INFORMATIQUE THÉORIQUE ET APPLICATIONS

JANA RYŠLINKOVÁ

Church-Rosser property and decidability of monadic theories of unary algebras

Informatique théorique et applications, tome 21, nº 3 (1987), p. 323-329.

<http://www.numdam.org/item?id=ITA_1987__21_3_323_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 21, n° 3, 1987, p. 323 à 329)

CHURCH-ROSSER PROPERTY AND DECIDABILITY OF MONADIC THEORIES OF UNARY ALGEBRAS (*)

by Jana RYŠLINKOVÁ (1)

Communicated by J.-E. PIN

Abstract. – *The main question we are interested in is the decidability of monadic theories (logical second-order theories) of some unary algebras. Here, the Church-Rosser property of the immediate inference relation for the presentation of unary algebras plays an important role. We get as a corollary of more general theorems that the monadic theory of finitely presented unary algebras is decidable.*

Résumé. – *Nous nous intéressons aux problèmes de la décidabilité des théories monadiques (théories logiques du second ordre) de certaines algèbres unaires. Dans ces questions, la propriété de Church-Rosser de la relation d'inférence de la présentation des algèbres unaires, joue un rôle important. Nous obtenons, en tant que corollaire de théorèmes plus généraux, que la théorie monadique des algèbres unaires qui sont finiment présentées est décidable.*

INTRODUCTION

Many problems require a construction of decision algorithms for logical theories. It is relatively easy to formulate those problems in the language of the predicate calculus. But just in this case, there is no decidable algorithm, as it is stated by Church theorem. But limiting us to certain structures only, we shall be able to get the decidability of the corresponding theories. Some of them are studied in this paper. The structures are unary algebras.

The main question we are interested in is the decidability of monadic logical theories of some unary algebras. Here, the Church-Rosser property

(*) Received October 1985, revised January 1987.
(1) ÙFSČSAV, Jilská 1, 11000 PRAHA 1, Tchécoslovaquie.

0296-1598 87/03 323 7/$ 2.70/© Gauthier-Villars

of the immediate inference relation for the presentation of unary algebras plays an important role. We get as a corollary of more general theorems that the monadic theory of finitely presented unary algebras is decidable.

I. RELATIONS

In this part, basic notions, their properties and some notations will be given. Whenever we say "relation", we mean binary relation on a given set.

Let a set A be given and let R, S be relations on A. Denote by $xR \rightleftharpoons \{y \mid xRy\}$ the image of x in R, by $R^{-1} \rightleftharpoons \{\langle x, y\rangle \mid \langle y, x\rangle \in R\}$ the inverse relation, by $R \circ S \rightleftharpoons \{\langle x, y\rangle \mid \exists z \langle x, z\rangle \in R$ et $\langle z, y\rangle \in S\}$the composition of R and S, by id the identity relation on A, by $R^* \rightleftharpoons \mathrm{id} \cup R \cup R^2 \cup R^3 \cup \ldots$ the reflexive and transitive closure of R, by $R^\sim$ the smallest equivalence relation on A containing R. We say that R is *terminating* if there is no infinite chain $a_1, a_2, \ldots$ with $a_i R a_{i+1}$ for all $i=1, 2, \ldots$ Relation is *Church-Rosser* if $R^\sim = R^* \circ (R^{-1})^*$. Element $a \in A$ is called *irreducible* (with respect to R) if $aR = \varnothing$. It is easy to see that each equivalence class of $R^\sim$, where R is Church-Rosser and terminating, contains exactly one irreducible element. Let Σ be a finite set, called alphabet. The set of all finite strings over Σ (words) is denoted by Σ^*. The length of $a \in \Sigma^*$ is denoted by $|a|$, the empty word by Λ. Let $a, b \in \Sigma^*$. We say that a is a prefix of b if $b = au$ for some $u \in \Sigma^*$. Let $A \subseteq \Sigma^*$ and let $R \subseteq A \times A$ be a relation. A word is called *almost irreducible* (with respect to$R$) if each of its proper prefixes is irreducible with respect to R. R is called *thin* if it satisfies the following implication: if $\langle u, v\rangle \in R$ and u is almost irreducible, then v is almost irreducible, too.

