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

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

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.

INTRODUCTION

In recent programming methodology high level languages manipulate a variety of inductively defined data structures. This feature, initiated with LISP, is useful for integrating the recursion into programming and it is pursued for theoretical and practical benefit. In theory, any computation may be reduced, by coding, to a computation on the natural numbers. However, the coding may obscure the structure of the original problem and may lose clearness and simplicity in designing algorithms. In this framework the decidability of properties of abstractly defined data structures is useful for reasoning about programs, in termination proofs and in verification, as well in automated deduction.

Most of data domains like strings or trees are absolutely free algebras, called also (finite) term algebras, on a given signature. Other domains are initial algebras and can be presented as quotients of free algebras. Solving equations in absolutely free algebras was known to be useful for automated deduction since Herbrand [1930]. This need grew stronger after the implementation of the resolution rule (Robinson [1965]) and the development of Horn Logic Programming by Colmerauer and Kowalski in the early seventies.

The decidability of the first order theory of free algebras goes back to a landmark paper by Mal'cev [Mal61] who gave axioms for the locally free algebras. Quite closely Oppen [Op80] analyzed the first order theory of the recursively defined data structures and gave a decision procedure. The axioms of Mal'cev have been used to assign declarative meaning to the Negation as Failure Rule [Cl78,Ll87] in Horn Logic Programming. So, the decidability of the theory of the absolutely free algebras becomes indispensable in the Fitting [Fi85] and Kunen [Ku87] approach to the semantics of the Logic Programming. The work of Mal'cev falls into the scope of what is now called disunification [Com90]. This attempts to solve more general formulas than simply equations and it arises in many problems in computer science like the complement problem, the sufficient completeness problem for the specifications [GH78], the representation of answers to queries in Prolog II (see [Com90] for a discussion).

Recently, Venkataraman [Ven87] has considered decidability problems for the absolutely free algebras in the first order language with operation symbols, equality and a symbol for the subterm relation. In the presence of the partial order induced by the subterm relation, the full first order theory of

an absolutely free algebra, with some operation of arity greater than one, is undecidable. This was observed by McCarthy [McC77] , see also [VYH83]. However, Venkataraman [Ven87] proves that the problem of solving existential sentences is decidable and NP-complete.

In this paper we take into consideration algebras built on, possible infinite, terms. We solve the decision problem for the existential sentences in the first order language which has symbols for a finite number of operations, for the equality and the subterm relation. Infinite term algebras arose in mathematical investigations on the semantics of programming languages, mainly in the French school, see [Co85]. They became relevant also for the semantics of the new Prolog generations [Col84]. The decision problem for the theory of infinite terms without the subterm relation was solved by Maher [Mah88]. Disunification algorithms were studied by Comon and Lescanne [CL89]. In a subsequent paper Marongiu and Tulipani [MT89] complete Maher results and introduce some expressions, called terms with pointers, to represent the rational terms. This representation helps us to design, in this paper, the required procedures.

We work with a finite signature S where the subset of constant symbols S_0 is non empty and $S \setminus S_0$ contains a symbol, say f, of arity at least 2. Often we use an f of arity 2 to simplify notation. Our assumption is motivated by the feeling that, when $S \setminus S_0$ has no symbols of arity greater than 1, the full first order theory of rational or infinite terms is decidable as it is for finite terms (see [Ra77]). This will discussed in a future paper. Our language contains operation symbols, the equality and the symbol $\leq$ to be interpreted, in term algebras, in the preorder given by the subterm relation.

In Section 3, along a similar line pursued in [Ven87], we reduce the problem of deciding existential sentences to the problem of solving special systems, called reduced systems. In Section 4 we study the solution of reduced systems in the algebras $IT[X]$ and $RT[X]$ which are the infinite and the rational terms, respectively, formed by adding to the signature a new set X of free constants, called indeterminates. We give an algorithm for testing the solvability of a reduced system in $IT[X]$ and in $RT[X]$ and for determining solutions. Moreover, we prove that existential sentences in our language are true in $RT[X]$ if and only if they are true in $IT[X]$. In Section 5 we give a procedure for solving systems in the algebra RT of the rational terms and we prove that RT and the algebra IT of infinite terms have the same first order existential theory. It turns out that the existential theories of $RT[X]$, where X is non empty, and RT are different if and only if $S \setminus S_0$ has a unique symbol. We say in this case that S is singular. We have to treat differently singular and non singular signatures because in the first case there is only one full infinite tree, i.e. a term without constant symbols as subterm, and in the second case there are infinitely many full trees. In Section 6 we show that our method can be used also to give another proof of the decidability result of Venkataraman [Ven87] for the algebra of finite terms. Finally, in Section 7 we discuss axioms which direct the use of the rules in the previous procedures.

The undecidability of the first order theory of the algebra of finite terms carries on infinite terms [Tre90,Tre90a]. In fact, in our signature the fragment of Σ_1-sentences true in RT, denoted $Th_{\Sigma_1}(RT)$, is undecidable. In analogy with the arithmetical hierarchy we call Σ_1-sentences the sentences which are existential quantification of formulas where other quantifiers may appear if they are all bounded by the symbol $\leq$. Moreover, it can be proved that $Th_{\Sigma_1}(RT)$ is recursively enumerable, but the Σ_1-theory $Th_{\Sigma_1}(IT)$ of infinite term with subterm relation, unlike in the existential case, is very different from $Th_{\Sigma_1}(RT)$. In fact its degree of unsolvability, being Σ_1^1, is above the arithmetical hierarchy.

There are very recent papers which are related to our work . The paper [Com90a] in which the existential theory of a lexicographic path ordering on finite terms is proved to be decidable and the paper [MS90] where some decidability problems about rational trees are studied and, constructions and useful techniques are developed. The author is very grateful to the Referees for having informed him about the work in progress and for remarks and comments which have so much improved the final version of the paper.

1 Notation and preliminaries

A *signature* S is a set of ranked function symbols. The rank of an $f \in S$ is called the *arity* of f. As we said we assume that the set of constant symbols S_0 is non empty and that $S \setminus S_0$ contains a symbol of arity greater than one.

Let N_+^* be the free monoid of words on the alphabet of positive integers N_+; ε will denote 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 $j \leq p$. A function $t : D \to S$ is called a *term* 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. IT will denote the set of all terms in our fixed signature S. This is an algebraic structure over S. FT will denote the substructure of all the *finite terms*, i.e. of finite domain. Any element $p \in D$ is called an *occurrence*, or position, in t; D will be occasionally denoted by Occ(t). When t is finite the *depth* of t, denoted *depth*(t), is the maximum of the lengths of all the occurrences in $Occ(t)$.

Let V be any set of new elements such that $V \cap IT = \emptyset$. We define $IT[V]$, $FT[V]$ 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* and occasionally *indeterminates*. If $t \in IT[V]$ then $var(t)$ denotes the set of the variables in the range of t; more generally, if $H \subseteq IT[V]$, or it is any kind of syntactic object, then $var(H)$ denotes the set of variables which occur in every term of H.

Assume $s, t \in IT[V]$. Then *s is a subterm of t*, denoted $s \leq t$, if there is some $p \in$ Occ(t) such that Occ(s) $= \{q : p.q \in$ Occ(t)$\}$ and $s(q) = t(p.q)$ for every $q \in$ Occ(s). The term s is denoted by t/p. Observe that the interpretation of any n-ary operation f in $IT[V]$ is such that: $f(t_1, \ldots, t_n) = t$ iff Occ(t) $= \{\varepsilon, i.p : p \in$ Occ(t_i) for some $1 \leq i \leq n\}$ and $t(\varepsilon) = f$, $t/i = t_i$ for every $1 \leq i \leq n$.

$RT[V]$ is the substructure of $IT[V]$ of terms having a finite number of subterms; the elements of $RT[V]$ are called *rational terms*. Any such term can be represented by a syntactic expression which can be defined as follows. We consider the algebra of finite terms $FT[V \cup N_+]$ on the signature S, where N_+ is the set of the positive integers; we may suppose that S, the variables V and N_+ be pairwise disjoint. Then the set $R[V]$ of *terms with* *pointers* is

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

We call a *pointer* in t any occurrence $p \in Occ(t)$ such that $t(p) \in N_+$ and we denote by $point(t)$ the set of all pointers in t. If $p \in point(t)$ and $t(p) = m \in N_+$ then we denote by $t(p)\uparrow$ the unique position $q \in Occ(t)$ such that $q \prec p$ and $|p| - |q| = m$. Any pointer $p \in point(t)$ such that $t(p) = |p|$ will be called *maximal pointer*. If p is maximal then $t(p)\uparrow$ is the occurrence ε.

Any $t \in R[V]$ will also be called a syntactic term or simply a term when it is clear from the context. Although the elements of $R[V]$ are defined to be functions, they may also be thought of as well-formed expressions on the alphabet which represents the set $S \cup V \cup N_+$. In fact, the elements of $FT[V \cup N_+]$ can be defined as expressions in the usual inductive way.

Since $R[V]$ is an algebraic substructure of the absolutely free algebra $FT[V \cup N_+]$ it is possible to define *replacement* and *substitution* in terms with pointers. Given $t, s_1, \ldots, s_k \in FT[V \cup N_+]$ and occurrences $p_1, \ldots, p_k \in Occ(t)$, which are incomparable with respect to $\preceq$, we denote the replacement in t of $s_1, \ldots, s_k$ at positions $p_1, \ldots, p_k$ by $t[p_1 \leftarrow s_1, \ldots, p_k \leftarrow s_k]$. Furthermore, as usual, $t[s/v]$ will denote the substitution of s in t for the variable v. In an analogous way, the simultaneous substitution of many variables $t[s_1/v_1, \ldots, s_k/v_k]$ will be defined.

Note that $R[V]$ is stable for the operation of replacement and substitution. This means that when $t, s_1, \ldots, s_k \in R[V]$ then also $t[p_1 \leftarrow s_1, \ldots, p_k \leftarrow s_k]$ and $t[s_1/v_1, \ldots, s_k/v_k]$ are still in $R[V]$. Observe also that any substitution on $R[V]$ is a morphism which is the identity on V except a finite subset of variables. On the other hand, we recall, that replacement and substitution are defined also for infinite terms of $IT[V]$. Substitutions are morphisms of $IT[V]$ which are the identity on the variables except on a finite subset. Moreover, the substructures $RT[V]$ and $FT[V]$ are stable with respect to replacement and substitution. In what follows we denote by $[s_1/v_1, \ldots, s_k/v_k]$ either a substitution in $R[V]$ or in $IT[V]$ depending on whether all the s_i, for $i = 1, \ldots, n$, are in $R[V]$ or in $IT[V]$. The substitutions and the replacements will be put to the right of their arguments.

Observe that if $t \in R[V]$ and $p \in Occ(t)$ then the subterm t/p is in $FT[V \cup N_+]$ and t/p is in $R[V]$ if and only if $t(q) \leq |q| - |p|$ for every pointer q with $p \prec q$. Now we define the notion of *n-th unfolding* $t^{(n)}$, for

every $t \in R[V]$ and every natural number n, and we define the term $t/\!/p$, for every $p \in Occ(t)$. This turns out to be useful to represent the rational terms of $RT[V]$ by means of syntactic terms in $R[V]$ and to handle the notion of subterm at position p, respectively. We proceed by induction as follows: $t^{(0)}$ is t; $t^{(1)}$ is the term obtained with the replacement of t in t at every maximal pointer; $t^{(n+1)}$ is t if $depth(t) = 0$, i.e. t is a variable or a constant, and $t^{(n+1)} = f\left((t^{(1)}/1)^n, \ldots (t^{(1)}/k)^n\right)$, if $depth(t) > 0$, $t(\varepsilon) = f$ and f is of arity k. Then the term $t/\!/p$ is defined as $t^{(|p|)}/p$, for every $p \in Occ(t)$.

It is easy to see that if $t \in R[V]$ then $t^{(n)}$ and $t/\!/p$ are in $R[V]$ for every n. Moreover, the main properties are

(1.1) if $q = t^{(n)}(p)\uparrow$, for some $p \in Occ(t^{(n)})$, then $|q| \geq n$;

(1.2) $Occ(t^{(n)}) \subseteq Occ(t^{(n+1)})$ for every n;

(1.3) $t^{(n)}(p) = t^{(n+1)}(p)$ for every p, n such that $p \in Occ(t^{(n)})$ and $|p| < n$;

(1.4) $t^{(n)}/p = t^{(n)}/\!/p$ for every $p \in Occ(t^{(n)})$ with $n \geq |p|$.

