Direttore Responsabile: Ruggero Ferro
Iscrizione al Registro Stampa del Tribunale di Padova n. 1235 del 26.9.1990

Pubblicato con il contributo di:
Cassa di Risparmio di Padova e Rovigo

Stampa: Rotografica Padova

Decidability results for term algebras

Gabriele Marongiu *
Università di Bologna
Dipartimento di Matematica
P.zza di Porta S. Donato 5
I-40127 BOLOGNA

Sauro Tulipani *
Università di Camerino
Dipartimento di Matematica e Fisica
via Madonna delle Carceri
I-62032 CAMERINO†

INTRODUCTION

The main aim of this first paper is to give the necessary background for the second paper, henceforth denoted [II]. In section 3 we also give a self-contained proof of new undecidability results for certain term algebras.

Unless otherwise specified, all references are listed at the end of [II].

Algebraic calculus is the first example of a situation that is now frequent in computer science. Linguistic items become the data on which calculations take place. Syntactical structures in which the objects are terms originate in Herbrand's work and play a central role in mathematical logic. Such structures have become the principal support of information in the last generation of programming languages. Terms play the double role of linguistic elements and of objects to make computations. When this second feature is emphasized, terms are described as finite trees. The operations of unification and matching, the rewriting calculus oriented by strategies require the solution of certain first-order formulas in the algebra of finite trees. Infinite trees were introduced and studied by the French school in the late seventies to provide algebraic semantics of programming languages. The symbolic execution of flowchart schemes and of recursive program schemes gives rise, in a natural way, to rational and infinite trees respectively (see [Co85]). Furthermore, rational trees provide the right algebraic framework for the study of unifica-

*The authors thanks MURST for partial support.
†E-mail: tulipani@camvax.cineca.it .

tion without occur check. Then we may say that the investigation of term algebras has been fruitful for the analysis of programs.

Finite trees are essentially absolutely free algebras. The first-order theory of such algebras, which we shall denote by $\mathcal{T}_{FT}$, was axiomatized and investigated by Mal'cev [Mal61] who proved the decidability of $\mathcal{T}_{FT}$ by carrying out an analysis of its models. Mal'cev's axioms were used by Clark [Cl78] in order to assign to the negation as failure rule, shortly NAF, a declarative model theoretic meaning. Later Fitting [Fi85], Kunen [Ku87] and Colmerauer [Col84] have used the theory $\mathcal{T}_{FT}$ to provide semantics of the NAF rule and of rules which return computed answers more general than variable substitutions.

Recently, Maher [Mah88] has investigated a theory for infinite and and rational trees.[1]

Such theory that we denote by $\mathcal{T}_{IT}$ has properties analogous to the theory $\mathcal{T}_{FT}$. Maher [Mah88] proves the decidability of the theory of infinite and rational trees in a signature with at least two symbols. Marongiu and Tulipani [MT89] complete Maher's results for every signature and give a description of the complete exstensions of the theory $\mathcal{T}_{IT}$. Such a description, analogous to Mal'cev's for $\mathcal{T}_{FT}$, is made possible by the introduction of special expressions, called terms with pointers, that can be interpreted in every model of $\mathcal{T}_{IT}$.

The decidability of first-order sentences by transformation to a canonical form has been studied by Comon-Lescanne [CL89] both for finite and infinite terms. Model theoretic results concerning stability have been given for the theory $\mathcal{T}_{FT}$ by Bouscaren-Poizat[2] and Belegradek[3], for the theory $\mathcal{T}_{IT}$ by Toffalori[4].

The first-order theories obtained by $\mathcal{T}_{FT}$ and $\mathcal{T}_{IT}$ by adjoining the subterm relation are both undecidable provided the signature has operations of arity greater than 1. This was observed for finite terms by McCarthy [McC77].

[1]The axioms were firstly given in J. Jaffar, J.L. Lassez and M.J. Maher, *Prolog II as an Instance of the Logic Programming Language Scheme*, in: "Formal Descriptions of Programming Concepts III", M. Wirsing (ed.), North-Holland 1987, pp. 275-299.

[2]E. Bouscaren and B. Poizat, *Des Belles Paires aux Beaux Uples*, J. Symb. Logic 53 (2) (1988), pp. 434-442.

[3]O.V. Belegradek, *Theory of Models of Locally free Algebras*, Trudy Instituta, Matematiki Sibirskogo Otdelenija Akademii Nauk SSSP 8 (1988), pp. 3-25.

[4]C. Toffalori *Model theoretic questions for infinite terms*,submitted to Boll. UMI (1991).

Later, Venkataraman [Ven87] proves the decidability of the existential theory of finite terms with subterm relation in every signature and proved, on the other hand, that in certain signatures the $\exists\forall_{\leq}$ fragment is undecidable. We denote by $\exists\forall_{\leq}$ the fragment of sentences in prenex form with a prefix of existential quantifiers followed by universal quantifiers bounded by the predicate $\leq$. Treinen [Tre90] has extended the undecidability results to any algebra of terms. On the other hand, Tulipani [II] proves that in any finite signature the existential fragments of rational and infinite trees with subterm relation coincide and are a decidable theory.