II. UNARY ALGEBRAS

Take a signature σ containing names of unary operations, only. Each algebra $\mathscr{U} \rightleftharpoons \langle U; \sigma\rangle$ of type σ is called *unary algebra.* We shall consider signatures and sets U that are at most countable. Unary algebra will often be denoted by the same symbol as its basic set. $\Sigma \subseteq U$ is the set of generators of U if U is the smallest subalgebra of U containing Σ. Unary algebra $\mathscr{F}$ of type σ is *free* over the set Σ of free generators if for every unary algebra U of the same type and every map $\varphi : \Sigma \to U$ there is a homomorphism $\bar{\varphi} : \mathscr{F} \to \mathscr{U}$ with $\varphi(x) = \bar{\varphi}(x)$ for all $x \in \Sigma$. The cardinality of Σ is also called *rank* of $\mathscr{F}$. All free unary algebras of the same type σ and the same rank are isomorphic to a standard free unary algebra which will be described now. Take a set Σ disjoint with σ. F will be the set of all words over the alphabet $\Sigma \cup \sigma$, the first letter of which belongs to Σ and all the others to σ. Those words are called special. If $f \in \sigma$ and w is a special word, then the result of the operation f on w is the special word wf. The free unary algebras of type σ (card $\sigma = n$) with one generator will be denoted by $\mathscr{F}_n$. Unary algebra U of type σ is *presented by* $\langle F, R \rangle$ if F is a free unary algebra of type σ, $R \subseteqq F \times F$ and U is isomorphic to the factor-algebra $F/\mathscr{C}(R)$ where $\mathscr{C}(R)$ is the smallest congruence relation on F containing R. More explicitely, $\mathscr{C}(R)$ is $I_R^{\sim}$, where

$$I_R \rightleftharpoons \{\langle xu, yu \rangle \mid \langle x, y \rangle \in R, \quad u \text{ is a word over } \sigma\}$$

is the *immediate inference relation* associated with R. Note that for any almost irreducible with respect to I_R v, $\langle v, w \rangle \in I_R$ iff $\langle v, w \rangle \in R$. Indeed, by the definition of I_R, $\langle v, w \rangle \in I_R$ iff $v = xu$, $w = yu$ for some word u over σ and $\langle x, y \rangle \in R$. As v is almost irreducible, $\langle x, y \rangle \in R$ implies $x = v$, so u is the empty word and $w = y$. Note also that almost irreducibility with respect to I_R is equivalent to the almost irreducibility with respect to R.

This situation can be generalized. Suppose an arbitrary set $A \subseteqq \Sigma^*$ of words over alphabet Σ containing σ, with $A\sigma \subseteqq A$ and a relation $R \subseteqq A \times A$ are given. As before, we can take the smallest congruence on A containing R to obtain a unary algebra. We shall call it the unary algebra presented by $\langle A, R \rangle$ or—if it is clear which set A is taken—*presented by R*.

III. MONADIC SECOND ORDER THEORY OF A STRUCTURE

First, recall what is the monadic second order language $\mathscr{ML}(\tau)$ of a given signature τ containing predicate and function names and constants. This language has two sorts of variables—individual and set ones. Besides atomic formulas constructed in the first order language with equality in the standard way with the use of terms, there are atomic formulas of the form $t \in X$, where t is a term an X is a set variable. Further, formulas are constructed by the usual induction with the use of logical connectives and quantification over individual and set variables. Independently of τ we suppose that the language $\mathscr{ML}(\tau)$ always contains two logical constants F and T. If a structure $\mathscr{S}$ of type τ is given, then the set of all sentences of $\mathscr{ML}(\tau)$ which are true in $\mathscr{S}$ (set variables range over all subsets of $\mathscr{S}$) is called the *monadic theory* of $\mathscr{S}$ ($\mathscr{MTS}$). $\mathscr{MTS}$ is decidable if there is an algorithm to answer the following question: given a sentence of $\mathscr{ML}(\tau)$, is it true in $\mathscr{S}$ or not?

Consider the free unary algebra $\mathscr{F}_n$ and enlarge its signature by a binary predicate name $\preceq$. $x \preceq y$ is interpreted as "x is a prefix of y".

