Equational specifications, complete term rewriting systems, and computable and semicomputable algebras

Bergstra, J.A.; Tucker, J.V.

Published in:
Journal of the Association for Computing Machinery

DOI:
10.1145/227683.227687

Citation for published version (APA):
Equational Specifications, Complete Term Rewriting Systems, and Computable and Semicomputable Algebras

J. A. BERGSTRA
University of Amsterdam, Amsterdam, and University of Utrecht, Utrecht, The Netherlands

AND

J. V. TUCKER
University of Wales Swansea, Swansea, Wales

Abstract. We classify the computable and semicomputable algebras in terms of finite equational initial algebra specifications and their properties as term term rewriting systems, such as completeness. Further results on properties of these specifications, such as on their size and orthogonality, are provided which show that our main results are the best possible.

Categories and Subject Descriptors: D.3.3 [Programming Languages]: Language Constructs and Features; F.1.1 [Computation by Abstract Devices]: Models of Computation; F.3.2 [Logics and Meanings of Programs]: Semantics of Programming Languages; F.3.3 [Logics and Meanings of Programs]: Studies of Programming Constructs; F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic

General Terms: Languages, Theory

Additional Key Words and Phrases: Abstract data types, complete term rewriting systems, computable and semicomputable algebras, equational specifications with hidden functions, many sorted algebras, term rewriting systems

1. Introduction

In algebraic data type theory, data types are modelled semantically by many sorted universal algebras, and are specified by means of equational or conditional equational axioms, most commonly up to isomorphism using initial algebra semantics for the specification. Algebras of particular interest are the...
computable and semicomputable algebras. The algebras that can be algebraically specified using initial algebra semantics are precisely the semicomputable algebras [Bergstra and Tucker 1987].

We examine the term rewriting properties of finite equational hidden function specifications of data types and we give an algebraic characterization of the computable data types in terms of complete term rewriting systems. A complete term rewriting system is one whose reductions or rewrites satisfy the Church–Rosser property and are strongly terminating. The first theorem we prove is this:

**Theorem 1.1.** Let $A$ be a finitely generated minimal $\Sigma$ algebra. Then, the following are equivalent:

1. $A$ is computable.
2. There is a finite equational specification $(\Sigma_0, E_0)$ such that
   - (i) $\text{Sort}(\Sigma) = \text{Sort}(\Sigma_0)$ and $\Sigma \subseteq \Sigma_0$;
   - (ii) $(\Sigma_0, E_0)$ is a complete term rewriting system;
   - (iii) $I(\Sigma_0, E_0)_A \equiv A$.

Furthermore, the $(\Sigma_0, E_0)$ may be taken to be an orthogonal term rewriting system, and the sizes $|\Sigma_0|$ and $|E_0|$ depend upon the algebra $A$.

The fact that (2) implies (1) is straightforward and is a principal reason for the usefulness of complete term rewriting systems. The fact that (1) implies (2) is more difficult.

The specific properties of the equational specification $(\Sigma_0, E_0)$ constructed in the theorem suggest a number of questions. Of special interest is the fact that the size of the specification $(\Sigma_0, E_0)$ is large and depends on the algebra $A$. In our previous studies, we showed that any computable algebra could be given a very small equational specification: for example, in Bergstra and Tucker [1983b], we constructed a finite equational specification $(\Sigma_1, E_1)$ in which the number of hidden functions needed is $3n$ and the number of equations is $2n$, where $n$ is the number of sorts in the signature $\Sigma$ of the algebra $A$. In particular, we note that the size of $(\Sigma_1, E_1)$ is independent of $A$ and, indeed, independent of the number of constants and operations in the signature $\Sigma$ of $A$. Can any computable algebra be given such a small equational specification that is also a complete term rewriting system? We show that there is a finite data type such that any equational specification which is a complete term rewriting system must be dependent on the algebra and must be large (Theorem 6.1.1). Thus, the specification in the main theorem above cannot be improved in this regard.

To further complement the theorem and to provide a comprehensive picture of its scope we examine the term rewriting properties of computable and semicomputable algebras.