In first section of this paper we briefly review the results of Mal'cev [Mal71], Maher [Mah88] and Marongiu-Tulipani [MT89]. In particular we present the formalism and the main facts about terms with pointers. In second section, we consider the theories of finite, rational and infinite terms with the subterm relation with a short introduction to the decidability results of Venkataraman [Ven87] and Tulipani [II]. In third section, we give undecidability results by a method which proves that the structure of natural numbers is definable into any algebra of terms with subterm relation using $\exists\forall_{\leq}$ formulas. Then, we may apply Matijasevič's theorem to get undecidability results for every term algebra with subterm relation in any signature with some constant and at least a symbol of arity greater than 1. Using this technique we also prove a novel result which states that, in presence of the subterm relation and in signatures with symbols of arity greater than 1, the Σ_1 theory of rational trees and the Σ_1 theory of infinite trees are quite different. In fact, the first is r.e. and the second has degree not less than Σ_1^1 in the analytical hierarchy. Here, in analogy with the arithmetical hierarchy, we call Δ_0 the prenex formulas, whose quantifiers are bounded by the predicate $\leq$, and we call Σ_1 the formulas which are existential quantification of Δ_0 formulas.

1 Decidability for finite and infinite terms

1.1 Fundamental notions

In order to make this paper self-contained we repeat here, almost verbatim, part of the content of section 1 of [II].

Let S be an algebraic signature. The rank of a function symbol $f \in S$ is called the *arity* of f. We assume that the set S_0 of constant symbols is non empty and, unless otherwise stated, that S is finite. We often assume that S contains a symbol of arity greater than 1. Let us now describe the structures we are interested in.

Let N_+^* be the free monoid of words on the alphabet of positive integers N_+; ε denotes the empty word. If $p, q \in N_+^*$ then $|p|$ is the length of p, $p \preceq q$ means that p is an initial segment of q, $p \prec q$ if $p \preceq q$ and $p \neq q$ and $p.q$ is the concatenation of p with q. A non empty $D \subseteq N_+^*$ is a *tree domain* if it is closed under initial segments and if $i.p \in D$, for $i \in N_+$ then $j.p \in D$ for every $j \leq i$. A function $t : D \to S$ is called a *term* (or a tree in the signature S) if for every $p \in D$, $t(p) = s$ iff the arity of s is equal to the number of successors of p in D. We denote by IT the set of all terms in our fixed signature S. Any element $p \in D$ is called an *occurrence*, or position in t; the domain D of the function t will be denoted by $\mathrm{Occ}(t)$.

Let V be any set of new elements such that $V \cap IT = \emptyset$. We define $IT[V]$ as before by adding the set V to the signature, where any element of V is considered of arity 0. The elements of V are called *variables* or *indeterminates*. So we have that $IT = IT[\emptyset]$.

Assume $s, t \in IT[V]$. Then s is *a subterm of* t, denoted $s \leq t$, if there is some $p \in \mathrm{Occ}(t)$ such that $\mathrm{Occ}(s) = \{q : p.q \in \mathrm{Occ}(t)\}$ and $s(q) = t(p.q)$ for every $q \in \mathrm{Occ}(s)$. The term s is denoted by t/p. The set $IT[V]$ is an algebraic structure of signature S with respect to the syntactical operations of term formation that can be described in the following way. The interpretation of any n-ary f in $IT[V]$ is such that: $f(t_1, \ldots, t_n) = t$ iff $\mathrm{Occ}(t) = \{\varepsilon, i.p : p \in \mathrm{Occ}(t_i)$ for some $1 \leq i \leq n\}$ and $t(\varepsilon) = f$, $t/i = t_i$ for every $1 \leq i \leq n$. $FT[V]$ is the substructure of all *finite terms*, i.e. the terms of $IT[V]$ whose domain is finite; FT denotes $FT[\emptyset]$ and is a substructure of IT. We denote by $RT[V]$ the substructure of $IT[V]$ of terms having a finite number of subterms; the elements of $RT[V]$ are called *rational terms* and RT will denote $RT[\emptyset]$.

When the elements of $FT[V]$ play the role of syntactical expressions of a

first-order language, we think of them as words in a certain alphabet defined in the usual inductive way.

We denote by $\mathcal{L}$ the first-order language in signature S whose only predicate symbol is identity.

We consider now first-order theories in the language $\mathcal{L}$ whose models are structures of terms.

1.2 Theories of finite and infinite terms

Let $\mathcal{T}_{FT}$ be the first-order theory in language $\mathcal{L}$ whose non logical axioms are the universal closure of the following sets of formulas

$$(F1) \qquad f(v_1, \ldots, v_{n_f}) \neq g(w_1, \ldots, w_{n_g})$$

for f, g distinct function symbols in S of arity n_f, n_g, respectively;

$$(F2) \qquad f(v_1, \ldots, v_{n_f}) = f(w_1, \ldots, w_{n_f}) \to v_1 = w_1 \wedge \cdots v_{n_f} = w_{n_f}$$

for f function symbol of arity n_f;

$$(F3) \qquad t \neq v$$

for t term which contains the variable v and is different from v.

The axiom $(F3)$, which is a schema, in the computer science terminology is named Occur-check Axiom.