THEOREM (Rabin [2]): *The monadic theory of* $\langle F_n; \sigma, \preceq \rangle$ *is decidable.*

Further, we always consider free unary algebras together with $\preceq$. Let $R \subseteq F_n^N$ be an N-ary relation of F_n. ($N < \omega$). We say that R is definable in $\mathscr{M}\mathscr{T}\mathscr{F}_n$ if there exists a formula $\varphi_R(x_1, \ldots, x_N)$ of $\mathscr{M}\mathscr{L}\mathscr{F}_n$ such that $\varphi_R(a_1, \ldots, a_n)$ is true in F_n iff $\langle a_1, \ldots, a_n \rangle \in R$. Note that $\preceq$ is definable in $\mathscr{M}\mathscr{T}\mathscr{F}_n$ for all finite σ. This is not true for infinite σ. $A \subseteq F_n$ is *regular* iff it is definable (as unary relation) in $\mathscr{M}\mathscr{T}\mathscr{F}_n$. Another observation: operations on binary relations mentioned in part I preserve their definability. Indeed, let R, T be definable binary relations on F_n. Then $R \circ T$, R^{-1}, $R^{\sim}$ and R^* are definable, too. Let us give e. g. the formula defining R^*.

$$\Phi_{R^*}(x, y) \rightleftarrows x = y \vee \forall Z (x \in Z \ \& \ \forall z, z' (\langle z, z' \rangle \in R \ \& \ z \in Z \rightarrow z' \in Z) \rightarrow y \in Z).$$

IV. THE MAIN RESULT

An inference relation I_R on F_n which is Church-Rosser, terminating and thin is called *reduction* and it is denoted by $\underset{R}{\rightarrow}$. The reflexive and transitive closure of $\underset{R}{\rightarrow}$ is denoted by $\overset{*}{\underset{R}{\rightarrow}} b$. Note that in general, the definability of R does not imply that of I_R. Therefore, the definability of R is not sufficient to ensure the decidability of the monadic theory of the unary algebra presented by R. In case of definable relation R, the inference relation of which is a reduction, this difficulty can be escaped thanks to the porperty described in the following

LEMMA: *Let* $\underset{R}{\rightarrow}$ *be a reduction and let* $a, b \in F_n$ *be irreducible with respect to* $\underset{R}{\rightarrow}$. *Then for each* $f \in \sigma$, *there is* $af \overset{*}{\underset{R}{\rightarrow}} b$ *iff* $\langle af, b \rangle \in R^*$.

Proof: Let $af = u_0 \underset{R}{\rightarrow} u_1 \underset{R}{\rightarrow} \ldots \underset{R}{\rightarrow} u_m = b$. As af is almost irreducible and $\underset{R}{\rightarrow}$ is thin, then, by induction, u_i is almost irreducible for all $i = 1, \ldots, m$. But for almost irreducible words u_i, u_{i+1}, there is $u_i \underset{R}{\rightarrow} u_{i+1}$ iff $\langle u_i, u_{i+1} \rangle \in R$.

THEOREM: *Let Σ be an alphabet containing σ and let $A \subseteq \Sigma^*$ be closed under the operations from σ. Let R be a binary relation on A. If*

(i) *A is regular;*

(ii) *R is definable;*

(iii) *the inference relation I_R is a reduction, then the monadic theory of the unary algebra presented by $\langle A, R \rangle$ is decidable.*

Proof: First, it will be shown that the set Irr of all irreducible (with respect to $\underset{R}{\rightarrow}$) words of A is regular and, for each $f \in \sigma$, a formula of $\mathcal{MLF}_n$ will be given to define a unary operation on Irr. Then, it will be stated that such a unary algebra is isomorphic to $A/\mathscr{C}(R)$. As isomorphic algebras have identical theories, this is sufficient to prove the theorem.

Clearly, a belongs to the domain of R iff the formula $R\,\mathrm{Dom}\,(x) \rightleftharpoons \exists y\, R(x, y)$ is true in F_n for $x = a$. Further, a is an irreducible with respect to $\underset{R}{\rightarrow}$ word of A iff the formula

$$\mathrm{Irr}(x) \;\rightleftharpoons\; x \in A \;\&\; \forall y\, (y \preceq x \rightarrow \neg R\,\mathrm{Dom}(y))$$

is true in F_n for $x = a$. Let us take

$$\Phi_f(x, y) \;\rightleftharpoons\; \mathrm{Irr}(x) \;\&\; \mathrm{Irr}(y) \;\&\; R^*(xf, y).$$

For $\underset{R}{\rightarrow}$ is a reduction, Φ_f defines an operation on Irr. (Remember that the definability of R yields that of R^*). It remains to prove that the unary algebra Irr with operations defined by Φ_f, $f \in \sigma$, is isomorphic to $A/\mathscr{C}(R)$. By assumption, each congruence class of $A/\mathscr{C}(R)$ contains exactly one irreducible with respect to $\underset{R}{\rightarrow}$ element, hence there is a one-to-one correspondence between the elements of $A/\mathscr{C}(R)$ and those of Irr. Denote by $\bar{x} \in A/\mathscr{C}(R)$ the class containing x. Let $f \in \sigma$ and $a \in A$. Then $f(\bar{a}) = \overline{af}$. Suppose that a is irreducible. If af is also irreducible, then $\Phi_f(a, af)$ is trivially true in F_n. If af is not irreducible, then $af \overset{*}{\underset{R}{\rightarrow}} c$ for the unique irreducible c with $\bar{c} = \overline{af}$. By the previous lemma, $\langle af, c \rangle \in R^*$, hence $\Phi_f(a, c)$ is true in F_n. This proves that $A/\mathscr{C}(R)$ and Irr are isomorphic.