Let t be in $R[V]$. Then we define a formula $D_t(w, \vec{v})$ in the first order language $\mathcal{L}$ with equality and signature S. The free variables of such a formula are the variables $\vec{v}$ in $var(t)$ and a new variable w. We denote $point(t)$ by $\{p_1, \ldots, p_k\}$ and we take a set of new variables $\{w_1, \ldots, w_k\}$. We define the finite term $t' \in FT[V \cup \{w_1, \ldots, w_k\}]$ by $t' = t[p_i \leftarrow w_i \quad i = 1, \ldots, k]$. Then, $D_t(w, \vec{v})$ is the formula

$$\exists w_1 \ldots \exists w_k((w = t') \wedge \bigwedge_{1 \leq i \leq k} (w_i = t'/t(p_i)\uparrow))$$

Now, it is possible to give axioms for the first order theory $\mathcal{T}_{IT}$ of infinite terms in our signature S (see [Mah88,MT89,Com90]). They are the universal quantification over the free variables of the following

(F1) $f(v_1, \ldots v_k) = f(z_1, \ldots z_k) \quad \rightarrow \quad v_1 = z_1 \wedge \ldots \wedge v_k = z_k$ for every $f \in S$;

(F2) $f(v_1, \ldots v_k) \neq g(z_1, \ldots z_r)$ for all $f, g \in S$ with $f \neq g$;

(D) $\exists! w D_t(w, \vec{v})$ where t ranges on $R[V]$ for V countably infinite.

The syntactic terms of $R[V]$ can be interpreted in every model of the axioms of $\mathcal{T}_{IT}$. Such an interpretation extends the usual one when it is restricted to the terms in $FT[V]$. The interpretation is based on the following proposition. If $s \in R[V]$ and w is a variable different from s, we denote by $s^w_\uparrow$ the term in $R[V]$ defined by

$$s^w_\uparrow(p) = |p| \quad \text{if } s(p) = w \quad \text{and} \quad s^w_\uparrow(p) = s(p) \quad \text{otherwise.}$$

Of course, if $w \notin var(s)$ then $s^w_\uparrow$ is s itself. We define $s^w_\uparrow$ also when s is w to be the variable w.

Proposition 1.1 *Let $\mathcal{A}$ be a model of $\mathcal{T}_{IT}$ and $\alpha : V \longrightarrow \mathcal{A}$ be an assignment for the variables in V. Then, there exists a unique morphism $\tilde{\alpha} : R[V] \rightarrow \mathcal{A}$ such that α is the restriction of $\tilde{\alpha}$ to V and $\tilde{\alpha}(t[t^w_\uparrow/w]) = \tilde{\alpha}(t^w_\uparrow)$ for every term t and variable w. Moreover, $\tilde{\alpha}(t[s^w_\uparrow/w]) = \tilde{\beta}(t)$, for every variable $w \in V$ and every $s \in R[V]$, where β is the assignment such that $\beta(w) = \tilde{\alpha}(s^w_\uparrow)$ and $\beta(v) = \alpha(v)$ for $v \in V \setminus \{w\}$.*

Proof: By axioms in (D). (See [MT89]).

Now, we make some remarks and state some facts which follow easily from Proposition 1.1 and the various given definitions. To simplify notation, we occasionally denote by α the morphism $\tilde{\alpha}$ of the above Proposition.

Remarks

1.2 Proposition 1.1 allows us to interpret in models of $\mathcal{T}_{IT}$ any formula which is built as a first order formula on the atomic formulas $t = s$ for $t, s \in R[V]$ (see [MT89]). Such formulas will be called *formulas with pointers*. It is also clear that any formula with pointers is equivalent under axioms of $\mathcal{T}_{IT}$ to an ordinary first order formula which can be easily computed.

1.3 We may define the relation on $R[V]$ by: $t \sim s$ iff $\mathcal{T}_{IT} \models t = s$. Here, variables are thought universally quantified. The relation $\sim$ is a congruence relation on the algebra $R[V]$ and we have for all terms t, s and every natural number n .

(1.5) $t \sim t^{(n)}$;
(1.6) $t \sim s$ implies $t^{(n)} \sim s^{(n)}$;
(1.7) $t \sim s$ and $p \in Occ(t)$ with $|p| \leq n$ implies $p \in Occ(s^{(n)})$ and $t^{(n)}(p) = s^{(n)}(p)$;
(1.8) $t^{(n)}/p \sim t/\!/p$ for $n \geq |p|$;
(1.9) $t/\!/p \sim t/\!/q$ for every $p, q \in Occ(t)$ such that $q = t(p)\!\uparrow$.

The proof follows by the properties (1.1)–(1.4) and by Proposition 1.1.

1.4 By means of the notion of n-th unfolding we may define a morphism $e_V : R[V] \longrightarrow RT[V]$. Given $t \in R[V]$ we define $e_V(t) = \hat{t}$ where $\hat{t} : \bigcup_n Occ(t^{(n)}) \longrightarrow S \cup V$ and $\hat{t}(p) = t^{(n)}(p)$ if n is the minimum number such that $p \in Occ(t^{(n)})$ and $n \geq |p|$. By properties (1.1)–(1.4) the definition is correct. Moreover, by the various definitions and properties in Remark 1.3, we have

(1.10) $e_V(t/\!/p) = \hat{t}/p$ for every $p \in Occ(t)$;

(1.11) $\hat{t}$ is a rational term and it is the unique element such that the defining formula $D_t(w, \vec{v})$ is satisfied in $RT[V]$ under the assignment $w \mapsto \hat{t}$ and $v \mapsto v$ for every $v \in V$;

(1.12) e_V is a morphism and $Im(e_V) = RT[V]$;

(1.13) $t \sim s$ iff $\hat{t} = \hat{s}$;

(1.14) Let $\mathcal{A}$ be a structure for the signature S. Then, for every morphism $\beta : R[V] \longrightarrow \mathcal{A}$, which preserve the congruence $\sim$, there exists a unique morphism $\hat{\beta} : RT[V] \longrightarrow \mathcal{A}$ such that $\hat{\beta}(\hat{t}) = \beta(t)$; so, $\beta = e_V\hat{\beta}$. The morphism e_V will be called *canonical morphism.*

1.5 $IT[X]$ and $RT[X]$ are models of $\mathcal{T}_{IT}$ for every set of indeterminates X. In fact, given $t \in R[V]$ and an assignment $\alpha : V \longrightarrow RT[X]$, then the formula $D_t(w, \vec{v})$ is satisfied in $RT[X]$ and in $IT[X]$ by the assignment $v \mapsto \alpha(v)$ for $v \in V$ and $w \mapsto \hat{t}[\alpha(v)/v : \ v \in var(t)]$. Moreover, the map $e_V : R[V] \longrightarrow RT[V]$ is the unique map which, according to Proposition 1.1, extends the embedding $V \hookrightarrow RT[V]$.

1.6 For every formula with pointers Φ, every variable w and every term with pointers s

$$\mathcal{T}_{IT} \models \forall \vec{v} \left(\exists w (w = s \wedge \Phi) \longleftrightarrow \Phi[s^w_\uparrow/w] \right)$$

where $\vec{v}$ is a list of the variables in $var(\Phi, s) \setminus \{w\}$.

1.7 Let Φ be $v = w$ in the previous remark, where $v \notin var(s)$. Let $\mathcal{A}$ be a model of $\mathcal{T}_{IT}$ and α be an assignment for the variables in $var(s) \setminus \{w\}$. Then we may conclude that the interpretation of $s^w_\uparrow$ in $\mathcal{A}, \alpha$ is the unique solution of the equation $w = s(w)$. More generally, let $w_i = s_i(\vec{w})$ be a system, where $s_i \in R[\{w_1, \dots, w_n\} \cup X] \setminus \{w_1, \dots, w_n\}$, for $i = 1, \dots, n$. Then it is possible to compute unique elements $\tau_i \in R[X]$ such that

$$RT[X] \models \tau_i = s_i[\tau_j/w_j : 1 \le j \le n]$$

for $i = 1, \dots, n$. (See [Co85]).

1.8 For $t, s \in R[V]$ we define $t \trianglelefteq s$ iff there is $p \in Occ(s)$ such that $t \sim s//p$. Then

(i) The relation $\trianglelefteq$ is reflexive and transitive, i.e. a preorder.

(ii) $t \sim s$ implies $t \trianglelefteq s$; $t \trianglelefteq v$, for v variable, implies $t = v$.

(iii) $t \trianglelefteq s$ in $R[V]$ iff $\hat{t} \le \hat{s}$ in $RT[V]$, i.e. the canonical morphism e_V is a preorder morphism.

1.9 Let V be finite, then every morphism $R[V] \to R[X]$, which fixes the extra constants in N_+, is a substitution $\sigma = [s_1/v_1, \dots, s_n/v_n]$. Moreover, given σ, by Remark 1.4 there exists a morphism $\hat{\sigma} : RT[V] \to RT[X]$ such that $\sigma e_X = e_V \hat{\sigma}$. The morphism $\hat{\sigma}$ is nothing but the substitution $[\hat{s}_1/v_1, \dots, \hat{s}_n/v_n]$; so, every morphism $RT[V] \to RT[X]$ is $\hat{\sigma}$ for some σ. Moreover, for every $t, s \in R[V]$

(i) $t \sim s$ implies $t\sigma \sim s\sigma$

(ii) $t \trianglelefteq s$ implies $t\sigma \trianglelefteq s\sigma$

(iii) $\widehat{t\sigma} = \hat{t}\hat{\sigma}$.

In what follows only morphisms of this kind are considered.

1.10 When (i) of the previous remark can be reversed, i.e. for every $t, s \in R[V]$, $t\sigma \sim s\sigma$ implies $t \sim s$, we say that σ *is injective (modulo $\sim$)*. In fact, in this case $\hat{\sigma}$ is injective. When (ii) can be reversed we will say that σ *is a preorder morphism (modulo $\sim$)*. If one of the above conditions is satisfied only for all $t, s \in H$, where H is a fixed subset of $R[V]$, we will say that σ is injective (modulo $\sim$), or preorder morphism (modulo $\sim$), *on H*.

2 Subterm relation

We have already defined the notion $t \le s$, "t is subterm of s", for $t, s \in IT[X]$. It is a simple remark to observe that such a relation is a preorder, see Remark 1.8. The relation $\le$ is a partial order on the finite terms $FT[X]$. Moreover, here $\le$ coincides with $\trianglelefteq$.

Now, we consider the first order language $\mathcal{L}$ for the signature S with equality and the language $\mathcal{L}_\le$ which is obtained by adding to $\mathcal{L}$ a new binary relation symbol that we still denote $\le$. We call *formulas with pointers of $\mathcal{L}_\le$* the formulas which are built, as first order formulas, on the atomic formulas $t = s$ and $t \le s$, where $t, s \in R[V]$ and V is some countably infinite set of variables. We occasionally say terms and formulas instead of terms with pointers and formulas with pointers.

Definition 2.1 *Let $\mathcal{A}$ be a structure for $\mathcal{L}_\le$ and the restriction of $\mathcal{A}$ to $\mathcal{L}$ be a model of $\mathcal{T}_{IT}$. Then, we stipulate that $\mathcal{A}$* satisfies *the atomic formula with pointers $t \le s$ under the assignment α if $\mathcal{A}, \alpha$ satisfies, in the usual sense, the first order formula*

$$\exists u_1 \exists u_2\, (D_t(u_1, \vec{v}) \wedge D_s(u_2, \vec{v}) \wedge u_1 \le u_2)$$

where u_1, u_2 are new variables and the variables $\vec{v}$ of $var(t, s)$ are interpreted by α. We keep the notation $\mathcal{A}, \alpha \models t \le s$.

Remark 2.2 *The interpretation given in Definition 2.1 is well behaved. In fact, the property in Remark 1.6 is true also for sentences of $\mathcal{L}_\le$. Hence, every model $\mathcal{A}$ and assignment α satisfy, as in Definition 2.1, the substitutivity*

$$t = t' \wedge s = s' \longrightarrow (t \le s \leftrightarrow t' \le s')$$

where $t, t', s, s' \in R[V]$.

Now, we consider the following axioms in the language $\mathcal{L}_\le$:

(O1) Reflexive and transitive for $\le$

(O2) Antisymmetric for $\le$

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

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 recall (see [Mal61,Com90]) that the theory $\mathcal{T}_{FT}$ of finite terms in the language $\mathcal{L}$ has axioms (F1), (F2) and the infinite set of axioms

(OC) $t(v) \neq v$

for every $t \in FT[V]$, $v \in var(t)$, t different from v and V countably infinite.