We show that a computable algebra can have an infinite recursive equational specification without hidden functions that is an orthogonal complete term rewriting system (Theorem 4.3.1). From this construction, we obtain a finite equational specification without hidden functions for a finite algebra that is an orthogonal complete term rewriting system (Corollary 4.3.2). We construct an algebra of sets to show that the hidden functions in an equational specification that is a complete term rewriting system can be essential for the construction of normal forms (Theorem 6.2.1).
Finally, we consider semicomputable algebras and, in contrast to the theorem for computable algebras, show the following characterization (Theorems 7.1.1, 7.1.2, and 7.2.1):

**Theorem 1.2.** Let \( A \) be a finitely generated minimal \( \Sigma \) algebra. Then, the following are equivalent:

1. \( A \) is semicomputable.
2. There is an infinite recursively enumerable equational specification \((\Sigma, E)\) such that:
   1. \((\Sigma, E)\) is a complete term rewriting system;
   2. \( I(\Sigma, E) \cong A \).

However, the recursively enumerable complete term rewriting specification \((\Sigma, E)\) cannot be replaced by a recursive complete term rewriting specification, nor can it be replaced by a recursively enumerable orthogonal complete term rewriting specification.

The basic concepts on equational specifications and term rewriting systems are carefully defined in Section 3, and on computable and semicomputable algebras in Section 4. In Sections 5–7, we prove the theorems: results about computable algebras are in 5 and 6, and results about semicomputable algebras are in Section 7. Section 2 explains briefly some theoretical issues concerning data types which the theorems address.

This paper belongs to our series of studies on the adequacy and power of algebraic specification methods for data types which we began in Bergstra and Tucker [1979] (see also Bergstra and Tucker [1987]), which is summarised in Section 2.

A single sorted form of Theorem 1.1 was first announced in Bergstra and Tucker [1980b] and its proof outlined. Here, the theorem is reformulated using current term rewriting theory and a full proof in the many sorted case is given. The other theorems are new. For applications of the theorems, it is the many sorted case that is important. We have found that it is not satisfactory to transform the proof for single sorted algebras to a proof for many sorted algebras, because an informal account of the extension is unable to get at details we consider to be important.

As in our previous studies, we exploit proof methods based on recursion schemes on the natural numbers. Algebraic aspects of the \( \mu \)-recursive functions and the primitive recursive Kleene \( T \)-predicate are used to provide arguments that are algebraically detailed and natural. Related to the proof of Theorem 1.1 are methods for simulating the behavior of Turing machines using rewrite systems (mentioned in, e.g., Dershowitz [1987]). In particular, Dauchet [1989] indicates that a Turing machine computation can be encoded in a single orthogonal rewrite rule that gives rise to a terminating TRS. These Turing machine methods offer an approach different from the recursion scheme methods we have used here and in the past. In either case, the main technical problem in the paper is to obtain a specification of the target algebra without the use of hidden sorts.

The reader is assumed well versed in initial algebra specification methods: see Goguen et al. [1978], Ehrig and Mahr [1985], and Wirsing [1990]; knowledge of our earlier work is desirable but not strictly necessary. Knowledge of the theory of the recursive functions is necessary: see Cutland [1980], for instance.
Finally, we thank the referees for their many valuable comments that have helped us improve the paper.

2. Initial Algebra Semantics and Data Types

We will summarize the context for the theorems in the theory of data types.

2.1. Algebraic Semantics. A concrete implementation of a data type is modelled by a many sorted algebra $A$ finitely generated from initial values $a_1, \ldots, a_n \in A$ named in its finite signature $\Sigma$, that is, $A$ is a finitely generated minimal algebra. A data type is modeled by some class $K$ of minimal algebras of common signature. Two concrete data types are equivalent if they are isomorphic as algebras. An abstract data type can be modeled as a class $K$ of minimal algebras closed under isomorphism, that is, if $A \in K$ and $B \cong A$, then $B \in K$. Often, an abstract data type is modeled as an isomorphism type, that is, a class closed under isomorphism in which all algebras are isomorphic. Further semantic considerations involve the computability of the many sorted algebras used: $A$ may be a finite, computable, semicomputable or, perhaps, cosemcomputed algebra. These notions are based on theoretical ideas about the implementation of algebras on computers and, to be semantic properties, they must also be isomorphism invariants.