It is immediate to verify that for any set X of indeterminates, $FT[X]$ is a model of $\mathcal{T}_{FT}$. On the other hand, the structures $RT[X]$, $IT[X]$ satisfy axioms $(F1)$, $(F2)$ but do not schema $(F3)$. In fact, it is a characteristic property of these structures that of having elements which are solution of an equation $v = f(v, v)$ in the unknown v, or of a system $\{v_1 = f(v_1, v_2), v_2 = g(v_1, v_2, v_1)\}$ in the unknowns v_1, v_2. More precisely, let us consider a system of equations

$$D = \begin{cases} v_1 = t_1(\vec{v}, \vec{w}) \\ \vdots \\ v_n = t_n(\vec{v}, \vec{w}) \end{cases}$$

to be read as follows. We denote by $\vec{v}$ the sequence of distinct variables $v_1, \ldots, v_n$; by $\vec{w}$ a sequence of variables distinct from the variables $\vec{v}$ and by

$t_i(\vec{v},\vec{w})$ a term (finite!) whose variables are among the variables $\vec{v}$, $\vec{w}$. A system is said to be in *rational solved form* if it does not contain a *circular* set of equations, that is to say a set of equations of the form $v_{i_1} = v_{i_2}, \ldots, v_{i_{k-1}} = v_{i_k}, v_{i_k} = v_{i_1}$. Consider now the axioms ([Mah88] [Com90])

$$(F3') \qquad \forall \vec{w} \exists ! \vec{v} \bigwedge D$$

for every system D in rational solved form. We denote by $\mathcal{T}_{IT}$ the theory in the language $\mathcal{L}$ whose non logical axioms are $(F1)$, $(F2)$ and $(F3')$. We can easily see that for any set of indeterminates X, the structures $RT[X]$ e $IT[X]$ are models of $\mathcal{T}_{IT}$.

In each of the structures $FT[X]$, $RT[X]$, $IT[X]$, the elements of X can be characterized as the elements which satisfy the first-order formula $\mathrm{Ind}(v)$ defined as follows

$$\mathrm{Ind}(v) := \bigwedge_{f \in S} \neg \exists \vec{z} \left(v = f(z_1, \ldots, z_{n_f}) \right)$$

where $\vec{z}$ is a sequence of m variables with m the maximum arity of functions in S, and n_f is the arity of f. An element in a model of $\mathcal{T}_{FT}$ or $\mathcal{T}_{IT}$ wich satisfies the formula $\mathrm{Ind}(v)$, is called *indecomposable*, so every indeterminate in X is an indecomposable element of $FT[X]$, $RT[X]$, and $IT[X]$. Define now

$$\begin{array}{lll} IND^n & = \{\exists !^n \, v \, \mathrm{Ind}(v)\} & \text{for } n \in \omega \\ IND^\omega & = \{\exists^{\geq k} v \, \mathrm{Ind}(v) \quad \text{for every } k \in \omega\} & \end{array}$$

where $\exists !^n$ and $\exists^{\geq k}$ are to be interpreted as "There exist exactly n" and "There exist at least k" respectively. If $\nu \in \omega + 1$ the theories $\mathcal{T}_{FT}^\nu$, $\mathcal{T}_{IT}^\nu$ are defined as follows

$$\begin{array}{ll} \mathcal{T}_{FT}^\nu & = \mathcal{T}_{FT} + IND^\nu \\ \mathcal{T}_{IT}^\nu & = \mathcal{T}_{IT} + IND^\nu. \end{array}$$

It is now immediate to verify that:

$FT[X]$ is a model of $\mathcal{T}_{FT}^n$ iff $|X| = n$,

$RT[X]$ and $IT[X]$ are models of $\mathcal{T}_{IT}^n$ iff $|X| = n$,

$FT[X]$ is a model of $\mathcal{T}_{FT}^\omega$ iff X is infinite,

$RT[X]$ and $IT[X]$ are models of $\mathcal{T}_{IT}^\omega$ iff X is infinite.

The axiom $\neg \exists v \mathrm{Ind}(v)$, needed to form $\mathcal{T}_{FT}^0$, $\mathcal{T}_{IT}^0$ from $\mathcal{T}_{FT}$, $\mathcal{T}_{IT}$ respectively, in logic programming is called Domain Closure Axiom, shortly DCA. The theories $\mathcal{T}_{FT}^\nu$ were introduced and studied by Mal'cev [Mal61] [Mal71] whose results can be resumed in the following theorem.

Theorem 1.1 (Mal'cev 1962 [Mal71]) *Let S be a finite signature. Then the models of $\mathcal{T}_{FT}$ are exactly the locally free algebras. The theories $\mathcal{T}_{FT}^\nu$ for $\nu \in \omega + 1$ are all the complete extensions of the theory $\mathcal{T}_{FT}$. Hence the theory $\mathcal{T}_{FT}$ is decidable.*

Completely analogous results, proved in [Mah88] and [MT89], hold for the theories $\mathcal{T}_{IT}^\nu$. In particular we have:

Theorem 1.2 (Maher 1988 [Mah88]) *Let S be a finite signature with at least two elements. Then $\mathcal{T}_{IT}^0$ is complete. If S is infinite $\mathcal{T}_{IT}$ is complete. Hence the structures RT and IT are elementarily equivalent.*

From Maher's results it is almost immediate to derive that the structures $RT[X]$ and $IT[X]$ are elementarily equivalent for any set X of indeterminates.