Definition 2.3 *In the language $\mathcal{L}_{\leq}$ we define the theories:*

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

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

Remarks

2.4 $IT[X]$ and $RT[X]$ are models of $\mathcal{O}_{IT}$ and $FT[X]$ is model of $\mathcal{O}_{FT}$, for every set X of indeterminates, when the symbol $\leq$ is interpreted in the subterm relation. Moreover, $(IT[V],\leq) \models t \leq s$ holds, where the variables are universally quantified, iff $t \trianglelefteq s$ holds, for $t,s \in R[V]$.

2.5 Axioms similar to $\mathcal{O}_{FT}$ were already considered in [VYH83, Section 6] and in [Ven87]. Here, Venkataraman proves that the existential fragment of the sentences true in $(FT,\leq)$ is decidable and the problem is NP-complete. Observe that axiom (O3) is consequence of (O4). In the presence of the axioms for $\leq$, the theory $\mathcal{O}_{FT}$ is finitely axiomatizable. In fact, the Occur-check Axiom schema (OC) can be replaced by the finite set of axioms

$$\forall v_1 \ldots \forall v_n (\bigwedge_{1\leq i\leq n} f(v_1,\ldots,v_n) \not\leq v_i) \quad \text{for every } f \in S.$$

2.6 Let $\mathcal{A}$ be any model of $\mathcal{O}_{IT}$ and $\alpha : V \longrightarrow A$ be a variable assignment. Then, the morphism $\tilde{\alpha} : (R[V],\leq) \longrightarrow \mathcal{A}$ preserves the preorder, i.e. $s \trianglelefteq t$ implies $\tilde{\alpha}(s) \leq \tilde{\alpha}(t)$, for every $s,t \in R[V]$. Analogous property holds for models of $\mathcal{O}_{FT}$ and $FT[V]$.

2.7 Let $\mathcal{S}$ be a finite system of basic formulas with pointers, i.e. $\mathcal{S}$ contains formulas $t = s$, $t \neq s$, $t \leq s$, $t \not\leq s$ for $t,s \in R[V]$; we may suppose V finite. Then $\mathcal{S}$ is satisfiable in $RT[X]$, for some set X of indeterminates, iff there exists a substitution $\sigma : V \longrightarrow R[X]$ such that:

$$\begin{array}{lll} t\sigma \sim s\sigma & \text{if} & t = s \in \mathcal{S} \\ t\sigma \not\sim s\sigma & \text{if} & t \neq s \in \mathcal{S} \\ t\sigma \trianglelefteq s\sigma & \text{if} & t \leq s \in \mathcal{S} \\ t\sigma \not\trianglelefteq s\sigma & \text{if} & t \not\leq s \in \mathcal{S} \end{array}$$

Moreover, if $\eta : R[X] \longrightarrow R[Y]$ is a morphism which is injective (modulo $\sim$) and a preorder morphism (modulo $\sim$) then $\sigma\eta$ gives a solution of $\mathcal{S}$ in $RT[Y]$.

3 Satisfiability of existential sentences in models of $\mathcal{O}_{IT}$ and reduced systems

In this Section we deal with the satisfiability of sentences $\exists v_1 \ldots \exists v_n \Phi$, where Φ is a quantifier-free formula with pointers in the language $\mathcal{L}_{\leq}$. Such sentences are equivalent under the theory $\mathcal{O}_{IT}$ to mere existential sentences of $\mathcal{L}_{\leq}$ (see Remark 1.2 and Definition 2.1).

We will say that a transformation of sentences is correct with respect to a given theory $\mathcal{T}$ if whenever ψ is transformed into ψ_1 then $\mathcal{T} \models \psi \leftrightarrow \psi_1$. It is helpful to put in the language two special symbols $TRUE$ and $FALSE$ to be interpreted in obvious way. Any atomic formula with pointers $t = s$, where $s, t \in R[V]$, is called *equation with pointers.* It is called *elementary equation with pointers* if t is a variable in V. Now, we recall a Lemma [Hue76] which gives a decomposition of an equation with pointers into elementary equations with pointers. We denote by $\bigwedge E$, $\bigvee E$, the conjuction, the disjunction, respectively, of all the formula in the set E.

Lemma 3.1 (Elementarization). *There is a procedure such that for every equation with pointers $t = s$ computes a set E, where either $E = \{FALSE\}$ or E is a finite set, possibly empty, of elementary equations with pointers and*

$$\mathcal{T}_{IT} \models (t = s) \leftrightarrow \bigwedge E \ .$$

Here the variables are universally quantified and we agree that $\bigwedge \emptyset$ is $TRUE$. Moreover, every term with pointers u which appears in E is such that $u \trianglelefteq t$ or $u \trianglelefteq s$.

We now derive a corollary which will be useful later. We say that a set H of terms with pointers is closed under subterms if $t \in H$ and $s \trianglelefteq t$ implies $s \in H$. Moreover, we use the definitions given in Remark 1.10.

Corollary 3.2 *Let $\beta : R[V] \to R[X]$ be a morphism, determined by a substitution, and $H \subseteq R[V]$ be a set closed under subterms. Then,*

(1) *β is injective (modulo $\sim$) on H iff:*

(1i) $\quad t\beta \sim v\beta$ *implies* $t = v$, $\quad$ *for every* $t \in H$, $v \in var(H)$.

(2) *If β is injective on H and $H_0 \subseteq H$ then β is a preorder morphism (modulo $\sim$) on H_0 iff:*

(2i) $\quad t\beta \trianglelefteq v\beta$ *implies* $t = v$, $\quad$ *for every* $t \in H_0$, $v \in var(H)$.

Proof: First recall Remarks 1.9 and 1.10. Then observe that the proof of (1) is immediate by Lemma 3.1 and Remark 2.4. To prove (2) assume β is injective (modulo $\sim$) on H and assume (2i). Start with $t\beta \trianglelefteq s\beta$ for some $t, s \in H_0$. Then, by axiom schema (O4), only two cases can occur

Case 1: $t\beta \sim z\beta$ for some $z \trianglelefteq s$. Then, $t \sim z$ because β is injective (modulo $\sim$) on H. Hence, $t \trianglelefteq s$.

Case 2: There exists $v \in var(s)$ such that $t\beta \trianglelefteq v\beta$. Then $t \trianglelefteq s$ by (2i).

Axiom schema (O4) gives for every formula with pointers $s \leq t$ a finite, possibly empty, set D of equations and of formulas with pointers of the kind $s \leq v$, where $v \in var(t)$, such that $\mathcal{O}_{IT} \models s \leq t \leftrightarrow \bigvee D$. So, given a formula with pointers Φ, we replace, first, every atomic formula with pointers $s \leq t$, where t is not a variable, by the disjunction $\bigvee D$ which can be computed as described before. Then, we replace in Φ every equation with pointers $t = s$ with $\bigwedge E$, where E is the set computed in Lemma 3.1. Finally, we put the formula in disjunctive normal form. This procedure will be called *Elementarize* Φ. It is immediate to prove that the transformation is correct with respect to the theory $\mathcal{O}_{IT}$.

We call *reduced* a system $\mathcal{S}$ of conjunction of atomic formulas with pointers of the kind: $t \leq v$ or $t \not\leq v$ or $t \neq v$, where v is some variable and t is different from v.

Now, we describe a procedure along the same line as the unification algorithm (see [MT89,Com90]). The input is a given quantifier-free formula with pointers Φ and the output is a formula Φ' which is either $TRUE$ or $FALSE$ or a disjunction of reduced systems and $var(\Phi') \subseteq var(\Phi)$. Moreover, if $\vec{v}$ a list of the variables in Φ then $\mathcal{O}_{IT} \models \exists \vec{v} \Phi \leftrightarrow \exists \vec{v} \Phi'$.

We call *trivial* the following kind of formulas: $TRUE$, $\ t \leq t$, $\ t = t$, for any term with pointers t. We call *incoherent* their negations: $FALSE$, $t \not\leq t$, $\ t \neq t$. If Φ is in disjunctive normal form $\Phi = \bigvee_i \Phi_i$, where every Φ_i is conjunction of atomic formulas, then we call every Φ_i a disjunct.

The procedure is the following

Reduce Φ;
repeat

1. elementarize Φ;
2. cancel all the trivial atomic formulas in every disjunct of Φ;
3. if some disjunct is empty then return $TRUE$;
4. cancel all disjuncts which contain incoherent atomic formulas;
5. if the disjunction is empty then return $FALSE$;
6. eliminate the elementary formulas $v = t$ or $t = v$, where v is a variable and apply the substitutions $[t^v_\uparrow/v]$

until $TRUE$ or $FALSE$ is returned or Φ is disjunction of reduced systems.

The termination is clear since step 6 eliminates variables. The correctness of transformations 1–5 is clear. The correctness of transformation 6 is discussed in Remarks (2.2) and (1.6). So, the procedure returns a formula Φ' such that $\mathcal{O}_{IT} \models \exists\vec{v}\Phi \leftrightarrow \exists\vec{v}\Phi'$ and Φ' is disjunction of reduced systems. Observe also that if Φ'' denotes the set of elementary equations eliminated by 6, then the solutions of Φ are the solutions of the conjunction $\Phi' \wedge \Phi''$. Thus, to solve Φ one needs to solve Φ' since Φ'' is in solved form.

4 Satisfiability test for reduced systems

To solve the satisfiability of existential sentences in models of $\mathcal{O}_{IT}$ we may consider only reduced systems after the procedure given in Section 3. So, we consider a single reduced system $\mathcal{S}$ since the existential quantifier distributes over disjunction. We give a procedure which fails if and only if $\mathcal{S}$ is not satisfiable in a model of $\mathcal{O}_{IT}$. Furthermore, when $\mathcal{S}$ is satisfiable the procedure gives a solution in $RT[X]$, where X has cardinality not less of the variables in $\mathcal{S}$. The procedure uses the following transformation T0 and the tests T1 and T2.

T0 Denote by V the set $var(\mathcal{S})$. Define the relation R on V by: vRw iff there exists $t \leq w \in \mathcal{S}$ such that $v \in var(t)$. Let $\rightarrow$ be the transitive closure of R and $\sqsubseteq$ be the reflexive closure of $\rightarrow$. The relation $\sqsubseteq$ is called elsewhere Occur-check relation (see [JK90]). Let V_0 be the set of $v \in V$ such that there is no t for which $t \leq v \in \mathcal{S}$. Let $V_1, \ldots, V_n$ be the classes of the equivalence relation on $V \setminus V_0$ associated with the preorder $\sqsubseteq$. In other words, $v \sqsubseteq w$, $w \sqsubseteq v$ iff there is $1 \leq i \leq n$ such that $v, w \in V_i$. Observe that the classes $V_1, \ldots, V_n$ can be indexed such that:

(T0*) If $v \in V_i$, $w \in V_j$, $v \sqsubseteq w$ then $i \leq j$.

T1 If $v \sqsubseteq w$ and $v \not\leq w \in \mathcal{S}$, for some $v, w \in V$, then return $FAILURE$.

T2 If $t \leq v \in \mathcal{S}$, $s \not\leq w \in \mathcal{S}$, $v \sqsubseteq w$, $s \trianglelefteq t$, for some $v, w \in V$ and some $t, s \in R[V]$, then return $FAILURE$.

The tests T1, T2 are clearly necessary for the satisfiability of $\mathcal{S}$ in a model of $\mathcal{O}_{IT}$. The following Theorem proves that they are also sufficient.

Theorem 4.1 *Let $\mathcal{S}$ be a reduced system of formulas with pointers and variables V. If the tests* T1–T2 *do not fail on $\mathcal{S}$ then $\mathcal{S}$ has solution in $RT[X]$ where X is any set of cardinality greater or equal to the cardinality of V.*

Proof: It is clear that it is sufficient to prove the satisfiability of $\mathcal{S}$ in $RT[V]$. To be more clear, we fix a set X bijective to V and some bijection $v \mapsto x^v$ from V to X. Assume that V be partitioned into $V_0, V_1, \ldots, V_n$ as it is described in T0. Let $X_0, X_1, \ldots, X_n$ be the corresponding partition on

X under the fixed bijection. Denote $V_{\leq i} = \bigcup_{j \leq i} V_j$, $X_{\leq i} = \bigcup_{j \leq i} X_j$ for $i = 0, \ldots, n$. We will define substitutions $\gamma_i : R[V] \to R[V \cup X]$ for $i = 0, \ldots, n$ such that all the following conditions (Ci) are satisfied.