The semantics $K$ which model a data type can be investigated using the construction of an initial algebra $I(K)$ for $K$ with the result that every $A \in K$ is uniquely definable, up to isomorphism, as a unique epimorphic image of $I(K)$ or, equivalently, as a factor algebra $I(K)/\equiv_A$ for a unique congruence $\equiv_A$. If $I(K) \in K$, then this $I(K)$ can be used as a canonical algebra modelling the data type; if, in addition, the class $K$ is an isomorphism type then $I(K)$ “is” the data type. The idea is that $I(K)$ models the data type semantics in a way that is independent of methods for its implementation or specification.

2.2. Implementation Using Terms. The basic method for constructing this initial algebra $I(K)$, up to isomorphism, is as a factor algebra of the syntactic algebra $T(\Sigma)$ of all closed terms over $\Sigma$, because $T(\Sigma)$ is initial for the class $ALG(\Sigma)$ of all $\Sigma$ algebras. In fact, $I(K) \cong T(\Sigma)/\equiv_K$, where $\equiv_K$ is a congruence for which $t \equiv_K t'$ means that the terms $t$ and $t'$ are equivalent syntactic expressions in all the algebras of $K$, that is, $K \models t = t'$. The problem of implementing and specifying the data type $K$ via $I(K)$ can be investigated through the corresponding problem of implementing or specifying the congruence $\equiv_K$. A central technical idea is that of a transversal for the equivalence relation $\equiv_K$, which is a set of terms containing one and only one term for each equivalence class.

This algebra $T(\Sigma)/\equiv_K$ is of importance for implementing the data type, using symbolic computation techniques for representing terms and algorithms for term manipulation, especially algorithms for computing $\equiv_K$. In these circumstances, we may say that a data type $K$ is computable, or semicomputable, when $\equiv_K$ is a decidable or semidecidable relation on $T(\Sigma)$.

2.3. Algebraic Specifications. To specify the data type, an axiomatic theory $(\Sigma, E)$ is used so that $K \subseteq ALG(\Sigma, E)$. In particular, if $E$ is a set of equations or conditional equations and $K = ALG(\Sigma, E)$, then $I(K) \in K$, and

$E \vdash t = t' \iff t \equiv_K t'$,
where the proof system is that for equational or conditional equational logic applied to closed terms. Thus, for any recursively enumerable \( E \) we know that \( =_K \) is recursively enumerable. However, the specification \((\Sigma, E)\) is desired to be finite.

We know from Bergstra and Tucker [1987] that this finite equational or conditional equational method will not define all computable (and hence all semicomputable) data types. Enriching the method to allow the use of a finite number of hidden sorts and functions does enable it to specify any semicomputable (and hence any computable) data type. The question addressed here is:

*What finite algebraic specification methods exist that specify all and only the computable data types?*

As noted in the Introduction, one answer to this question in Bergstra and Tucker [1983b] is that an algebra \( A \) is computable if, and only if, it can be given an equational specification \((\Sigma, E)\), using a small number of hidden functions and equations, such that \( A \) is isomorphic with the initial and final algebras of \((\Sigma, E)\). In Bergstra and Tucker [1983a] the cosemicomputable algebras were shown to be precisely the algebras defined by algebraic specifications under final algebra semantics; see also Bergstra and Tucker [1980] and Meseguer et al. [1992].

Here the properties of the specification \((\Sigma, E)\) that determine the decidability of the congruences for initial algebras are analyzed. The equations \( E \) may be interpreted as left-to-right rewrite rules for transforming terms of \( T(\Sigma) \). Thus, \((\Sigma, E)\) serves both as an axiomatic specification for a variety of models, and as a *term rewriting system*, intended to formalize a system of deductions, governed by simple algebraic substitution rules, within which a deduction

\[
t \rightarrow t' \quad \text{implies} \quad t =_K t'
\]

(but not conversely). The choice of \((\Sigma, E)\) leads to a transversal or set \( J \) of normal forms for \( =_K \): given \( t, t' \in T(\Sigma) \), to decide \( t =_E t' \) one uses \( E \) to calculate their prescribed "normal forms" \( n, n' \in J \) and on completing the deductions \( t \rightarrow_E n, t' \rightarrow_E n' \) one checks \( n = n' \).

The semantics of a type \( K \) is supposed to be uniquely determined up to isomorphism with an initial algebra \( I(K) \), and not by a particular syntactical construction, however canonical an implementation. The decidability of \( =_K \) implies the computability of the algebra \( T(\Sigma)/=_K \) under our definition and, in particular, since the concept of a computable algebra is an isomorphism invariant, we can remove all mention of syntax in the semantical concept of a computable data type and identify these with the computable algebras.