V. FINITELY PRESENTED UNARY ALGEBRAS

We shall give an example of relation with a Church-Rosser inference relation. First, we state that finitely presented unary algebras satisfy the condition of Theorem of section IV.

THEOREM 1: *Let A, Σ be as before, Σ finite and let $R \subseteq A \times A$ be a finite relation. Then there is a finite relation $Q \subseteq A \times A$ with*

(i) $\mathscr{C}(Q) = \mathscr{C}(R)$;

(ii) I_Q *is a reduction.*

Proof: Let m be the maximal length of all words in $R\,\mathrm{Dom} \cup R\,\mathrm{Im}$, $R\,\mathrm{Im}$ being the image of R. Suppose there is a linear ordering $\leqq$ on A such that $|a| < |b|$ implies $a \leqq b$. In each $\mathscr{C}(R)$-equivalence class choose a minimal (with respect to $\leqq$) element. Define Q as the set of all pairs $\langle \alpha, \beta \rangle \in \mathscr{C}(R)$, $\alpha \neq \beta$ and such that $|\alpha| \leqq m$ and β is the minimal element of its $\mathscr{C}(R)$-class. It is clear that $R \subseteq Q^{\sim} \subseteq \mathscr{C}(R)$, hence $\mathscr{C}(Q) = \mathscr{C}(R)$. If $\langle \alpha, \beta \rangle \in Q$ then, by definition, β is irreducible with respect to I_Q and $|\beta| \leqq |\alpha|$. Hence, the chain $\alpha u = v_0, \ldots$ with $\langle v_i, v_{i+1} \rangle \in I_Q$ for all $i = 0, 1, \ldots$ cannot have more than $|u| + 1$ members. Therefore, I_Q is terminating.

Now we shall prove the Church-Rosser property of I_Q, i. e. we shall prove that $I_Q^{\sim} \subseteq I_Q^* \circ (I_Q^{-1})^*$. Take $\langle a, b \rangle \in I_Q^{\sim}$ $(a \neq b)$. Then there is a chain $x_0, \ldots, x_k$ of elements of A with $a = x_0$, $b = x_k$ and for each $i = 0, \ldots, k-1$, $\langle x_i, x_{i+1} \rangle \in I_Q \cup I_Q^{-1}$.

(*a*) If $\langle x_i, x_{i+1} \rangle \in I_Q (\langle x_i, x_{i+1} \rangle \in I_Q^{-1})$ for each $i = 0, \ldots, k-1$, then $\langle a, b \rangle \in I_Q^*$ ($\langle a, b \rangle \in (I_Q^{-1})^*$ resp.) and there is nothing more to prove.

(*b*) Let for no i, $1 \leqq i \leqq k-1$, there be

$$\langle x_{i-1}, x_i \rangle \in I_Q^{-1} \ \& \ \langle x_i, x_{i+1} \rangle \in I_Q.$$

This means that either $\langle a, b \rangle \in I_Q^*$ or $\langle a, b \rangle \in (I_Q^{-1})^*$ or there is a unique $j = 1, \ldots, k-1$ with $\langle x_{j-1}, x_j \rangle \in I_Q$ and $\langle x_j, x_{j+1} \rangle \in I_Q^{-1}$, i. e. $\langle a, b \rangle \in I_Q^* \circ (I_Q^{-1})^*$.

(*c*) So, let $\langle x_{i-1}, x_i \rangle \in I_Q^{-1}$ and $\langle x_i, x_{i+1} \rangle \in I_Q$ for some $i = 1, \ldots, k-1$. We shall prove that in this situation, there is a shorter chain $a = y_0, \ldots, y_{k-1} = b$ with $\langle y_j, y_{j+1} \rangle \in I_Q \cup I_Q^{-1}$ for all $j = 0, \ldots, k-2$. Then, having proved that, we get in a finite number of steps a chain $a = z_0, \ldots, z_r = b$ with $1 \leqq r < k$ and such that there is no $j = 1, \ldots, r-1$ with $\langle z_{j-1}, z_j \rangle \in I_Q^{-1}$ & $\langle z_j, z_{j+1} \rangle \in I_Q$. This leads us to the situation described in (*b*) which proves the Church-Rosser property of I_Q.