$(Ci)_1$	$var(v\gamma_i)$	$\subseteq$	$X_{\leq i}$	for $v \in V_{\leq i}$ and $v\gamma_i = v$ otherwise;
$(Ci)_2$	$t\gamma_i$	$\trianglelefteq$	$v\gamma_i$	for all $t \in R[V]$, $v \in V_{\leq i}$ such that $t \leq v \in \mathcal{S}$;
$(Ci)_3$	$s\gamma_i$	$\not\trianglelefteq$	$v\gamma_i$	for all $s \in R[V]$, $v \in V$ such that there is $w \in V$ and $s \not\leq w \in \mathcal{S}$, $v \sqsubseteq w$;
$(Ci)_4$	$s\gamma_i$	$\not\trianglelefteq$	$t\gamma_i$	for all $s \not\leq w \in \mathcal{S}$, $t \leq v \in \mathcal{S}$ such that $v \sqsubseteq w$;
$(Ci)_5$	$u\gamma_i$	$\not\sim$	$v\gamma_i$	for all $v \in V$, $u \in R[V]$ such that $u \neq v \in \mathcal{S}$.

Observe that by the Remark 2.7, the substitution γ_n gives a solution of the system $\mathcal{S}$ in $RT[X]$.

First, we define γ_0 by $v\gamma_0 = x^v$ if $v \in V_0$ and $v\gamma_0 = v$ otherwise. Then $(C0)_1$ is true by the definition of γ_0; $(C0)_2$ is true by emptiness; $(C0)_3$ is true because of T1; $(C0)_4$ is true because of T2; $(C0)_5$ is true because $v \neq v \notin \mathcal{S}$ and $u \sim v$ implies $u = v$, when v is a variable.

Then, we assume to have defined γ_{i-1} satisfying the condition $C(i-1)$ for $i > 0$ and we define γ_i as follows. We fix a function symbol f in the signature of arity greater than one. To simplify notation we assume that f is of arity two. Otherwise we may do a similar proof with the binary term $f(v_1, \ldots, v_1, v_2)$.

Let $L = (t_1, \ldots, t_p)$ be a list of elements of $R[V \cup X]$ and $x \in X$. Then define, by induction on p, a syntactic term $\langle x, L\rangle \in R[V \cup X]$ as follows (see Fig. 1) $\langle x, L\rangle = f(x, u_p)$ where $u_0 = x$, $u_i = f(t_i, u_{i-1})$ for $1 \leq i \leq p$. The terms $u_0, \ldots, u_p$ will be called *principal subterm* of $\langle x, L\rangle$.

Let now $M_i = \{t\gamma_{i-1} : t \leq v \in \mathcal{S} \text{ for some } v \in V_i\}$ and L_i be a list of all the terms in M_i. Observe that, by (T0*) and by $(Ci-1)_1$, we have

(4.1) $$M_i \subseteq R[V_i \cup X_{\leq(i-1)}]$$

Then, as we said in Remark 1.7, it is possible to compute $\tau_i^v \in R[X_{\leq i}]$ such that

(4.2) $$\tau_i^v \sim \langle x^v, L_i\rangle \rho_i \quad \text{for every } v \in V_i ,$$

where $\rho_i = [\tau_i^v / v : v \in V_i]$.

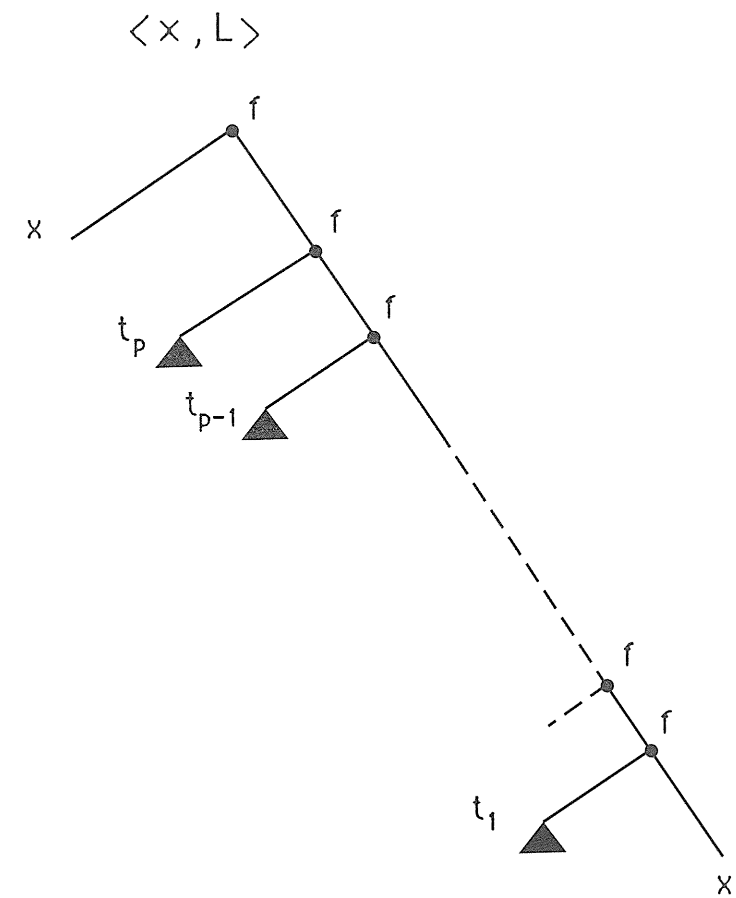

Fig. 1

Hence, we define

(4.3) $$v\gamma_i = \begin{cases} \tau_i^v & \text{if } v \in V_i \\ v\gamma_{i-1} & \text{if } v \in V \setminus V_i \end{cases}$$

We now claim the following properties:

(CL1) $\gamma_i = \gamma_{i-1}\rho_i$;

(CL2) if $t\gamma_{i-1} \in M_i$ then $t\gamma_i \trianglelefteq \tau^v$, for every $v \in V_i$;

Let $H = \{s | \ s \in R[V \cup X],\ var(s) \cap X_i = \emptyset\}$ then

(CL3) ρ_i is injective (modulo $\sim$) on H, (CL4) $s\rho_i \sim u\rho_i$ is impossible if $s \in H$ and u is a principal subterm of $\langle x^v, L_i\rangle$ for some $v \in V_i$.

Proof of (CL1): By $(Ci-1)_1$ and by definition of ρ_i and γ_i.

Proof of (CL2): By definition $t\gamma_{i-1} \trianglelefteq \langle x^v, L_i\rangle$. Hence

$$t\gamma_i = t\gamma_{i-1}\rho_i \trianglelefteq \langle x^v, L_i\rangle\rho_i \sim \tau_i^v .$$

Proof of (CL3): It is sufficient to verify (1i) of Corollary 3.2. So, assume

$$(4.4) \qquad t\rho_i \sim z\rho_i \qquad \text{for } t \in H, \quad z \in var(H) .$$

We may distinguish three cases.

Case 1: $z \notin V_i$. Then $z\rho_i = z$. Hence, by (4.4) and the definition of ρ_i, $t = z$.

Case 2: $z \in V_i$ and t is a variable. Then we may assume that $t \in V_i$, otherwise, by symmetry, we are in Case 1. So, (4.4) implies $\tau_i^t \sim \tau_i^z$. This implies $x_i^t = x_i^z$. Hence, $t = z$.

Case 3: $z \in V_i$ and t is not a variable. Then, by the definition of τ_i^z, we have $x^z = (t/\!/1)\rho_i$. This is impossible since $var(t) \cap X_i = \emptyset$.

Proof of (CL4): Assume u to be a principal subterm of $\langle x^v, L_i\rangle$ for some $v \in V_i$. Then, $u = u_q$, where $u_0 = x^v$ and $u_k = f(t_k, u_{k-1})$, for every $0 < k \le q$ and some t_k in the list L_i. Now, we prove a contradiction assuming

$$(4.5) \qquad s\rho_i \sim u_q\rho_i \qquad \text{for some } s \in H.$$

The proof is by induction on q. If $q = 0$ then (4.5) implies $s\rho_i \sim x^v$. This implies $s = x^v$ which is impossible since $x^v \in X_i$. If $q > 0$ then $u_q = f(t_q, u_{q-1})$, where $var(t_q) \cap X_i = \emptyset$. Now, we distinguish three cases.

Case 1: s is a variable not in V_i. Then, (4.5) implies $s \sim u_q\rho_i$. Hence, $x^v \in var(s)$. This is impossible because $s \in H$.

Case 2: $s \in V_i$. Then, (4.5) implies $x^s = t_q\rho_i$. This is impossible because $var(t_q) \cap X_i = \emptyset$.

Case 3: s is not a variable. Then (4.5) implies $(s/\!/2)\rho_i = u_{q-1}$. This is impossible by inductive hypothesis.

Now, we are able to prove the conditions (Ci).

Proof of $(Ci)_1$. This follows from $(Ci-1)_1$ and (4.3).

Proof of $(Ci)_2$. This follows from $(CL2)$.

Proof of $(Ci)_3$. We take $v, w \in V$, $s \in R[V]$ such that $s \not\leq w \in \mathcal{S}$, $v \sqsubseteq w$. Moreover, we assume

$$(4.6) \qquad s\gamma_i \trianglelefteq v\gamma_i$$

Then we prove a contradiction by distinguishing three cases.

Case 1: $v \in V_k$, $k < i$. Then $v\gamma_i = v\gamma_{i-1}$. Hence, (4.6) implies $var(s\gamma_i) \subseteq X_{\le(i-1)}$. Therefore, $var(s) \cap V_i = \emptyset$. Hence, $s\gamma_i = s\gamma_{i-1}$. Thus, (4.6) contradicts $(Ci-1)_3$.

Case 2: $v \in V_i$. Then $v\gamma_i = \tau_i^v$. Now, looking at the definition of τ_i^v (see Fig. 1 and (4.6)), we have that $r \trianglelefteq \tau_i^v$ implies either $r \sim \tau_i^u$ for some $u \in V_i$ or $r \sim z\rho_i$ for some principal subterm z of $\langle x_i^u, L_i\rangle$ and some $u \in V_i$ or $r \sim z\rho_i$ for some $z \trianglelefteq t\gamma_{i-1}$ and some $t\gamma_{i-1} \in M_i$. Therefore, by Claim (CL4) we have to examine only two subcases.

Subcase 2.1: $s\gamma_i \sim \tau_i^u$ for some $u \in V_i$. Then, by (4.3), $(CL1)$, $(Ci-1)_1$ and $(CL3)$ we have $s\gamma_{i-1} \sim u\gamma_{i-1}$. Moreover, $u \sqsubseteq v$ by definition of V_i. This contradicts $(Ci-1)_3$.

Subcase 2.2: There exist $t\gamma_{i-1} \in M_i$ and $z \trianglelefteq t\gamma_{i-1}$ such that $s\gamma_i \sim z\rho_i$. Then, $var(s\gamma_{i-1}, z) \cap X_i = \emptyset$ by $(Ci-1)_1$. Hence by $(CL1)$ and $(CL3)$ we have $s\gamma_{i-1} \sim z$. Therefore, $s\gamma_{i-1} \trianglelefteq t\gamma_{i-1}$. This contradicts $(Ci-1)_4$.

Case 3: $v \in V_k$, $k > i$. Then $v\gamma_i = v$. Hence, (4.6) implies $s = v$. So, we have $v \not\leq w \in \mathcal{S}$ and $v \sqsubseteq w$. This is impossible by the test T1.

Proof of $(Ci)_4$. Let $t \le v \in \mathcal{S}$, $s \not\leq w \in \mathcal{S}$ and $v \sqsubseteq w$. Assume by hypothesis to be contradicted that

$$(4.7) \qquad s\gamma_i \trianglelefteq t\gamma_i$$

Then, only two cases can occur by $(CL1)$.

Case 1: There is $z \trianglelefteq t\gamma_{i-1}$ such that $s\gamma_i \sim z\rho_i$. Then, by $(CL3)$, we have $s\gamma_{i-1} \trianglelefteq t\gamma_{i-1}$. This is impossible by $(Ci-1)_4$.

Case 2: There exists $u \in var(t) \cap V_i$ such that $s\gamma_i \trianglelefteq \tau_i^u$. Then $u \sqsubseteq v \sqsubseteq w$. So, (4.7) implies $s\gamma_i \trianglelefteq u\gamma_i$ where $u \sqsubseteq w$ and $s \not\leq w \in \mathcal{S}$. This is impossible by $(Ci)_3$ which was already proved.

Proof of $(Ci)_5$. This is immediate by $(CL3)$ and $(Ci-1)_5$.