So with regard to the content of Theorem 1.1, the ease with which statement (2) implies (1) is proved is evidence for the usefulness of complete term rewriting system specifications, whereas the implication that (1) implies (2) is considered as the affirmative answer to the question about adequacy: *Do these finite complete term rewriting system equational specification methods define all the data types one wants?*

The examples and Theorem 1.2 differentiate the computable and semicomputable algebras using related properties of term rewriting systems.
3. Reduction Systems, Term Rewriting, and Equational Specifications

We describe many sorted algebraic reduction systems that are meant to abstract the essential structure of term rewriting systems. Then we describe the concepts and notations concerning many sorted term rewriting systems and algebraic specifications that we will need. Supporting references are: Meinke and Tucker [1992] and Wechler [1992], for basic algebra; Ehrig and Mahr [1985] and Wirsing [1990], for algebraic specifications; and Klop [1992], for single sorted term rewriting.

3.1. Signatures and Algebras. The notations for signatures and algebras are as follows:

3.1.1. Signatures. A signature \( \Sigma \) consists of a nonempty set \( S \), whose elements are called sorts, and a family 
\[
\langle \Sigma_{w,s} : w \in S^*, s \in S \rangle
\]
of sets, where the elements of \( \Sigma_{w,s} \) for \( \lambda \) the empty string, are called constant names or symbols of sort \( s \); and the elements of \( \Sigma_{w,s} \) are called function names or symbols of type \( w \rightarrow s \).

A signature \( \Sigma \) is finite if \( S \) is finite, each \( \Sigma_{w,s} \) is finite, and all but finitely many \( \Sigma_{w,s} = \emptyset \). We assume all signatures are finite.

Let \( \Sigma^1 \) and \( \Sigma^2 \) be signatures. Then \( \Sigma^1 \) is a subsignature of \( \Sigma^2 \) if \( S^1 \subseteq S^2 \) and for each \( w \in S^{1*} \) and \( s \in S^1 \)
\[
\Sigma^1_{w,s} \subseteq \Sigma^2_{w,s}.
\]
We write \( \Sigma^1 \subseteq \Sigma^2 \).

3.1.2. Algebras. Let \( S \) be a signature. A \( S \) algebra \( A \) consists of a family
\[
\langle A_s : s \in S \rangle
\]
of nonempty sets \( A_s \), called the carriers of \( A \), together with families of elements
\[
\Sigma^A_{w,s} = \langle c_A \in A_s : c \in \Sigma_{w,s} \rangle
\]
and families of functions
\[
\Sigma^A_{w,s} = \langle \sigma^A_A : A_{w(1)} \times \cdots \times A_{w(k)} \rightarrow A_s : \sigma \in \Sigma_{w,s} \rangle
\]
A \( S \) algebra is minimal if it contains no proper subalgebras.

If \( A \) is a \( S \) algebra and \( \Sigma^0 \subseteq \Sigma \), then \( A|_{\Sigma^0} \) is the algebra obtained from \( A \) by deleting the constants and operations of \( A \) not named in \( \Sigma^0 \) and \( \langle A \rangle_{\Sigma^0} \) is the smallest \( \Sigma^0 \) algebra contained in \( A \).

3.2. Reduction Systems and Algebraic Reduction Systems. We begin with a sequence of basic definitions.

Let \( A = \langle A_s : s \in S \rangle \) be an \( S \) sorted family of nonempty sets, and \( \equiv = \langle \equiv_s : s \in S \rangle \) be an \( S \) sorted family of equivalence relations on \( A \). A transversal for \( \equiv \) is a set \( J = \langle J_s : s \in S \rangle \) where for each \( s \in S \), \( J_s \subseteq A_s \) and for each \( a \in A_s \), there is one and only one \( t \in J_s \) such that \( t \equiv_s a \).

Let \( A = \langle A_s : s \in S \rangle \) be a \( S \) sorted family of nonempty sets. A reduction system or a replacement system on the many sorted set \( A \) is an \( S \) sorted family 
\[
\rightarrow_R = \langle \rightarrow_R_s : s \in S \rangle
\]
of reflexive and transitive binary relations on $A$. For $a, b \in A$, if $a \rightarrow_R b$ we say $a$ reduces to $b$ (under $\rightarrow_R$), or that $b$ is a reduct of $a$ (under $\rightarrow_R$).