[*Example:* Denote I_Q by $\rightarrow$ and I_Q^{-1} by $\leftarrow$. Let

$$a = x_0 \rightarrow x_1 \rightarrow x_2 \leftarrow x_3 \rightarrow x_4 = b.$$

We suppose that $x_2 \leftarrow x_3 \rightarrow x_4$ can be replaced by $x_2 \leftarrow x_4$ or by $x_2 \rightarrow x_4$. Hence, there is either $a = x_0 \rightarrow x_1 \rightarrow x_2 \leftarrow x_4 = b$, i.e. $\langle a, b \rangle \in I_Q^* \circ (I_Q^{-1})^*$ or $a = x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow x_4 = b$, i.e. $\langle a, b \rangle \in I_Q^* \subseteq I_Q^* \circ (I_Q^{-1})^*$.]

It remaine to prove that, for all $x, y, z \in A$, $\langle x, y \rangle \in I_Q$ & $\langle x, z \rangle \in I_Q$ implies $\langle y, z \rangle \in I_Q \cup I_Q^{-1}$ or $y = z$.

CLAIM: Let α' be a prefix of α, $\alpha = \alpha' u$ and let both $\langle \alpha, \beta \rangle$ and $\langle \alpha', \beta' \rangle$ belong to Q for some $\beta, \beta' \in A$. Then $\beta' u = \beta$ or $\langle \beta' u, \beta \rangle \in Q$.

Indeed, since $\langle \alpha' u, \beta \rangle \in \mathscr{C}(R)$ and $\langle \alpha' u, \beta' u \rangle \in \mathscr{C}(R)$ we have $\langle \beta' u, \beta \rangle \in \mathscr{C}(R)$, by the transitivity. Further, $\langle \alpha', \beta' \rangle \in Q$ yields $|\beta' u| \leqq |\alpha' u| \leqq m$, and $\langle \alpha, \beta \rangle \in Q$ yields that β is the minimal element of its $\mathscr{C}(R)$-class. Hence, by the definition of Q, $\langle \beta' u, \beta \rangle \in Q$ or $\beta' u = \beta$.

Now, let $\langle x, y \rangle, \langle x, z \rangle \in I_Q$. This means that for some prefixes α, α' of x and some prefixes β, β' of y, z respectively, there is $\langle \alpha, \beta \rangle \in Q$ and $\langle \alpha', \beta' \rangle \in Q$. Suppose first that $\alpha = \alpha' u$ for some subword u of x. Then there is a postfix t of x such that

$$x = \alpha t = \alpha' u t, \qquad y = \beta t, \qquad z = \beta' u t.$$

By the claim, either $\beta' u = \beta$ or $\langle \beta' u, \beta \rangle \in Q$. In both cases, $\langle z, y \rangle \in I_Q$ or $z = y$. If, to the contrary, $\alpha' = \alpha v$ for some subword v of x then, by the claim, $\beta v = \beta'$ or $\langle \beta v, \beta' \rangle \in Q$. Hence $\langle y, z \rangle \in I_Q$ or $z = y$. This proves the Church-Rosser property of I_Q.

To complet the proof, note that for an almost irreducible with respect to Q a there is $\langle a, b \rangle \in I_Q$ iff $\langle a, b \rangle \in Q$ and $Q\,\mathrm{Im} \subseteq \mathrm{Irr}$, hence I_Q is thin.

COROLLARY: *Let* Σ *be finite,* $\sigma \subseteq \Sigma$ *and let* $A \subseteq \Sigma^*$ *be regular. If* $R \subseteq A \times A$ *is finite, then the unary algebra presented by* $\langle A, R \rangle$ *has a decidable monadic theory.*

REFERENCES

1. R. W. BOOK, *The Power of the Church-Rosser Property in String Rewriting Systems,* Proc. 6th Conf. on Automated Deduction, L.N.C.S., vol. 85, Springer-Verlag, 1982, pp. 360-368.
2. M. O. RABIN, *Decidability of Second-Order Theories and Automata on Infinite Trees,* T.A.M.S., 141, 1969.
3. M. JANTZEN, *Thue Systems and the Church-Rosser Property,* M.F.C.S.'84, L.N.C.S., Vol. 175, pp. 80-95.