5 Solving reduced systems in RT

When $\mathcal{S}$ is a reduced system in the variables V Theorem 4.1 gives criteria to solve $\mathcal{S}$ in $RT[X]$ where X has cardinality not less than V. In this Section we first prove that every solution $\gamma : R[V] \to R[X]$ can be composed with a preorder morphism $\eta : R[X] \to R[y]$ to obtain a solution of $\mathcal{S}$ in the rational trees with a single indeterminate y. This gives necessary and sufficient conditions for the solvability of $\mathcal{S}$ in some model of the theory $\mathcal{O}_{IT}$ (see Theorem 5.7). Then, we look for a solution δ in the rational terms by taking $\delta = \gamma\eta\beta$, where $\beta : R[y] \to R[\emptyset]$. When the signature S is not singular a such β exists for any system and, when S is singular, a condition on the reduced system $\mathcal{S}$ must be satisfied; moreover, the construction of β is different. Hence, we have that the existential theories of $(RT[y], \leq)$ and $(RT, \leq)$ are equal if and only if the signature is not singular. Moreover, we have decidability conditions for the existential theory of $(RT, \leq)$ also in singular signature.

Before the main result, we give a definition and we prove some technical lemmas.

Definition 5.1 *Let $t \in R[V]$ be an term. We define the* size *of t, denoted $\|t\|$, by*

$$\|t\| = \min\{depth(s) \ : \ s \in R[V], \ s \sim t\}$$

where $depth(s)$ is $\max\{|p| : p \in Occ(s)\}$ and $|p|$ denotes the length of the word p. If Φ is a syntactic object then $\|\Phi\|$ denotes the maximum size of the terms which appears in Φ.

Remark 5.2 *By definition, $t \sim s$ implies $\|t\| = \|s\|$. So, we may define unambiguously the size $\|\hat{t}\|$ of every rational term $\hat{t} \in RT[V]$.*

Remark 5.3 *Let t be a finite term. Then $\|t\| = depth(t)$. So, for every $m \leq \|t\|$ there exists some subterm s of t such that $\|s\| = m$; moreover, $s \trianglelefteq t$ and $\|s\| = \|t\|$ implies $s = t$. The properties fail when t is in $R[V]$ and not in $FT[V]$.*

Here we use a fixed function symbol f of arity greater than 2. To simplify notation we may assume that f is binary otherwise we could use the binary term $f(v_1, \dots, v_1, v_2)$.

Lemma 5.4 *Let X be a finite set. Then, for every $m \geq |X|$ there exists an injective map from X to $FT[y]$, say $x \mapsto h^x$, such that*

(i) *The morphism $\eta : RT[X] \to RT[y]$ determined by the substitution $[h^x/x : x \in X]$ is injective and a preorder morphism (modulo $\sim$).*

(ii) *If $t \in Range(\eta)$ then either $y \notin var(t)$ or $f(y, y) \trianglelefteq t$.*

(iii) *Let $\beta : FT[y] \to FT$ be any substitution. Then the elements $\{x\eta\beta : x \in X\}$ are pairwise distinct and of the same size $m + 1 + \|y\beta\|$.*

Proof: Assume $X = \{x_1, \dots, x_n\}$. Let $x_0, x_{n+1}, \dots, x_m$ be new indeterminates. For $i = 0, 1, \dots, m$ define inductively $k_i \in FT[x_0, \dots, x_m]$ by

$$k_0 = f(x_0, x_0), \quad k_i = f(x_i, k_{i-1}), \quad \text{for } 1 \leq i \leq m. \tag{5.1}$$

Then, put

$$h^{x_i} = k_m[f(y, y)/x_i, \ y/x_j : \ 0 \leq j \leq m, \ j \neq i] \quad \text{for } 1 \leq i \leq n. \tag{5.2}$$

Proof of (i). We use the Corollary 3.2. So, assume $t\eta \sim x\eta$. Then $t\eta \in FT[y]$ and $t\eta = h^x$. So, t must be some variable in X. Hence, by construction (5.2) (see Fig. 2), $t = x$. Now, assume $t\eta \trianglelefteq x\eta$. Then $var(t) \neq \emptyset$, otherwise $\Lambda \trianglelefteq h^x$ for some constant symbol in the signature S. Let $z \in var(t)$. Then $z\eta \trianglelefteq t\eta \trianglelefteq x\eta$. Since all h^u, for $u \in X$, have the same depth, we have that $z = x$ and $x\eta = t\eta$. Hence, $t = x$ by the injectivity of η.

Proof of(ii). Let $t = s\eta$. Then $var(s) = \emptyset$ implies $y \notin var(t)$ and $var(s) \neq \emptyset$ implies $f(y, y) \trianglelefteq t$.

Proof of (iii). Assume $x_i\eta\beta = x_j\eta\beta$ and $i \neq j$. Then $h^{x_i}\beta = h^{x_j}\beta$. So, by definition (5.2) (see Fig. 2), we have $f(y\beta, y\beta) = y\beta$. This is impossible because $y\beta \in FT$. Moreover, the definitions (5.1), (5.2) imply that $\|h^{x_i}\beta\| = \|h^{x_i}\| + \|y\beta\| = m + 1 + \|y\beta\|$ for every $1 \leq i \leq n$.

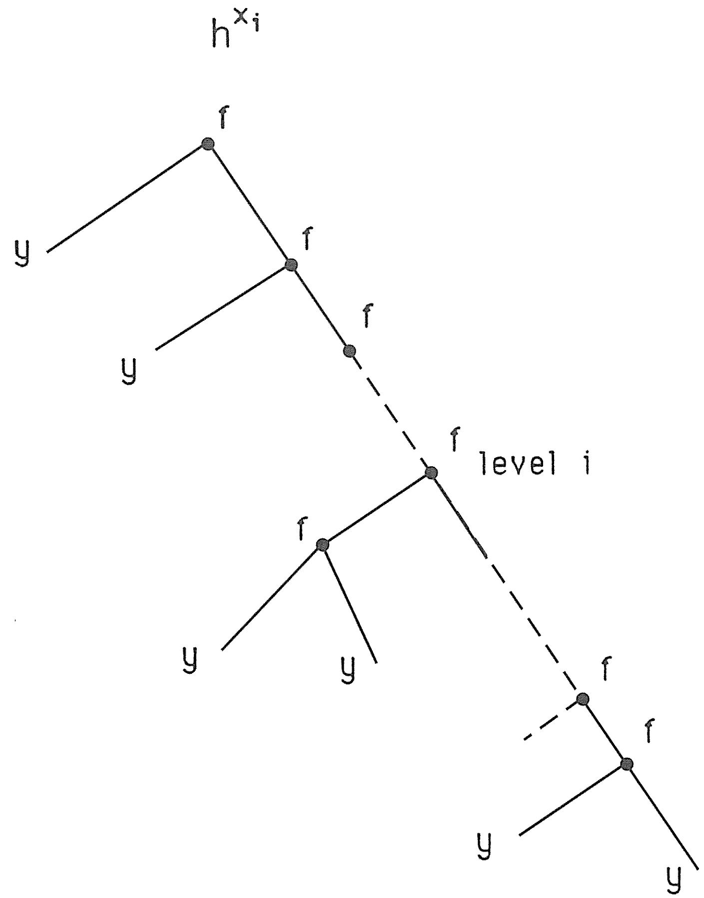

Fig. 2

Lemma 5.5 *Let* Λ *be a fixed constant symbol in the signature. Then for every positive integer* m *there exists a* $b_m \in R[\emptyset]$ *such that for all* $u, v, d \in R[\emptyset]$

(i) $f(u,v) \trianglelefteq b_m$ *implies* $u = \Lambda$ *or* $v = \Lambda$;

(ii) $d \trianglelefteq b_m$ *implies* $d = \Lambda$ *or* $\|d\| > m$;

(iii) *Let* $H \subseteq R[y]$ *be closed under subterms and* $\|H\| < m$. *Then* $\beta = [b_m/y]$ *is injective (modulo* $\sim$*) on* H.

Proof: We define a function $t : \{1,2\}^* \longrightarrow FT[\Omega]$, where Ω is an indeterminate, by induction as follows

$$(5.3) \qquad \begin{aligned} t_\varepsilon &= \Omega\,, \\ t_{q1} &= t_q[f(\Omega,\Lambda)/\Omega]\,, \\ t_{q2} &= t_q[f(\Lambda,\Omega)/\Omega]\,, \end{aligned}$$

where ε is the empty word. Then, for every $p \in \{1,2\}^*$ we have (see Fig. 3)

$$(5.4) \qquad t_p(q) = f \quad \text{iff} \quad q \prec p \qquad \text{for every } q \in Occ(t_p);$$

$$(5.5) \qquad t_p(r) = \Lambda \quad \text{iff} \quad \text{not } r \preceq p \quad \text{for every } r \in Occ(t_p);$$

$$(5.6) \qquad p \in Occ(t_p) \quad \text{and} \quad t_p(p) = \Omega\,.$$

Now, we define the element $b_m \in R[\emptyset]$ by $b_m = (t_\sigma)^\Omega_\uparrow$ where σ is the word $121221\ldots12^{(i)}1\ldots12^{(m)}$. Then $\hat{b}_m$ is a rational tree such that

$$(5.7) \qquad \text{every subtree } \hat{d} \text{ of } \hat{b}_m \text{ is } \Lambda \text{ or } \hat{b}_m/p \quad \text{for some } p \preceq \sigma\,,$$

by (5.4), (5.5) and (5.6). Moreover,

$$(5.8) \qquad \|d\| > m \qquad \text{if } d \neq \Lambda$$

since $\hat{d}$ has a chain of more than m subtrees. In fact, by definition of b_m, $\hat{b}_m/r \neq \hat{b}_m/q$ for all $r \prec q \prec \sigma$.

Now, by definition (5.3), $f(u,v) \trianglelefteq t_p$ implies $u = \Lambda$ or $v = \Lambda$. This entails a proof (i). The proof of (ii) follows from (5.7) and (5.8). For the proof of (iii) we use Corollary 3.2 as follows. Assume that $s\beta \sim y\beta$ and $s \neq y$ for $s \in H$. Then, $s^y_\uparrow \sim b_m$ by Remark 1.7. Therefore, $\|b_m\| = \|s^y_\uparrow\| \leq \|s\| < m$. This is impossible by (5.8).

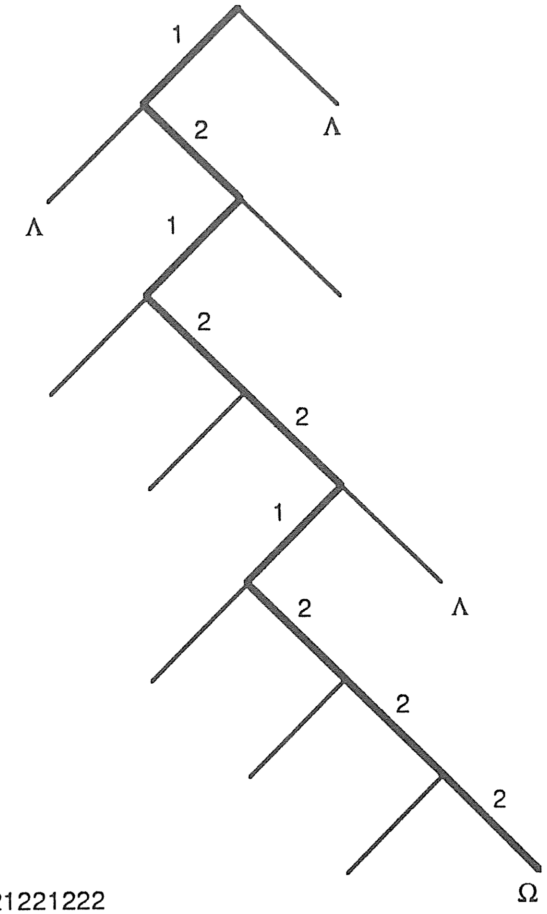

Fig. 3

p = 121221222

Lemma 5.6 *Assume that the signature has two function symbols f, g of positive arity, where f is the binary term used in the previous lemmas. Then, for every positive integer m, there exists $b_m \in RT$ such that*

(i) $f(b_m, b_m) \not\trianglelefteq b_m$;

(ii) $d \trianglelefteq b_m$ *implies* $\|d\| > m$;

(iii) *Let $H \subseteq R[y]$ be closed under subterms and $\|H\| < m$. Then $\beta = [b_m/y]$ is injective (modulo $\sim$) on H.*

Proof: Firstly we define, by induction on the natural number k, the finite terms $g^{(k)}$, $t^{(k)}$ as follows (see Fig. 4)

$$\begin{aligned} g^{(0)} &= \Omega, & g^{(k+1)} &= g^{(k)}[\Omega/g(\Omega,\ldots,\Omega)]\,, \\ t^{(0)} &= \Omega, & t^{(k+1)} &= t^{(k)}[\Omega/f(g^{(k)},\ldots,g^{(k)})]\,. \end{aligned}$$

Then, we define $b_m = (t^{(m)})^{\Omega}_{\uparrow}$. By construction $b_m(\varepsilon) = f$ and $f(d,e) \trianglelefteq b_m$ implies $d(\varepsilon) = g$, $e(\varepsilon) = g$. Hence (i) holds. Property (ii) holds since on each branch of b_m there exists a chain of more than m subtrees. The proof of (iii) is quite analogous to the proof of (iii) of the previous Lemma 5.5.