An element $a \in A_s$ is a normal form for $\rightarrow_R$ if there is no $b \neq a$ so that $a \rightarrow_R b$; the set of all normal forms for $\rightarrow_R$ is denoted $NF(\rightarrow_R) = \langle NF_s(\rightarrow_R) : s \in S \rangle$.

The reduction system $\rightarrow_R$ is confluent or Church–Rosser if for each $s \in S$ and for any $a, b \in A_s$ if there are $b_1, b_2 \in A_s$ so that $a \rightarrow_R b_1$ and $a \rightarrow_R b_2$, then there is $c \in A_s$ so that $b_1 \rightarrow_R c$ and $b_2 \rightarrow_R c$.

The reduction system $\rightarrow_R$ is weakly terminating or weakly normalizing if, for each $s \in S$ and for each $a \in A_s$, there is some normal form $b \in A_s$ so that $a \rightarrow_R b$.

The reduction system $\rightarrow_R$ is strongly terminating or strongly normalizing if, for each $s \in S$, there does not exist an infinite chain

$$a_0 \rightarrow_R a_1 \rightarrow_R \ldots \rightarrow_R a_n \rightarrow_R \ldots$$

of reductions in $A$, wherein for $i \in \mathbb{N}$, $a_i \neq a_{i+1}$.

The reduction system $\rightarrow_R$ is complete if it is Church–Rosser and strongly terminating.

A reduction system is Church–Rosser and weakly terminating if, and only if, every element reduces to a unique normal form. Clearly strong termination entails weak termination.

Let $\equiv_R$ denote the smallest equivalence relation on $A$ containing $\rightarrow_R$. It is an easy exercise to show that for each $s \in S$ and for $a, a' \in A_s$,:

$$a \equiv_R a' \iff \text{there is a sequence } a = b_1, \ldots, b_k = a' \text{ such that for each pair } b_i, b_{i+1} \in A_s, \text{ there exists a common reduct } c_i \in A_s \text{ for } 1 \leq i \leq k - 1.$$ Using this characterization of $\equiv_R$, it is straightforward to prove this fact:

**Lemma 3.2.1.** The reduction system $\rightarrow_R$ on $A$ is Church–Rosser if, and only if, for each $s \in S$ and for any $a, a' \in A_s$ if $a \equiv_R a'$, then there is $c \in A_s$ so that $a \rightarrow_R c$ and $a' \rightarrow_R c$.

**Lemma 3.2.2.** Let $\rightarrow_R$ be a Church–Rosser weakly terminating reduction system on $A$. Then the set $NF(\rightarrow_R)$ of normal forms is a transversal for $\equiv_R$.

**Proof.** Since every element $a \in A_s$ reduces to some normal form $n \in NF_s(\rightarrow_R)$, the set $NF(\rightarrow_R)$ contains representatives for each equivalence class of $\equiv_R$. To check uniqueness, let $n, m \in NF(\rightarrow_R)$ and assume $n \equiv_R m$. By Lemma 3.2.1, there is $c \in A_s$ so that $n \rightarrow_R c$ and $m \rightarrow_R c$, but since $n, m$ are normal forms $n = c, m = c$ and so $n = m$. Q.E.D.

**Definition 3.2.3.** Suppose now that $A$ is a many sorted algebra. Then by an algebraic reduction system $\rightarrow_R$ on the algebra $A$ we mean a reduction system $\rightarrow_R$ on the family of carriers of $A$, which is closed under the operations of $A$ in the sense that for each operation

$$\sigma : A_{w(1)} \times \cdots \times A_{w(k)} \rightarrow A_s$$
of $A$, for all $a_i, b_i \in A_{w(i)}$ and $1 \leq i \leq k$,
$$a_i \rightarrow_{R_{w(i)}} b_1, \ldots, a_k \rightarrow_{R_{w(k)}} b_k \Rightarrow \sigma(a_1, \ldots, a_k) \rightarrow_{R} \sigma(b_1, \ldots, b_k).$$

**Lemma 3.2.4.** If $\rightarrow_{R}$ is an algebraic reduction system on an algebra $A$, then $\equiv_R$ is a congruence on $A$.

We next explain how a reduction system is generated by a set of one-step reductions and how these sets of one-step reductions can be determined from quite arbitrary sets.