Theorem 1.3 (Marongiu-Tulipani 1989 [MT89]) *Let S be any finite signature. Then every sentence in $\mathcal{L}$ is effectively equivalent modulo $\mathcal{T}_{IT}$ to a Boolean combination of sentences $\exists^{\geq k} v \, \mathrm{Ind}(v)$. Hence $\mathcal{T}_{IT}$ is decidable and the theories $\mathcal{T}_{IT}^\nu$ for $\nu \in \omega + 1$ are all its complete extensions.*

1.3 Quantifier elimination

We now discuss the quantifier elimination techniques used for the proofs of the above results. The key idea is that every sentence of theory $\mathcal{T}$ is provably equivalent in $\mathcal{T}$ to a Boolean combination of formulas that can be algorithmically handled in $\mathcal{T}$.

1.3.1

Mal'cev proves that every sentence of $\mathcal{L}$ is equivalent modulo $\mathcal{T}_{FT}$ to a Boolean combination of sentences of the form $\exists^{\geq k} v \mathrm{Ind}(v)$; from this all the results for the the theories $\mathcal{T}_{FT}^\nu$ with $\nu \in \omega + 1$ are deduced.

1.3.2

Kunen [Ku87] considers the theory $\mathcal{T}_{FT}$ in infinite signature and proceeds as follows. Let Inv$S$ be the collection of all unary function symbols inv_f^i for each function symbol f in S of positive arity n_f and each i, $1 \le i \le n_f$; let S^+ be the new signature $S \cup \mathrm{Inv}S$. $\mathcal{T}_{FT}^+$ is the theory in signature S^+ obtained by adding to $\mathcal{T}_{FT}$ the axioms which are the universal closure of the following formulas, for every function symbol f of S and every i, $1 \le i \le n_f$.

(INV1) $$f(v_1, \ldots, v_{n_f}) = w \rightarrow \mathrm{inv}_f^i(w) = v_i$$

(INV2) $$\neg\exists\vec{v}(f(v) = w) \rightarrow \mathrm{inv}_f^i(w) = w$$

Then, the following results are obtained.

Theorem 1.4 (Kunen 1987 [Ku87]) *Every formula of $\mathcal{T}_{FT}^+$ is equivalent modulo $\mathcal{T}_{FT}^+$ to an open formula. Owing to the fact that every open sentence can be evaluated in $\mathcal{T}_{FT}^+$ which is a conservative extension of $\mathcal{T}_{FT}$, the completeness and decidability of $\mathcal{T}_{FT}$ follow.*

1.3.3

Here is the method used by Maher [Mah88].

- He proves that every sentence of the theory $\mathcal{T}_{IT}$ is equivalent to a Boolean combination of *basic formulas* which express the fact that certain systems of equations have a solution.
- Then he proves that:
  (i) if signature S is infinite, any basic formula can be evaluated in $\mathcal{T}_{IT}$; the completeness of $\mathcal{T}_{IT}$ follows;
  (ii) if signature is finite and contains at least two function symbols, any basic formula can be evaluated in $\mathcal{T}_{IT}^0$; so, the completeness of $\mathcal{T}_{IT}^0$ is obtained.

This method can also be applied to the finite case to get analogous results for the theories $\mathcal{T}_{FT}$ and $\mathcal{T}_{FT}^0$.

1.3.4

In [MT89] an alternative approach to quantifier elimination for infinite terms is proposed. The main tool used consists of new syntactical expressions called *terms with pointers* that we want now briefly describe (for further details, see [II]).

1.4 Terms with pointers

Consider the algebra of finite terms $FT[V \cup N_+]$ in signature S where N_+ is the set of positive integers. We may suppose the sets S, V, N_+ to be pairwise disjoint. Then, the set $R[V]$ of terms with pointers is

$$R[V] = \{t : t \in FT[V \cup\ N_+] \text{ and } t(p) \in N_+ \text{ implies } t(p) \le |p|\ \}$$

So, the terms $f(1, v)$ e $f(f(2, v), 1)$ are terms with pointers, but $f(2, v)$ is not because the natural number 2 is in the occurrence $p = 1$ and $|p| = 1$. Any term with pointers can be thought of as an expression which represents a rational term. The terms with pointers $f(1, w)$ and $f(f(2, w), 1)$ represent the rational terms that are solutions of the equations $v = f(v, w)$ and $v = f(f(v, w), v)$ respectively, for the unknown v with parameter w. It is possible to define a function
$$e_V : R[V] \rightarrow RT[V]$$
which maps any term with pointers t into the rational term $\hat{t}$ represented by t. Given a term with pointers t and $p \in Occ(t)$ it may happen that t/p, which is an element of $FT[V \cup N_+]$, is not an element of $R[V]$; however, it is possible to define and calculate a term with pointers $t/\!/p$ which satisfies the condition
$$e_V(t/\!/p) = \hat{t}/p$$
and so represents a subterm of the rational term represented by t. We can verify that every subterm of $\hat{t}$ is represented by some term with pointers in the set $\{t/\!/p : p \in Occ(t)\}$.

We can now briefly describe the quantifier elimination method for infinite terms proposed in [MT89]. The language $\mathcal{L}$ is extended in two ways. On the one hand, terms with pointers are used in the role of first-order terms. This makes sense owing to the two facts:

(i) it is possible to define what means that an equation or a formula which contains terms with pointers is satisfied in a model of $\mathcal{T}_{IT}$ (see [II] Proposition1.1);

(ii) the syntactical transformations, which usually are applied to sets of firs-order equations, can also be applied to sets of equations with pointers (see [II] Lemma3.1).