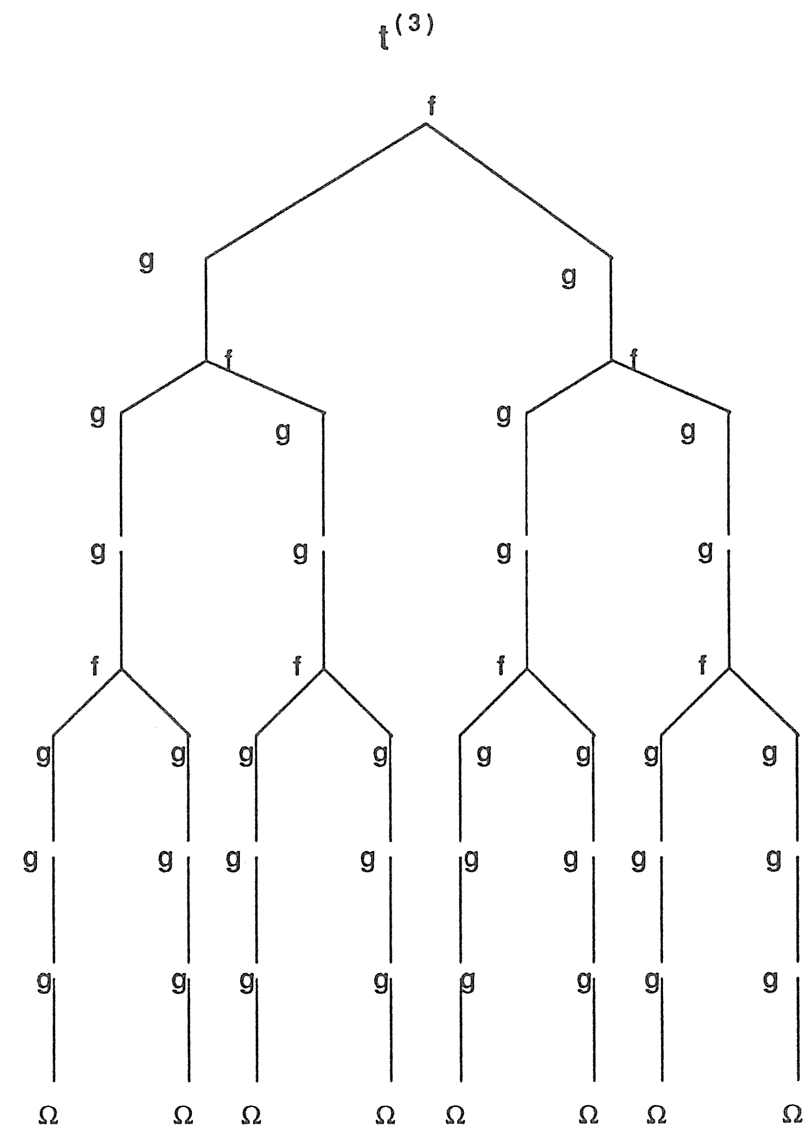

Fig. 4

Theorem 5.7 *Let $\mathcal{S}$ be a reduced system of atomic formulas with pointers in the signature S and with $var(\mathcal{S}) = V$. Then* (i)—(iii) *are equivalent*

(i) *$\mathcal{S}$ has solution in some model of $\mathcal{O}_{IT}$;*

(ii) *The tests* T1, T2 *do not fail on $\mathcal{S}$;*

(iii) *$\mathcal{S}$ has solution in $RT[y]$.*

Moreover, let S_0 be the (non empty) set of constant symbols in S. Assume either that S is non singular, i.e. $|S \setminus S_0| \geq 2$, or $S_0 \neq C_v$ for all $v \in V$, where $C_v = \{\Lambda : \Lambda \in S_0, (\exists w \in V)\ v \sqsubseteq w,\ \Lambda \not\leq w \in \mathcal{S}\}$. Then (i)—(v) *are equivalent, where*

(iv) *$\mathcal{S}$ has solution in RT;*

(v) *$\mathcal{S}$ has solution in every model of $\mathcal{O}_{IT}$.*

Proof: (i)→(ii), (iii)→(i) are clear.
(ii)→(iii). Let $V = var(\mathcal{S})$ and assume (ii). Then, Theorem 4.1 proves that there is some X and some substitution $\gamma : R[V] \to R[X]$ which gives a solution for $\mathcal{S}$ in $RT[X]$. Let $m = |X|$ and $\eta : R[X] \to R[y]$ be defined as in Lemma 5.4. Then, the substitution $\delta = \gamma\eta$ gives a solution in $RT[y]$ since η is injective and preorder morphism (modulo $\sim$) (see Remark 2.7).

Now, we assume (ii) and we fix a solution $\gamma : R[V] \to R[X]$ as in Theorem 4.1. The we split the further assumption in two parts and in either cases we prove (iv).

ASSUMPTION 1: S is *non singular*. Say f the fixed (binary) symbol used in the construction of γ. Let $\eta : R[X] \to R[y]$ be the morphism given in Lemma 5.4. Thus, as we proved before, $\delta = \gamma\eta$ is a solution for $\mathcal{S}$. Let K be the set of terms with pointers which appears in $\mathcal{S}$. Let H be the set of subterms of terms in $K\delta$. Fix an integer $m > \|H\|$, compute $b_m \in R[\emptyset]$ as in Lemma 5.6 and let $\beta : R[y] \to R[\emptyset]$ be defined by $\beta = [b_m/y]$. Now, we claim the following

(5.9) β is injective (modulo $\sim$) on H,

(5.10) β is a preorder morphism (modulo $\sim$) on $K\delta$.

After (5.9)–(5.10) we prove that $\delta\beta$ is a solution for $\mathcal{S}$, hence (iv), as follows. If $t \leq v \in \mathcal{S}$ then $t\delta\beta \trianglelefteq v\delta\beta$ because δ is a solution and β is a morphism. If $r \neq u \in \mathcal{S}$ then $r\delta \not\sim u\delta$ because δ is a solution and (5.9). Finally, if $s \not\leq w \in \mathcal{S}$ then $s\delta\beta \not\trianglelefteq w\delta\beta$ because δ is a solution and (5.10).

Proof of (5.9) is by (iii) of Lemma 5.6. To prove (5.10) we may use (2i) of Corollary 3.2. Hence, we prove that the assumption

(5.11) $t\beta \trianglelefteq y\beta$ and $y \neq t$, for some $t \in K\delta$

leads to contradiction. We assume (5.9) and we distinguish two cases.

Case 1: $y \notin var(t)$. Then $t\beta = t$. So, by (5.11) $t \trianglelefteq b_m$ and $\|t\| < m$. This contradicts (ii) of Lemma 5.6.

Case 2: $y \in var(t)$. Since $t \in K\delta$ and $Range(\delta) = Range(\gamma\eta) \subseteq Range(\eta)$, by (ii) of Lemma 5.4, we have $f(y, y) \trianglelefteq t$. Therefore, (5.11) implies $f(b_m, b_m) \trianglelefteq b_m$. This contradicts (i) of Lemma 5.6.

ASSUMPTION 2: $S_0 \neq C_v$, for every $v \in V$. Firstly we define a morphism $\theta : R[X] \to R[X]$. For every $x \in X$ let h^x be the term in $R[y]$ as in Lemma 5.4, i.e. $h^x = x\eta$. Put $x\theta = h^x[x/y]$. Then, in complete analogy with the proof of Lemma 5.4, we have

(5.12) θ is injective and a preorder morphism (modulo $\sim$);

(5.13) if $t \in Range(\theta)$ and $x \in var(t)$ then $f(x, x) \trianglelefteq t$.

Now, $\delta = \gamma\theta$ is a solution of $\mathcal{S}$ since γ is a solution and (5.12). Then, let us look at the inductive definition of γ in the proof of Theorem 4.1. By the definition of γ_0 and by (4.3), (4.2) and (4.1) it is possible to prove by induction on i that, for every $u \in V$, if $x^u \in var(v\gamma_i)$ then $u \sqsubseteq v$. Therefore, by $\gamma = \gamma_n$ and by the definition of θ we have

(5.14) $x^v \in var(w\delta)$ implies $v \sqsubseteq w$, for all $v, w \in V$.

Now, let K be the set of terms with pointers in $\mathcal{S}$, H be the set of subterms of terms in $K\delta$ and H_0 be $K\delta \setminus S_0$. By Assumption 2 we can choose, for every $v \in V$, a constant symbol $\Lambda_v \in S_0 \setminus C_v$. Then, fix an integer $m > \|H\|$ and define b^v_m as in Lemma 5.5 with respect to the constant symbol Λ_v. Moreover, let $\beta : R[X] \to R[\emptyset]$ be defined by $x^v\beta = b^v_m$. Now, along the line pursued before, we prove

(5.15) β is injective (modulo $\sim$) on H;

(5.16) β is a preorder morphism (modulo $\sim$) on H_0.

After (5.15)–(5.16) we prove that $\delta\beta$ is a solution for $\mathcal{S}$, hence (iv), as follows. If $t \leq v \in \mathcal{S}$ then $t\delta\beta \trianglelefteq v\delta\beta$ because δ is a solution and β is a morphism. If $r \neq u \in \mathcal{S}$ then $r\delta \not\sim u\delta$ because δ is a solution and (5.15). If $s \not\leq w \in \mathcal{S}$ then we distinguish two cases.

Case 1: $s \notin S_0$. Then $\{s\delta, w\delta\} \subseteq H_0 = K\delta \setminus S_0$. So, $s\delta\beta \not\trianglelefteq w\delta\beta$ because δ is a solution and (5.16).

Case 2: $s \in S_0$. Then, $s\delta\beta \trianglelefteq w\delta\beta$ would imply $s \trianglelefteq w\delta\beta$. But, $s = s\delta \not\trianglelefteq w\delta$ because δ is a solution. So, there exists $x^v \in var(w\delta)$ such that $s \trianglelefteq x^v\beta$. Hence, $s = \Lambda_v$ by construction of b^v_m and $v \sqsubseteq w$ by (5.14). Thus, $\Lambda_v \not\leq w \in \mathcal{S}$ and $v \sqsubseteq w$. This would imply $\Lambda_v \in C_v$ which contradicts the definition of Λ_v.

Proof of (5.15). We use (1i) of Corollary 3.2. Hence we assume $t\beta = v\beta = b^v_m$ for some term t in H. If $x^w \in var(t)$ then $b^w_m \trianglelefteq b^v_m$, hence $b^w_m = b^v_m$. So, by (iii) of Lemma 5.5, we have $t = v$.

Proof of (5.16). We use (2i) of Corollary 3.2. Hence, we prove that the assumption

(5.17) $t\beta \trianglelefteq x^v\beta$ and $x^v \neq t$, for some $t \in H_0$

leads to contradiction. We assume (5.17) and we distinguish two cases.

Case 1: $var(t) = \emptyset$. Then $t\beta = t$ and, by (5.17), $t \trianglelefteq b_m$ and $\|t\| < m$. So, by (ii) of Lemma 5.5 we have that $t = \Lambda_v$. This is impossible since $\Lambda_v \notin H_0$.

Case 2: $var(t) \neq \emptyset$. Let $x^w \in var(t)$. Since $t \in K\delta$ and $Range(\delta) = Range(\gamma\theta) \subseteq Range(\theta)$, by (5.13) we have $f(x^w, x^w) \trianglelefteq t$. Therefore, (5.17) implies $f(b_m, b_m) \trianglelefteq b_m$ which contradicts (i) of Lemma 5.5.

Remark 5.8 *Observe that the reduced system*

$$\{v \leq w, \quad \Lambda_1 \not\leq v, \quad \Lambda_2 \not\leq w, \quad f(v,v) \neq v\}$$

in the singular signature $\{\Lambda_1, \Lambda_2, f\}$ *has no solutions in* RT, *but* $[y/v, y/w]$ *is a solution in* $RT[y]$. *Therefore, the extra condition to prove* (iii)$\to$(iv) *in Theorem 5.7, is necessary.*

Moreover, observe that when $C_v = S_0$ *and the signature* $S = S_0 \cup \{f\}$ *is singular then any possible solution for the system* $\mathcal{S}$ *in* RT *must assign to* v *the full* k*-ary tree, if* k *is the arity of* f. *So, if* $\sigma : V \to R[\emptyset]$ *defines a solution then* $\sigma(v) \sim f(1, \ldots, 1)$.