Let $\rightarrow_{R}$ be a reduction system on an $S$ sorted subset $A = (A, : s \in S)$, that is, $X = \langle X_i : s \in S \rangle$ where $X_i \subseteq A_i \times A_i$. Then $X$ is said to generate $\rightarrow_{R}$ as a set of one-step reductions if $X$ is reflexive and $\rightarrow_{R}$ is the smallest transitive set containing $X$, that is, the transitive closure of $X$.

Let $\equiv_{R}$ be an algebraic reduction system on an $S$ sorted algebra $A$. Then $X \subseteq A \times A$ is said to generate $\equiv_{R}$ as a set of algebraic one-step reductions if $X$ is reflexive, $X$ is closed under unit substitutions in the following sense: writing $(a, b) \rightarrow_{Xw(i)}$ as $a \rightarrow_{Xw(i)} b$, for any operation
$$\sigma : A_{w(1)} \times \cdots \times A_{w(k)} \rightarrow A_s$$
of $A$, for any $1 \leq i, j \leq k$ and $j \neq i$, $a_j \in A_{w(j)}$, and $a \rightarrow_{Xw(i)} b$, it follows that
$$\sigma(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_k) \rightarrow_{R} \sigma(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k);$$
and $\equiv_{R}$ is the transitive closure of $X$.

In the set-theoretic case any reflexive set determines a reduction system in its transitive closure. In the algebraic case, any reflexive set, closed under unit substitutions, can be shown to determine an algebraic reduction system in its transitive closure. Thus, in either case, starting with an arbitrary set $D \subseteq A \times A$ one can construct a one-step reduction relation $\rightarrow_{D(1)}$, containing it and hence a set-theoretic or algebraic reduction system $\rightarrow_{D}$.

### 3.3. Term Algebras

We will apply these ideas to specify algebraic reduction systems on the term algebra $T(\Sigma)$ and connect them with the initial algebras of equational theories. First, we give definitions of the primary notions of terms, equations, term evaluation etc.

#### 3.3.1. Terms

Let $X$ be a set of variable names. For $s \in S$ and $x \in X$, we call $x^s$ an $s$ sorted variable. Let $X_s'$ be the set of all $s$ sorted variables.

Let $V = \langle V_s : s \in S \rangle$ where $V_s \subseteq X_s$. We define the $\Sigma$ term algebra $T(\Sigma, V)$ of terms over $\Sigma$ in variables of $V$ as follows.

The family of carriers of $T(\Sigma, V)$ is
$$\langle T_s(\Sigma, V) : s \in S \rangle$$
where the $T_s(\Sigma, V)$ are inductively defined simultaneously over $S$:

(i) for $x^s \in V_s$, $x^s \in T_s(\Sigma, V)$;
(ii) for $c \in \Sigma_0$, $c^s \in T_s(\Sigma, V)$; and
(iii) for $\sigma \in \Sigma_0$, where $w = W(1) \cdots W(k)$, and $t_i \in T_{w(i)}$, $\sigma^s(t_1, \ldots, t_k) \in T_s(\Sigma, V)$.

Notice that the type can be determined from each term.
The constants of \( T(\Sigma, V) \) are defined for \( c \in \Sigma_{h,s} \),
\[
c_{T(\Sigma, V)} = c^s
\]
and the operations are defined for \( \sigma \in \Sigma_{w,s} \),
\[
\sigma_{T(\Sigma, V)}(t_1, \ldots, t_k) = \sigma^s(t_1, \ldots, t_k)
\]
for \( t_i \in T_{w(i)}(\Sigma, V) \).

This makes \( T(\Sigma, V) \) a \( \Sigma \)-algebra.

We write \( T(\Sigma, X) \) for \( V_s = X_s, s \in S \), the complete family of sorted variables named by \( X \). \( T(\Sigma, V) \) is a subalgebra of \( T(\Sigma, X) \). We write \( T(\Sigma) \) when \( V_s = \emptyset, s \in S \). The terms of \( T(\Sigma) \) are called closed.