On the other hand, signature S is expanded to $S^+ = S \cup \mathrm{Inv}S$, in analogy to Kunen's approach, and the theory $\mathcal{S}^0_{IT}$, obtained from $\mathcal{T}^0_{IT}$ by adding axioms (INV1) and (INV2), is considered. Moreover terms with pointers in signature $S \cup \mathrm{Inv}S$ are included.

At this point it is possible to define what means that a sentence with pointers in signature S^+ is a theorem of the theory $\mathcal{S}^0_{IT}$. Then, the following result is obtained.

Theorem 1.5 *Any sentence with pointers in signature S^+ is effectively equivalent in $\mathcal{S}^0_{IT}$ to an open sentence with pointers in signature S.*

An open sentence with pointers can now be evaluated by elementarization procedure (see [II] Lemma 3.1).

The completeness of $\mathcal{T}^0_{IT}$ is now deduced and from this also the completeness of $\mathcal{T}^\nu_{IT}$ for $\nu \in \omega$ easily follows. An analogous argument gives the same result for the theory $\mathcal{T}^\omega_{IT}$.

2 Decidability of theories with subterm relation

We consider now the structures $(FT[X], \leq)$, $(RT[X], \leq)$ and $(IT[X], \leq)$ obtained by expanding the algebraic structures of terms by the binary subterm relation $\leq$. This relation is a partial order on $FT[X]$ and a preorder on the structures of infinite terms $RT[X]$ and $IT[X]$. Denote by $\mathcal{L}_\leq$ the language obtained by adding to $\mathcal{L}$ a new binary relation symbol which we still denote $\leq$. As we shall see in section 3, the structures of terms with subterm relation are undecidable. Nevertheless, for some applications, the existential fragments of these theories deserve attention.

2.1 Existential theories

We denote by E the set of existential first-order sentences in the language $\mathcal{L}_\leq$ and by $Th_E(FT[X], \leq)$, $Th_E(RT[X], \leq)$ and $Th_E(IT[X], \leq)$, the sets of sentences in E which are true in the indicated structures. Concerning such theories the following results hold.

Theorem 2.6 ([Ven87]) *The theory $Th_E(FT[X], \leq)$ is decidable.*

Theorem 2.7 ([II]) *Let $X = \{x_1, \ldots\}$ be a non empty set of indeterminates. Then,*

$$Th_E(RT[x_1], \leq) = Th_E(RT[X], \leq) = Th_E(IT[X], \leq).$$

Moreover this set of sentences is decidable. If the signature has more than one element of positive arity, then

$$Th_E(RT[x_1], \leq) = Th_E(RT, \leq) = Th_E(IT, \leq).$$

When the signature has only one element of positive arity we have

$$Th_E(RT[x_1], \leq) \neq Th_E(RT, \leq) = Th_E(IT, \leq).$$

These results are obtained by studying the solvability of certain systems of atomic formulas with pointers. We refer the interested reader to [II] where signature is supposed to have at least a symbol of arity greater than 1; the case of a signature whose symbols are all of arity ≤ 1 is much simpler.

2.2 Axiomatizations of subterm relation

Consider now the following axioms in the language $\mathcal{L}_\leq$.

(O1) Reflexive and transitive property for $\leq$

(O2) Antisymmetric property for $\leq$

(O3) $\forall v \forall v_1 \ldots \forall v_n \left(v \leq f(v_1, \ldots, v_n) \leftrightarrow (v = f(v_1, \ldots, v_n) \vee \bigvee_{1 \leq i \leq n} v \leq v_i)\right)$

for all $f \in S$; if the arity n is 0, then $\bigvee_{1 \leq i \leq n}(v \leq v_i)$ disappears.

(O4) $\forall\vec{v}\forall z\Big(z \leq t \quad \leftrightarrow \quad (\bigvee_{p\in Occ(t)} z = t/\!/p \quad \vee \quad \bigvee_{v\in var(t)} z \leq v\Big)$

where t ranges on $R[V]$, V is countably infinite , and $\vec{v}$ is a list of the variables in $var(t)$.

Then, we define the theories in the language $\mathcal{L}_{\leq}$

$\mathcal{O}_{IT}$ with axioms $\mathcal{T}_{IT}$, (O1), (O4) ;

$\mathcal{O}_{FT}$ with axioms $\mathcal{T}_{FT}$, (O1), (O2), (O3) .

Observe that axioms (O4) are stated using terms with pointers. However, it is possible (see [II] Definition2.1) to transform axioms (O4) in first-order sentences of $\mathcal{L}_{\leq}$. Now, we have that, for any set X of indeterminates,

$IT[X]$ and $RT[X]$ are models of $\mathcal{O}_{IT}$, while

$FT[X]$ is model of $\mathcal{O}_{FT}$.

The theories $\mathcal{O}_{IT}$ and $\mathcal{O}_{FT}$ prove that the transformations and the procedures used to decide the existential theories of $RT[X]$ and $FT[X]$, respectively are correct (see sections 3–6–7 of [II]).

3 Undecidability

It was observed by McCarthy [McC77] that the theory $Th(FT[X], \leq)$ is undecidable if signature S contains symbols of arity greater than 1. The same holds for the theories $Th(RT[X], \leq)$ and $Th(IT[X], \leq)$. Venkataraman [Ven87] has proved, for some signature, the undecidability of the fragment $\exists\forall_{\leq}$ of $Th(FT, \leq)$. The method he used consists in codifying Post's problem on strings into the named fragment. Treinen [Tre90] generalized Venkataraman's method and succeeded in proving that the $\exists\forall$ fragment of rational and infinite trees as well as various other fragments of other algebraic structures are undecidable.