The above remarks and Theorem 5.7 prove that the existential theory of $(RT, \leq)$ *can be decided by the following procedures. They are different for a singular and non singular signature. The termination of the procedures is clear.*

test(Φ) {*where* Φ *is a quantifier-free formula* }
  if Reduce(Φ) *does not fail and returns* $\bigvee \mathcal{S}_i$
  then *for every* i test1($\mathcal{S}_i$)
  else *return* not SATISFIABLE.

test1($\mathcal{S}$) {*where* $\mathcal{S}$ *is a reduced system* }
  if T1–T2 *fail*
  then *return* not SATISFIABLE
  else *distinguish the cases*
    Case 1: S *is* non singular. *Return* SATISFIABLE
    Case 2: S singular.
      if $S_0 = C_v$ *for some variable* v
      then test($\mathcal{S}[v/f(1, \ldots, 1)]$)
      else *return* SATISFIABLE.

6 Venkataraman Theorem Revisited

Following the lines of the proof for the decision of existential sentences of theory $Th(RT, \leq)$, we can give an analogous proof for the decision of the existential sentences of $Th(FT, \leq)$. The latter result was obtained by Venkataraman in [Ven87]. Our proof is straightforward after the technique developed in the previous sections.

Remark 6.1 *The satisfiability problem for existential sentences in models of $\mathcal{O}_{FT}$ can be solved by means of a test for the satisfiability of reduced systems. Such systems will, of course, contain no pointers. In fact, there is an analogous procedure to the one given in Section 3. We describe below the slight modifications.*

Formulas $t = v$, $t \leq v$, where $v \in var(t)$ and t is different from v, have to be classified as *incoherent* formulas. Therefore, formulas $t \neq v$, $t \not\leq v$, where t, v are as before, have to be classified trivial. Moreover, only the substitutions $[t/v]$, where $v \notin var(t)$, are allowed.

Now, it is clear that the modified procedure transforms quantifier-free formulas of $\mathcal{L}_{\leq}$ into a disjunction of reduced systems. Furthermore, the transformation is correct with respect to the satisfiability of the input and output formulas in models of $\mathcal{O}_{FT}$.

Remark 6.2 *Let $\mathcal{S}$ be a reduced system of atomic formulas of $\mathcal{L}_{\leq}$. Then, analogously as in Section 4, we may test the satisfiability of $\mathcal{S}$ in a model of $\mathcal{O}_{FT}$ as follows.*

The tests T1, T2 remain the same, but in T0 we have to put the controls

T0′: Do as in T0, compute the relation $\rightarrow$ on $var(\mathcal{S})$. If $v \rightarrow v$ and $t \leq v \in \mathcal{S}$ for some $v \in var(\mathcal{S})$ and some term $t \notin var(\mathcal{S})$ then return $FAILURE$;

T0″: After T0′, for all different variables v, w with $v \rightarrow w$ and $w \rightarrow v$ apply the substitution $[v/w]$ and cancel the trivial formulas. If there are incoherent formulas the return $FAILURE$.

The test T0′ is correct by the Occur-check Axiom of $\mathcal{O}_{FT}$ and T0″ is correct by the antisymmetric property of the partial order. So, by T0″ the equivalence classes $V_1, \ldots, V_n$ are singletons. Moreover, if $t \leq v \in \mathcal{S}$ and

$v \in V_i$ then, by the property (T0*), $var(t) \subseteq V_1 \cup \ldots \cup V_{i-1}$. This forces the necessarily unique term τ_i^v defined in (4.2) to be in $FT[X_{\leq i}]$. Thus, the following Theorem can be proved along the proof of Theorem 4.1.

Theorem 6.3 *Let $\mathcal{S}$ be a reduced system of atomic formulas with variables in V. Assume that the tests* T0′, T0″, T1, T2 *do not fail on on $\mathcal{S}$. Then there is a substitution $\gamma : FT[V] \rightarrow FT[X]$, where X is bijective to V, such that*

(a) *γ solves $\mathcal{S}$ in $FT[X]$;*

(b) *$x^v \in var(v\gamma)$ and not $v\gamma = x^v$, i.e. $x^v < v\gamma$, for every $v \in V$.*

Here, $v \mapsto x^v$ is a bijection from V to X.

Corollary 6.4 *Let $\mathcal{S}$ be a reduced system of atomic formulas. Then, the following are equivalent*

(i) *$\mathcal{S}$ has solution in some model of $\mathcal{O}_{FT}$;*

(ii) *The tests* T0′, T0″, T1, T2 *do not fail on $\mathcal{S}$;*

(iii) *$\mathcal{S}$ has solution in $FT[y]$.*

Now, we give a procedure for testing the solvability of a system $\mathcal{S}$ in FT. Then we prove its correctness. We denote by $Size(r)$ the set of terms t in FT such that $\|t\| = r$.

Procedure $sat(\mathcal{S})$

Case 1: $var(\mathcal{S}) = \emptyset$. $\mathcal{S}$ is $SATISFIABLE$ in FT iff all sentences in $\mathcal{S}$ are true in FT.

Case 2: $var(\mathcal{S}) = V \neq \emptyset$.

2a) **if** $\mathcal{S}$ is not reduced **then** compute a disjunction $\bigvee \mathcal{S}_i$ of reduced systems with the procedure described in Remark 2.1; return $SATISFIABLE$ iff, for some i, $sat(\mathcal{S}_i)$ does it.

2b) **If** the tests T0′, T0″, T1, T2 fail on $\mathcal{S}$ **then** return $FAILURE$.

2c) For every $v \in V$ put $G_v = \{s | s \in FT,\ s \not\leq v \in \mathcal{S}\}$

and let $r = 1 + \max\{\|s\| :\ s \in \bigcup_{v \in V} G_v\}$.

2d) Compute the Occur-check relation $\sqsubseteq$ on V.

Case 2.1: $(\exists v \in V)(\forall b \in Size(r))(\exists w \sqsupseteq v)(\exists s \in G_w)\,(s \leq b)$.

Choose a witness $v \in V$ for the above formula
and return $SATISFIABLE$ iff for some $u \in FT$,
$\|u\| < r$, $sat(\mathcal{S}[u/v])$ does it.

Case 2.2: not case 2.1. Return $SATISFIABLE$.

Correctness of Case 1 is clear; 2a) is correct by Remark 6.1 and 2b) since $FT \subseteq FT[X]$. Thus, we have to prove the correctness of Case 2.1 and Case 2.2. The distinction of these cases resembles the use of a barrier in the proof of Venkataraman [Ven87, Section 3].

Assume Case 2.1 and assume that $\sigma : FT[V] \rightarrow FT$ is any possible solution of $\mathcal{S}$. Let v be a witness for the assertion in Case 2.1. We have to prove that

(6.1) $$\|v\sigma\| < r$$

If (6.1) were not true then there would exist $b \in FT$ such that $b \leq v\sigma$ and $\|b\| = r$ (see Remark 5.3). Hence, for some $w \sqsupseteq v$ and some $s \in G_w$, we would have $s \leq b$. Thus, $s \leq v\sigma \leq w\sigma$ which is impossible.

Assume now Case 2.2. Then, for every $v \in V$, fix a witness b^v in FT of size r such that

(6.2) $$(\forall w \sqsupseteq v)(\forall s \in G_w)(s \not\leq b^v)\ .$$

Then we have to prove that $\mathcal{S}$ has solution in FT .

Since the execution has not terminated in 2b), the tests T0′, T0″, T1, T2 do not fail on $\mathcal{S}$. So, let $\gamma : FT[V] \rightarrow FT[X]$ be a substitution which solves $\mathcal{S}$ as in Theorem 6.3. Let $m = \max\{\|V\|, 1 + \|\mathcal{S}\gamma\|\}$ and let η be the morphism, relative to m, as in Lemma 5.4 . Define elements in FT by

(6.3) $$d^v = v\eta[b^v/y]\,.$$

So, by (iii) of Lemma 5.4,

(6.4) $\{d^v : v \in V\}$ is a set of pairwise distinct element of size $m+1+r$.

Then, we define

(6.5) $$\beta : FT[X] \rightarrow FT, \qquad \beta = [d^v/x^v]$$

and we prove that $\gamma\beta$ satisfies $\mathcal{S}$. First, we prove that

(6.6) β is injective on the set H of term of size $< m$.

To prove (6.6) we can use Corollary 3.2 since H is closed under subterms. So, assume $t\beta = v\beta$, for some $t \in H$. Then, $t\beta = d^v$ and $t\beta$ has size $> m$ by (6.4). Hence, t must contain some variable, say u. Thus, $d^u \leq t\beta \leq d^v$. Therefore, we have $u = v$, again by (6.4), and $t = v$ by the Occur-check Axiom. Then, hypothesis (1i) of Corollary 3.2 is proved. Hence (6.6).

Now, if $t \leq v \in \mathcal{S}$ then $t\gamma\beta \leq v\gamma\beta$ since γ is a solution and β is a morphism (see Remark 1.9). If $t \neq v \in \mathcal{S}$ then $t\gamma\beta \neq v\gamma\beta$ since γ is a solution and (6.6). It remains to prove only that:

(6.7) $$s\gamma\beta \not\leq w\gamma\beta \qquad \text{for every formula } s \not\leq w \in \mathcal{S}\ .$$

Assume that (6.7) is not true for some formula. Then, since $s\gamma \not\leq w\gamma$ and since β is injective on terms of $\mathcal{S}\gamma$, must exist some $x^v \in var(w\gamma)$ such that

(6.8) $$s\gamma\beta \leq x^v\beta = d^v\ .$$

Now, we distinguish a priori two cases that we prove both impossible.

Case 1: $s \in G_w$. Then $s\gamma\beta = s$ because s is ground. Hence, $s \leq d^v$ by (6.8). On the other hand, by definition (6.3) of d^v, we have that $s \leq d^v$ implies $s \leq b^v$ or $b^v \leq s$ (see Fig. 5). Now, $s \leq b^v$ contradicts (6.2) and $b^v \leq s$ implies the contradiction $r = \|b^v\| \leq \|s\| < r$ by definition of G_w and r.

Case 2: $s \notin G_w$. Then there exists $u \in var(s)$ and $x^u < u\gamma$, by (b) of Theorem 6.3. Hence, $x^u\beta < u\gamma\beta$ because β is an injective morphism. Thus, $x^u\beta < u\gamma\beta \leq s\gamma\beta$. Therefore, by (6.5) and (6.8), $d^u < d^v$. This is a contradiction since d^u, d^v are finite terms of the same size.

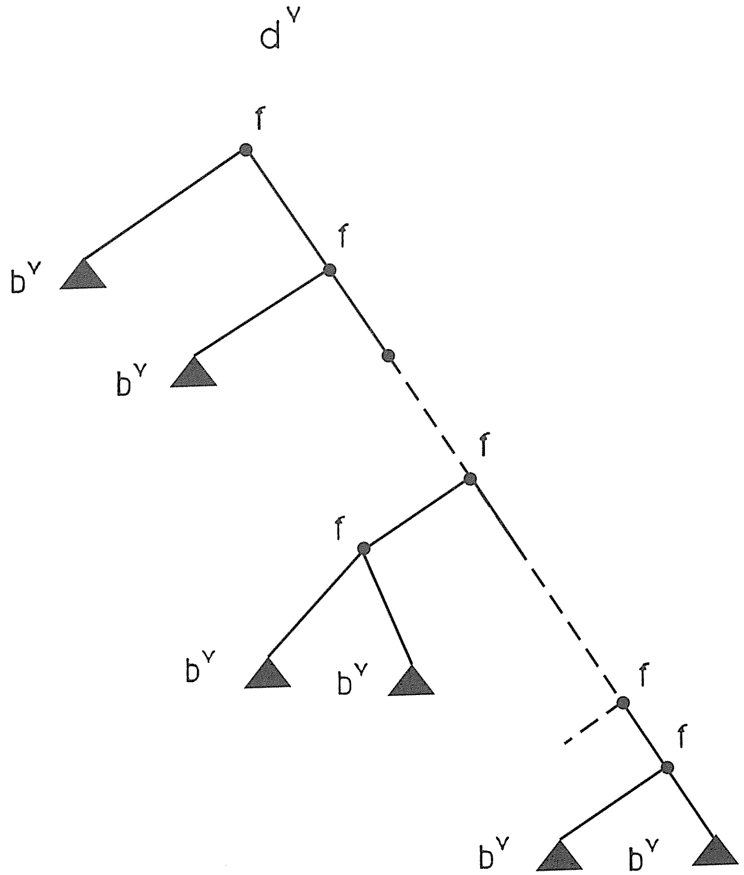

Fig. 5

Remark 6.5 *Let $M \subseteq \{0, 1, \ldots, \omega\}$ be a recursive set, then consider the problem of deciding if the number $\#\mathcal{S}$ of the solutions of a given system $\mathcal{S}$ is in M. This problem is decidable, as was observed by Venkataraman* [Ven87] *. In fact, $\mathcal{S}$ has a finite number of solutions if and only if $\mathcal{S}$ falls always in Case 2.1 during the execution of the procedure $sat(\mathcal{S})$. Moreover, an upper bound for $\#\mathcal{S}$ can be easily estimated. This contrasts with an analogous problem for the solution of diophantine equations, where Davis* [Dav72] *proves that for non trivial subsets M the problem is unsolvable.*

The analogous problem for solving systems in the algebra of rational or infinite terms is even easier. In fact, any reduced system has in RT either 0 or 1 or infinitely many solutions.