A signature \( \Sigma \) is (fully) instantiated or nonvoid if for all \( s \in S \)
\[
T_s(\Sigma) \neq \emptyset.
\]

**Definition 3.3.1.1.** A term rewriting system or TRS is any algebraic reduction system on a term algebra.

3.3.2. Equations. Let \( \Sigma \) be a signature and \( X \) a set of variable names. An equation of sort \( s \in S \) is an expression \( e \) of the form
\[
t(X) = t'(X),
\]
where \( t(X), t'(X) \in T(\Sigma, X) \). Let \( \text{Eqn}_{s}(\Sigma, X) \) be the set of such equations and
\[
\text{Eqn}(\Sigma, X) = \langle \text{Eqn}_{s}(\Sigma, X) \rangle_{s \in S}.
\]
Let \( E = \langle E_s \rangle_{s \in S} \) be a set of equations with \( E_s \subseteq \text{Eqn}_{s}(\Sigma, X) \). Then \( E \) is finite if \( S \) is finite and \( E_s \) is finite for each \( s \in S \).

Let \( e, e' \in T_s(\Sigma, X) \). We say \( e \) and \( e' \) are \( \alpha \)-equivalent if there is a permutation of the set \( X \) of variable names that transforms \( e \) to \( e' \). We write \( e \equiv_{\alpha} e' \) if \( e \) and \( e' \) are equivalent.

Let \( \{ e \}_a = \{ e' \in \text{Eqn}_{s}(\Sigma, X) \mid e' \equiv_{\alpha} e \} \).

Let \( E = \langle E_s \rangle_{s \in S} \) be a set of equations. Define the \( \alpha \)-closure \( \hat{E} \) of \( E \) to be
\[
\hat{E} = \langle \hat{E}_s \rangle_{s \in S},
\]
where
\[
\hat{E}_s = \{ e' \in \text{Eqn}_{s}(\Sigma, X) \mid e' \equiv_{\alpha} e \text{ for some } e \in E_s \} = \bigcup_{e \in E_s} \{ e \}_a,
\]
We say that \( E \) is \( \alpha \)-closed if \( E = \hat{E} \).

3.3.3. Term Evaluation. We define the term evaluation \( \Sigma \) homomorphism \( \text{val}_A: T(\Sigma) \to A \). The map \( \text{val}_A = \langle \text{val}_s^A : s \in S \rangle \) is defined by induction on terms simultaneously over \( S \).

For \( c \in \Sigma_{h,s} \),
\[
\text{val}_s^A(c^s) = c_s^A.
\]

For \( \sigma \in \Sigma_{w,s} \),
\[
\text{val}_s^A(\sigma^s(t_1, \ldots, t_k)) = \sigma_s^A(\text{val}_{w(1)}(t_1), \ldots, \text{val}_{w(k)}(t_k)).
\]
Equational Specifications

Then $\text{val}_A$ is clearly a homomorphism (by definition of constants and operations on $T(\Sigma)$). We often write $\text{val}$ for $\text{val}_A$ when the $A$ is understood.

**Lemma 3.3.3.1.** The map $\text{val}_A: T(\Sigma) \to A$ is $\Sigma$ homomorphism and is unique as such.

The congruence derived from $\text{val}_A$ we write

$$\equiv_A = \langle \equiv'_A \mid s \in S \rangle$$

and $\equiv'_A$ on $A$, is defined by

$$t \equiv'_A t' \quad \text{iff} \quad \text{val}_A(t) = \text{val}_A(t').$$

Thus, if $\text{val}_A$ is an epimorphism,

$$T(\Sigma)/\equiv_A \cong A$$

Note $A$ is $\Sigma$ minimal if $\text{val}_A$ is a surjection.

Consider $\equiv_A$ on $T(\Sigma)$.

A term transversal for $A$ is a family $T = \langle T_s : s \in S \rangle$ such that for each $s \in S$, $T_s \subseteq T_s(\Sigma)$ and for each $a \in A$, there is exactly one $t \in T_s$ such that $\text{val}_A(t) = a$.

A canonical term transversal for $A$ is a term transversal $T$ such that $\sigma(t_1, \ldots, t_k) \in T^s(i)$ for each subterm $t_i \in T(\Sigma)$.

A standard construction of a canonical term transversal $T$ is to order $T(\Sigma)$ lexically and for each $a \in A$ choose the first (and so shortest) $t \in T(\Sigma)$ such that $\text{val}_A(t) = a$. To see this is canonical, note that if $t = \sigma(t_1, \ldots, t_k)$ and $t_i$ is not a shortest term for $a \in A_{w(i)}$ then we can replace $t_i$ with a shorter term that would contradict that $t$ is in the transversal $T$.