We assume our signature contains at least a constant symbol that we denote Λ and a symbol of arity greater than 1 that we denote f. We assume f binary to simplify notation, but we can get the same results, in case of arity greater than 2, by using the binary term $f(u, v, \ldots, v)$. We shall show

that the structure of natural numbers is definable into any algebra of terms $(FT[X], \leq)$, $(RT[X], \leq)$, $(IT[X], \leq)$ by means of $\exists\forall_{\leq}$ formulas. In this way we can extend the well known undecidability results to any signature containing at least a constant and a function symbol of arity greater than 1; moreover we can establish that the theories $Th(RT, \leq)$, $Th(IT, \leq)$ are quite different, as already stated in introduction (see Propositions 3.11 e 3.12).

3.1 Interpretations

In analogy with arithmetical hierarchy we say that a formula α of $\mathcal{L}_{\leq}$ is Δ_0 if every quantifier which occurs in α is bounded by the symbol $\leq$. A formula α of $\mathcal{L}_{\leq}$ is a Σ_1 formula if it is an existential quantification of a Δ_0 formula. A $\forall_{\leq}$ formula is a formula logically equivalent to a prenex formula with universal quantifiers bounded by $\leq$. Finally we shall denote by $\exists\forall_{\leq}$ the subset of Σ_1 of the formulas which are existential quantifications of formulas in $\forall_{\leq}$.

Let us consider the following $\forall_{\leq}$ formulas in the language $\mathcal{L}_{\leq}$. Denote by m the maximum arity of operations in signature S, by n_g the arity of the generic operation g and by S' the set $S \setminus \{\Lambda, f\}$. We stipulate, as usual, that the conjunction of the empty set of formulas is **true** or, alternatively, $\Lambda = \Lambda$.

$$\begin{aligned}
nat_0(v) &:= (\forall y \leq v)(\forall x_1, \ldots, x_m \leq v)\Big(\bigwedge_{g\in S'}(y \neq g(x_1, \ldots, x_{n_g}))\wedge \\
&\quad \wedge(y = f(x_1, x_2) \rightarrow x_1 = \Lambda) \wedge (v \neq \Lambda)\Big) \\
nat(v) &:= nat_0(v) \wedge f(\Lambda, v) \neq v \\
funct(h) &:= (\forall x_1, x_2, x_3, y_1, y_2, y_3 \leq h)\Big(\big(\bigwedge_{1\leq i\leq 3}(x_i = f(\Lambda, y_i)) \\
&\quad \wedge f(x_1, x_2) \leq h \wedge f(x_1, x_3) \leq h\big) \rightarrow x_2 = x_3\Big)
\end{aligned}$$

To increase readability, in what follows we shall denote the term $f(\Lambda, x)$ by $succ(x)$. For any natural number $n \in N$ we denote by $\underline{n}$ its codification in FT defined inductively by

$$\underline{0} = f(\Lambda, \Lambda), \qquad \underline{n+1} = succ(\underline{n}).$$

Denote by NAT the set $\{\underline{n} : n \in N\}$; it will play the role of the natural numbers. Observe also that the subterm relation on NAT codifies the usual order relation on natural numbers.

Then, the following proposition can be easily proved.

Proposition 3.8 *Let* (Term, $\leq$) *be any substructure of* $(IT[X], \leq)$ *for some* X*. Then,*

(i) $nat_0(v)$ *defines* NAT *in* $(FT, \leq)$*;*

(ii) $nat(v)$ *defines* NAT *in* (Term, $\leq$)*;*

(iii) (Term, $\leq$) $\models funct(h)$ *implies that the set*

$$\{(a,b) : a, b \in NAT, f(a,b) \leq h\} \text{ is a function.}$$

We can now describe two Σ_1 formulas which codify addition and multiplication in NAT.

Proposition 3.9 *In* $\mathcal{L}_{\leq}$ *there exist two* $\forall_{\leq}$ *formulas, which we denote by* $add(h,x,y,z)$ *and* $mult(h,x,y,z)$*, such that, for every* $m, n, r \in N$*,*

$$(\text{Term}, \leq) \models \exists h\, add(h, \underline{m}, \underline{n}, \underline{r}) \quad \textit{iff} \quad m + n = r$$

$$(\text{Term}, \leq) \models \exists h\, mult(h, \underline{m}, \underline{n}, \underline{r}) \quad \textit{iff} \quad m \cdot n = r.$$

Proof. We can take as $add(h,x,y,z)$ the formula which has quantification prefix $(\forall x_1, x_2 \leq x)(\forall z_1, z_2 \leq z)$ and whose matrix is the conjunction of the following formulas

$$y \leq z$$

$$f(x,z) \leq h$$

$$f(x_1, z_1) \leq h \rightarrow (x_1 = \underline{0} \leftrightarrow z_1 = y)$$

$$(x_1 = succ(x_2) \wedge z_1 = succ(z_2) \wedge f(x_1, z_1) \leq h) \rightarrow f(x_2, z_2) \leq h$$