7 Axioms for the decision of existential fragments

We denote by $S_0 = \{\Lambda_1, \ldots, \Lambda_k\}$ the (non empty) set of constant symbols in our finite signature S. Moreover, f is a fixed symbol in S of arity greater than one; to simplify notation we think f of arity 2. S is singular if $S = S_0 \cup \{f\}$. We fix an infinite set of indeterminates $\{x_0, \ldots, x_n \ldots\}$. For every $\nu \leq \omega$ we denote by FT_ν the algebraic structure $FT[x_n : \; n < \nu]$ in the signature S. Analogously, we use the notation RT_ν, IT_ν for every $\nu \leq \omega$. We denote by E the set of existential sentences of our first order language $\mathcal{L}_{\leq}$ and by $Th_E(\mathcal{A})$ the set of sentences in E which are true in $\mathcal{A}$, where $\mathcal{A}$ is any structure for $\mathcal{L}_{\leq}$.

Remark 7.1 *According to the inclusions of the relative algebras of terms, we have*

$$Th_E(FT, \leq) \subseteq Th_E(RT, \leq);$$

$$Th_E(FT_1, \leq) \subseteq Th_E(RT_1, \leq);$$

$$Th_E(FT, \leq) \subseteq Th_E(FT_1, \leq);$$

$$Th_E(RT, \leq) \subseteq Th_E(RT_1, \leq);$$

The first two inclusions are clearly proper. The third is proper since

$$\exists x (\Lambda_1 \not\leq x \wedge \ldots \wedge \Lambda_k \not\leq x)$$

is true in FT_1 and not in FT. The last inclusion is proper for singular signatures (see Remark 5.8) since

$$\exists x \, (\Lambda_1 \not\leq x \wedge \ldots \wedge \Lambda_k \not\leq x \wedge f(x, x) \neq x)$$

is true in RT_1 but not in RT. However, Theorem 5.7 proves that

$$Th_E(RT, \leq) = Th_E(RT_1, \leq) = Th_E(IT, \leq)$$

for non singular signatures. Furthermore, it proves that, for every signature,

$$Th_E(RT_1, \leq) = Th_E(RT_\nu, \leq) = Th_E(IT_\nu, \leq) \quad \text{for } 1 \leq \nu \leq \omega.$$

Moreover, for singular signatures, $Th_E(RT, \leq) = Th_E(IT, \leq)$. This will also follow by (2) *of next Corollary.*

Now, we consider the set of axioms:

$$\begin{array}{lcl}\delta & := & \forall v\,(\Lambda_1 \not\leq v \vee \ldots \vee \Lambda_k \not\leq v \vee f(v,v)=v) \\ \tau_1 & := & \exists x\left(\forall \vec{v} \bigwedge_{g\in S}(x \neq g(\vec{v}))\right) \\ \delta_m & := & \forall v(\bigwedge_{t\in FT,\, \|t\|<m} (t\neq v) \longrightarrow \bigvee_{s\in FT,\, \|s\|=m} (s\leq v) \\ & & \text{for every positive integer } m.\end{array}$$

Axiom δ is true in RT and asserts that the full binary tree labelled with f is the unique element which does not admit constant subterms. Axiom τ_1 asserts the existence of at least an indeterminate; it is true in $RT[X]$ and in $FT[X]$ when $X \neq \emptyset$, but it is false in RT and in FT. Axioms δ_m when interpreted in FT say that every term of size not less than m must have at least a subterm of size m.

To formulate the next Corollary to the results obtained in Sections 5 and 6, we need the following

Definition 7.2 *Let H be a set of sentences. We say that a theory T decides the sentences E in H iff for every $\alpha \in E$ the following are true:*

$$T \vdash \alpha \quad \text{iff} \quad \alpha \in H;$$

$$T \vdash \neg\alpha \quad \text{iff} \quad \alpha \notin H.$$

Corollary 7.3

(1) $\mathcal{O}_{IT} \cup \{\tau_1\}$ *decides the sentences E in $Th_E(RT_1, \leq)$;*

(2) $\mathcal{O}_{IT} \cup \{\delta\}$ *decides the sentences E in $Th_E(RT, \leq)$ when the signature is singular;*

(3) $\mathcal{O}_{FT} \cup \{\tau_1\}$ *decides the sentences E in $Th_E(FT_1, \leq)$;*

(4) $\mathcal{O}_{FT} \cup \{\delta_m : m < \omega\}$ *decides the sentences E in $Th_E(FT, \leq)$.*

Proof: Denote by $\mathcal{T}_k$ the first set of axioms in (k) for $1 \leq k \leq 4$.
Proof of (1). Observe that for every model $\mathcal{M}$ of $\mathcal{T}_1$ there is an order embedding $RT_1 \hookrightarrow \mathcal{M}$. Then apply Theorem 5.7.
Proof of (2). Assume that some quantifier-free formula Φ has solution in some model $\mathcal{M}$ of $\mathcal{T}_2$ and not in RT. Choose Φ where the number n of the variables is minimal. Of course $n > 0$. Then, by the procedure Reduce, we can find a reduced system $\mathcal{S}$, with variables contained in $var(\Phi)$, which has solution in $\mathcal{M}$ and not in RT. Thus, by Theorem 5.7, it is $C_v = S_0$ in $\mathcal{S}$ for some variable v. Then, since axiom δ is true in $\mathcal{M}$, the claimed solution $\sigma : var(\mathcal{S}) \to \mathcal{M}$ is such that $\sigma(v)$ is the full binary tree labelled with f (see Remark 5.8). Hence, by substituting v in $\mathcal{S}$ for the term with pointers $f(1,1)$, we would have a quantifier-free formula in less than n variables which has solution in $\mathcal{M}$ but not in RT.
Proof of (3). Observe that, for every model $\mathcal{M}$ of $\mathcal{T}_3$ there is an order embedding $FT_1 \hookrightarrow \mathcal{M}$. Then apply Corollary 6.4.
Proof of (4). Let $\mathcal{M}$ be a model of $\mathcal{T}_4$. Then there is an order embedding $FT \hookrightarrow \mathcal{M}$. It is sufficient to prove that every system $\mathcal{S}$ that has a solution in $\mathcal{M}$ it has, in fact, a solution in FT. Assume not. So, it must exist a reduced system $\mathcal{S}$ as a counterexample, where $var(\mathcal{S}) = \{v_1, \ldots, v_n\}$ and n is minimum. Then it follows that, for every solution σ of $\mathcal{S}$ in $\mathcal{M}$, it is $v_i\sigma \in \mathcal{M} \setminus FT$, for every $i = 1, \ldots, n$. Moreover. the tests T0′, T0″, T1, T2 do not fail on $\mathcal{S}$ by Corollary 6.4, since $\mathcal{M}$ is model of $\mathcal{O}_{FT}$. So, the procedure sat($\mathcal{S}$) either terminates in Case 2.1 or in Case 2.2. Now, assume Case 2.1. Then there is a variable v which is a witness for the assertion in Case 2.1. Thus, by the axiom δ_r there is an element $b^v \in FT$ of size r with $b^v < \sigma v$ and such that the negation of (6.2) is true. Hence, for some $w \sqsupseteq v$ and some $s \in G_w$

$$s\sigma = s \leq b^v < v\sigma \leq w\sigma \quad \text{and} \quad s \not\leq w \in \mathcal{S}.$$

This is a contradiction. Therefore, the procedure $sat(\mathcal{S})$ terminates in Case 2.2 and the system $\mathcal{S}$ has solution in FT.

References

[Cl78] K. L. Clark (1978), *Negation as Failure* Logic and Databases , H. Gallaire and J. Minker (eds.), Plenum, New York .

[Col84] A. Colmerauer (1984), *Equations and inequations on finite and infinite trees*, FGCS'84 Proceedings, 85-99.

[CL89] H. Comon, P. Lescanne (1989), *Equational Problems and Disunification* **J. of Symbolic Computation** 7, 375-426.

[Com90] H. Comon (1990), *Computational Logic: Essays in Honor of Alan Robinson* chapter Disunification: a Survey. MIT Press, (to appear).

[Com90a] H. Comon (1990), *Solving symbolic ordering constraints.* **International J. on Foundations of Computer Science**, 1(4), 387-411.

[Co85] B. Courcelle (1985), *Fundamental Properties of Infinite Trees*, **Theoretical Computer Science** 25(2), 95-169.

[Dav72] M. Davis (1972), *On the number of Solutions of Diophantine equations*, **Proc. Amer. Math. Soc.** 35, 552-554.

[Fi85] M.R. Fitting (1985), *A Kripke-Kleene Semantics for Logic Programs*, **J. of Logic Programming** 2, 295-312.

[GH78] J. V. Guttag and J. J. Horning (1978), *The algebraic specification of abstract data types*, **Acta Informatica**, 10, 27-52.

[Hue76] G. Huet (1976), *Résolution d'équations dans les langages d'ordre* $1, 2, \ldots \omega$. Thèse d'Etat, Univ. Paris 7.

[JK90] J. P. Jouannaud and C. Kirchner (1990), *Solving equations in abstract algebras: A rule-based survey of unification.* In: J. L. Lassez and G. Plötkin, editors, **Computational Logic: Essays in Honor of Alan Robinson**. MIT-Press. To appear.

[Ku87] K. Kunen (1987), *Negation in Logic Programming*, **J. of Logic Programming** 4, 289-308.

[Ll87] J. W. Lloyd (1987), *"Foundation of Logic Programming"*, Springer-Verlag, Berlin 1984, 2nd ed. 1987.

[Mah88] M. J. Maher (1988), *Complete Axiomatizations of the Algebras of Finite, Infinite and Rational Trees* ,**Proc. 3rd IEEE Symp. Logic in Computer Science**, Edinburgh, 348-357.

[MS90] M. J. Maher and P. j. Stuckey (1990), *On inductive inference of cyclic structures.* In: F. Hoffman, editor, **Annals of Mathematics and Artificial Intelligence**, Vol. F. J. C. Baltzer Scientific Pub. Company. To appear.

[Mal61] A. I. Mal'cev (1961), *On the elementary theories of locally free algebras*, **Soviet Math. Doklady**, 768-771.

[Mal71] A. I. Mal'cev (1971), *Axiomatizable classes of locally free algebras of various types*, The Metamathematics of Algebraic Systems: Collected Papers, Studies in Logic, North Holland, pp. 262-281.

[MT89] G. Marongiu, S. Tulipani (1989), *Quantifier Elimination for Infinite Terms* **J. Archiv for Mathematical Logic**. To appear.

[McC77] J. McCarthy (1977), *Representation of Recursive Programs in First Order Logic*, Computer Science Department, Stanford CA.

[Op80] D. C. Oppen (1980), *Reasoning about recursively defined data structures*, **J. of the Association for Computing Machinery** 27(3), 403-411.

[Ra77] M. O. Rabin (1977) *Decidable Theories*, pp. 595–630, in: Handbook of Mathematical Logic, Studies in Logic vol. 90 , North-Holland.

[Tre90] R. Treinen (1990), *A new method for undecidability proofs of first order theories.* Tech. Report A-09/90, Universität des Saarladandes, Saarbrücken, May 1990.

[Tre90a] R. Treinen (1990), *A new method for undecidability proofs of first order theories.* In: K. V. Nori and C. E. Veni Madhavan, editors,**Proceedings of the Tenth Conference on Foundations of Software Technology and Theoretical Computer Science**, p.p. 48-72. Springer Lecture Notes in Computer Science, vol. 472.

[Ven87] K. N. Venkataraman (1987), *Decidability of the purely existential fragment of the theory of term algebras*, **J. of the Association for Computing Machinery** 34(2), 492-510.

[VYH83] K. N. Venkataraman, A. Yasuhara, F. Hawrusik (1983), *A view of computability on term algebras*, **J. Comp. Syst. Sci.** 26(3), 410-471.