity of terms in $M(F, X)$ where F and X are finite, if and only if it accepts a term the depth d of which satisfies:*

$$n \leqq d<2\,n.$$

Proof classical: If a term t is accepted, of depth d satisfying $n \leqq d<2\,n$, then there exists a *chain of subterms of length d*, that is a sequence:

$$t=s_0, s_1, \ldots, s_i, \ldots, s_j, \ldots, s_d,$$

where s_i is a subterm of s_{i-1} and $s_i \neq s_{i-1}$, for $1 \leqq i \leqq d$. There are more than n subterms so that there exist two subterms $s_i \neq s_j$ with $s_i\,\mu = s_j\,\mu$. Intuitively the subterm s_j can replace s_i arbitrarily many times without changing $t\,\mu$. Precisely define:

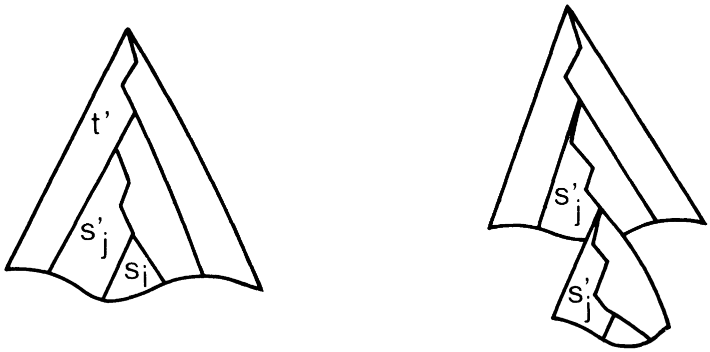

Figure 2

– t' such that $t = t'[s_j/x]$, and
– s' such that $s_j = s'[s_i/x]$, where x does not occur in t (cf. *fig.* 2).
Then:

$$t_n = t' \underbrace{[s'/x] \dots [s'/x]}_{n \text{ times}} [s_i/x],$$

is accepted by the automaton for all $n \in \mathbb{N}$.

Conversely suppose an infinite number of terms is accepted, and in particular, since $F+X$ is finite, a term t of depth at least n. Consider a chain:

$$t = s_0, s_1, \dots, s_n,$$

where s_i is a subterm of s_{i-1} $(1 \leqq i \leqq n)$, and of no other subterm of s_{i-1}: for some $f \in F$, $s_{i-1} = f(\dots s_i \dots)$. Since there are only n states, $s_i\,\mu = s_j\,\mu$ for some $i<j$. Associate with t the term t' obtained by replacing in t the subterm s_i by s_j, and write $t\,R\,t'$. Since t' contains less symbols from F than t', R is noetherian. Hence there exists a term $\bar{t}$ with $t\,R^*\,\bar{t}$, such that $\bar{t}\,R\,u$ is impossible. In $\bar{t}$, all chains of subterms have length less than n. Consider the last replacement: $s\,R\,\bar{t}$. There exists $c \in M(F, X)$ with:

$$s = c[s_i/x] \ \&\ \bar{t} = c[s_j/x].$$

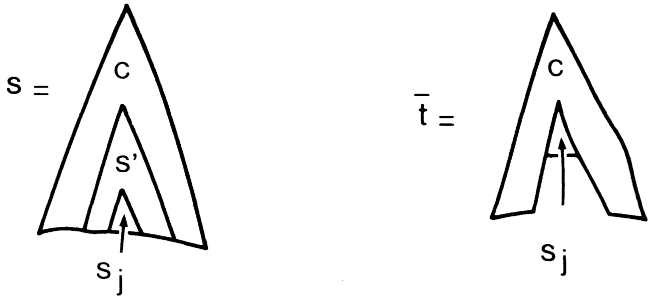

Figure 3

Define s' as the term such that $s_i = s'[s_j/x]$. The longest chain of subterms of s is:

$$s = s_0, s_1, \ldots, s_i, \ldots, s_j, \ldots, s_n, \ldots, s_d,$$

where $i+d-j<n$ since if is the length of a chain of subterms of $\bar{t}$, *viz* the chain:

$$s_0, \ldots, s_{i-1}, s_j, \ldots, s_n, \ldots, s_d.$$

In particular $j-i<n$. Replacing s_j by s_i in $\bar{t}$ and iterating $[(2n-d)/(j-i)]$ times yields a term of depth in $[n, 2n[$, accepted by Q. ■

To prove the theorem, construct the automaton as in proposition 7, and run it on the terms of depth d satisfying $n \leqq d < 2n$. Since there exists only a finite number of such terms, the automaton stops with the answer

REFERENCES

1. N. Bourbaki, *Théorie des Ensembles*, Chapt. III, § 6, No. 5, Hermann, Paris, 1963.
2. G. Huet, *Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems*, *in* Proceedings of the 18th annual I.E.E.E. Symposium on Fondations of Computer Science, October 1977.
3. G. Huet and D. S. Lankford, *On the Uniform Halting Problem for Term Rewriting Systems*, Rapport de Recherche, No. 283, I.R.I.A., March 1978.
4. D. E. Knuth and P. Bendix, *Simple Words Problems in Universal Algebras*, *in* Computational Problems in Abstract Algebras, Ed., J. Leech, Pergamon Press, 1970, pp. 263-297.
5. D. S. Lankford and A. M. Ballantyne, *The Refutation Completeness of Blocked Permutative Narrowing and Resolution* (to appear).
6. J. C. Raoult and J. Vuillemin, *Operational and Denotational Equivalences Between Recursive Programs*, Rapport de Recherche, No. 9, L.R.I., Orsay, June 1978.
7. J. W. Thatcher and J. B. Wright, *Generalized Finite Automata Theory with an Application to a Decision Problem of Second Order Logic*, Math. System Theory, Vol. 2, 1968, pp. 57-81.