Assume now that $h, \underline{m}, \underline{n}, \underline{r}$ satisfy such formula in a term algebra. Then, $n \leq r$ by the first line. The set $\{(a,b) : a, b \in N,\ f(\underline{a}, \underline{b}) \leq h\}$ contains a subset of pairs of the form

$$(m,r), (m-1, r-1), \ldots, (m-k, n-k)$$

and so it must exist a k such that $m - k = 0$ or $r - k = n$, by the second and the fourth line. Hence, by the third line we have necessarily $m - k = 0$ and $r - k = n$. So, $r = m + k$. Viceversa, given m, n and $r = m + n$ the term h

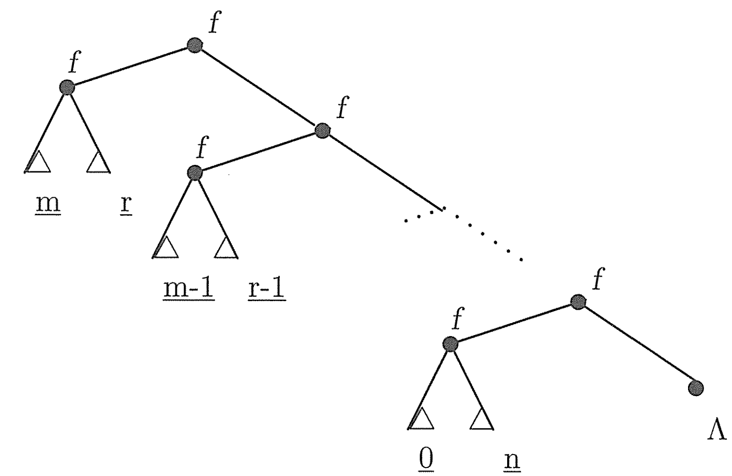

FIG. 1

satisfies $add(h, \underline{m}, \underline{n}, \underline{r})$.

We can argue similarly to get the formula $mult(h,x,y,z)$; the idea is that when $m > 0, n > 0, r > 0$ the term h has to contain the natural bijection between the sets

$$\{m, m-1, \ldots, 1\} \times \{n, n-1, \ldots, 1\} \quad \text{and} \quad \{r, \ldots, 1\}$$

where we think of the pairs in the first set to be ordered by the lexicographic order induced by the usual order on the natural numbers. We can take as $mult(h,x,y,z)$ the formula which has as bounded quantification prefix $(\forall x_1, x_2 \leq x)(\forall y_1, y_2 \leq y)(\forall z_1, z_2 \leq z)$ and whose matrix is the conjunction of the following formulas

$$z = \underline{0} \leftrightarrow (x = \underline{0} \vee y = \underline{0})$$

$$f(f(x,y),z) \leq h$$

$$f(f(x_1,y_1),z_1) \leq h \rightarrow ((x_1 = \underline{1} \wedge x_2 = \underline{1}) \leftrightarrow z_1 = \underline{1})$$

$$(y_1 \neq \underline{1} \wedge x_2 = x_1 \wedge y_1 = succ(y_2) \wedge z_1 = succ(z_2) \wedge f(f(x_1,y_1),z_1) \leq h)$$

$$\rightarrow f(f(x_2,y_2),z_2) \leq h$$

$$(y_1 = \underline{1} \wedge y_2 = y \wedge x_1 = succ(x_2) \wedge z_1 = succ(z_2) \wedge f(f(x_1,y_1),z_1) \leq h)$$

$$\rightarrow f(f(x_2,y_2),z_2) \leq h$$

Corollary 3.10 *Assume that our signature has at least a constant and a symbol of arity greater than* 1 *and that* (Term, $\leq$) *is any substructure of* $(IT[X], \leq)$ *for some* X. *Then we have*

(1) (Term, $\leq$) *is strongly undecidable.*

(2) *The theories* $\mathcal{O}_{FT}$ *and* $\mathcal{O}_{IT}$ *are essentially undecidable.*

(3) *The fragment* $Th_{\exists\forall_{\leq}}$(Term, $\leq$) *of the sentences in* $\exists\forall_{\leq}$ *which are true in* (Term, $\leq$) *is undecidable.*

Proof. (1) are (2) easy consequences of the fact that the structure of the natural numbers $\mathcal{N} = (N, +, \cdot, 0, 1, \leq)$ is definable in (Term, $\leq$). For (3) remember that $nat(x)$, $add(h, x, y, z)$, $mult(h, x, y, z)$ are $\forall_{\leq}$ formulas. Then, for any purely existential sentence α in the language of arithmetic a sentence α' in the fragment $\exists\forall_{\leq}$ of the language $\mathcal{L}_{\leq}$ can be constructed in order that α is true in $\mathcal{N}$ if and only if α' is true in (Term, $\leq$). Now, (3) is obtained from Matijasevič's theorem.

Consider now Σ_1 fragments.

Proposition 3.11 $Th_{\Sigma_1}(RT, \leq)$ *is recursively enumerable. More precisely, the* Σ_1 *sentences of* $\mathcal{L}_{\leq}$ *which are true in* $(RT, \leq)$ *are exactly the* Σ_1 *sentences deducible from the theory* $\mathcal{O}_{IT}$.

Proof. Observe that every model of $\mathcal{O}_{IT}$ is end-extension of $(RT, \leq)$; $\mathcal{A}$ end-extension means that $\mathcal{A}$ is extension and $b \in \mathcal{A}$ and $b \leq a \in RT$ imply $b \in RT$. So, conclude that a Σ_1 sentence which is true in RT is also true in any model of $\mathcal{O}_{IT}$.

In section 1 we have seen that the first-order theories of RT and IT in language $\mathcal{L}$ are equal and decidable. This does not happen for Σ_1 theories as the following proposition states.

Proposition 3.12 $Th_{\Sigma_1}(IT, \leq)$ *is not recursively enumerable; actually it is at least* Σ^1_1.

Proof. Let us show that $Th_{\Sigma_1}(IT, \leq)$ is at least in position Σ^1_1 in the analytical hierarchy. To obtain this, it is sufficient to prove that

For any Σ^1_1 sentence of the arithmetic α, a Σ_1 sentence α^* of $\mathcal{L}_{\leq}$ can be constructed such that

(1) $$\mathcal{N} \models \alpha \text{ if and only if } (IT, \leq) \models \alpha^*$$

where $\mathcal{N}$ is the structure of natural numbers.

Consider the formulation of second-order arithmetic which uses variables for unary functions and whose atomic formulas are of the form

(a) $u + v = w$

(b) $u \cdot v = w$

(c) $H_i(u) = v$

where u, v, w are numerical variables or numerals and H_i is a variable for unary function. We can suppose α to be of the form

(2) $$\exists H_1 \cdots \exists H_r Q_1 x_1 \cdots Q_k x_k \delta$$

where $H_1, \ldots, H_r$ are variables for unary functions, $Q_i x_i$ are first-oder quantifiers possibly bounded and δ is a quantifier free formula whose atomic subformulas are of the form (a), (b), (c).

Let now v be a numerical variable or a numeral and let $\tilde{v}$ be the term of $\mathcal{L}_{\leq}$ defined by

$$\tilde{v} = \begin{cases} v & \text{if } v \text{ is a numerical variable} \\ \underline{m} & \text{if } v \text{ is the numeral } \overline{m} \end{cases}$$

where $\overline{m}$ denotes the numeral corresponding to the natural number m in the language of arithmetic.

Suppose now we are given α as in (2); let us construct $\delta^{\perp}$ by replacing every subformula of δ of the form (a), (b), (c), respectively, with

$(\exists p \leq \Omega) add(p, \tilde{u}, \tilde{v}, \tilde{w})$

$(\exists q \leq \Omega) mult(q, \tilde{u}, \tilde{v}, \tilde{w})$

$f(\tilde{u}, \tilde{v}) \leq h_i$

where p, q, Ω, $h_1, \ldots, h_r$ are new distinct variables of $\mathcal{L}_{\leq}$ and $\leq$ is the usual predicate of $\mathcal{L}_{\leq}$. Define now the formula α^* as follows

$$\exists\Omega\exists h_1 \cdots \exists h_r Q_1^* x_1 \cdots Q_k^* x_k \left(\bigwedge_{1 \leq i \leq k} funct(h_i) \wedge \delta^{\perp} \right)$$

where the quantifier $Q_i^* x_i$ is obtained by relativizing the quantifier Q_i to the predicate $x_i \leq \Omega \wedge nat(x_i)$. We give now a sketch of a proof of (1). Assume $\mathcal{N} \models \alpha$. Let $H_1, \ldots, H_r$ be numerical functions which satisfy α (we denote the functions as the corresponding variables). Using (iii) of Proposition 3.8 it is easy to define, for any $H_i, i = 1, \ldots, r$ a term, possibly infinite, which we denote by h_i such that, for every $a, b \in N$,

$$H_i(a) = b \quad \text{if and only if} \quad f(\underline{a}, \underline{b}) \leq h_i$$

and such that h_i satisfies $funct(h_i)$ in $(IT, \leq)$ (the construction is similar to that of term in figure FIG. 1). Besides, we construct an infinite term Ω which has as its subterms all the elements of NAT, all the $f(\underline{a}, \underline{b})$ such that the pairs (a, b) determine the natural bijection between

$$\{m, \ldots, 0\} \quad \text{and} \quad \{r, \ldots, r-n\} \quad \text{for every } m, n, r \in N \text{ such that } m+n = r$$

and all the terms $f(\underline{a}, \underline{b})$ which determine the natural bijection between

$$\{m, \ldots, 1\} \times \{n, \ldots, 1\} \quad \text{and} \quad \{r, \ldots, 1\} \quad \text{for every } m, n, r \geq 1.$$

Using now Propositions 3.8 e 3.9 we get that $(IT, \leq) \models \alpha^*$. The converse can be proved straightforwardly by using the same propositions and the definition of $\delta^{\perp}$.

to appear in Information and Computation

Decidability of the existential Theory of Infinite Terms with subterm Relation

Sauro Tulipani*
University of Camerino

Abstract

We examine the problem of solving equations, disequations and atomic formulas built on the subterm relation in algebras of rational and infinite terms (trees). We prove that this problem is decidable for any such algebra in a finite signature S with possible new free constants. Moreover, even in presence of subterm relation, the existential theory of rational trees is the same as the existential theory of infinite trees. We leave out the easier case where S has no symbols of arity greater than one. When S has only a symbol of arity greater than one, the decision procedure is different in case that the algebra of rational or infinite trees contains new free constants or not.

*The author thanks MURST and CNR for partial support and thanks the Mathematical Institute of the Oxford University for hospitality during the preparation of the first draft of this paper. Permanent address: Dipartimento di Matematica e Fisica, Università, I-62032 Camerino, Italy; e-mail: tulipani@camvax.cineca.it .