**3.4. Term Rewriting Systems.** Let $T(\Sigma, X)$ be the algebra of terms over $\Sigma$ in variable names $X$. Let $E \subseteq \text{Eqn}(\Sigma, X)$ be a set of equations such that for each $t = t' \in E$ the LHS $t$ is not a variable and all the variables in the RHS $t'$ also appear in $t$. We can define a set $D(E) \subseteq T(\Sigma) \times T(\Sigma)$ by

$$D(E)_s = \{(t(r_1, \ldots, r_k), t'(r_1, \ldots, r_k)) : t = t' \in E, \text{ and } r_i \in T(\Sigma)\}$$

and so obtain the smallest set $\rightarrow_{E(1)}$ of algebraic one-step reductions containing $D(E)$, and the algebraic reduction relation $\rightarrow_{E}$ it generates. This formalizes the use of equations in derivations of terms in $T(\Sigma)$ where the reduction $t \rightarrow_{E} t'$ requires substitutions to be made in some equation $e \in E$ and the LHS of $e$ is replaced by the RHS of $e$ in $t$ to obtain $t'$.

**Definition 3.4.1.** We call the pair $(\Sigma, E)$ an equational term rewriting system or equational TRS, for short.

The first set of properties of a term rewriting system $(\Sigma, E)$ is now defined by applying the properties of reduction systems to $\rightarrow_{E}$; for example:

The term rewriting system $(\Sigma, E)$ is complete if the reduction system $\rightarrow_{E}$ on $T(\Sigma)$ is Church–Rosser and strongly terminating.

We denote by $\text{NF}(\Sigma, E)$ the set of all normal forms of $\rightarrow_{E}$ and by $\equiv_{E}$ the congruence associated to $\rightarrow_{E}$.

**Lemma 3.4.2.** $T(\Sigma, E) = T(\Sigma)/\equiv_{E}$ is the initial algebra of $\text{ALG}(\Sigma, E)$. 

LEMMA 3.4.3. Let $A$ be a minimal $\Sigma$ algebra. Let $(\Sigma, E)$ be a weakly terminating TRS. If $A \vdash E$ and $\text{NF}(\Sigma, E)$ is a transversal for $\equiv_A$, then

$$T(\Sigma, E) = T(\Sigma) / \equiv_A = A.$$  

PROOF. We shall show that for $t, t' \in T(\Sigma)$,

$$t \equiv_E t' \iff t \equiv_A t'.$$

Case (i). Suppose $t \equiv_E t'$. Then, by Birkhoff's Completeness Theorem, $E \vdash t = t'$ and since $A \in \text{ALG}(\Sigma, E)$ we have $E \vdash t = t'$, by soundness. This means that $\text{val}_A(t) = \text{val}_A(t')$ in $A$, that is, $t \equiv_A t'$.

Case (ii). Suppose $t \equiv_A t'$. Since the TRS $(\Sigma, E)$ is weakly terminating we can calculate its normal forms for all terms using a function $\text{nf}_E$. We know that

$$t \equiv_A \text{nf}_E(t) \quad \text{and} \quad t' \equiv_A \text{nf}_E(t').$$

By the result of case (i), using $A \vdash E$,

$$t \equiv_A \text{nf}_E(t) \quad \text{and} \quad t' \equiv_A \text{nf}_E(t').$$

Since $t \equiv_A t'$,

$$\text{nf}_E(t) \equiv_A \text{nf}_E(t'),$$

but since $\text{NF}(\Sigma, E)$ is a transversal for $\equiv_A$, this implies

$$\text{nf}_E(t) = \text{nf}_E(t').$$

Thus,

$$\text{nf}_E(t) \equiv_E \text{nf}_E(t')$$

and by (*)

$$t \equiv_E t'.$$  

Q.E.D.

Definition 3.4.4. The term rewriting system $(\Sigma, E)$ is left linear if for all $t = t' \in E$, each variable that appears in $t$ does so only once.

The term rewriting system $(\Sigma, E)$ is nonoverlapping if

(i) for any pair of different equations $t = t', r = r' \in E$, the terms $t$ and $r$ do not overlap in the following sense: there exist closed substitutions $\tau, \rho$ of $t, r$ such that $\rho(r)$ is a subterm of $\tau(t)$ and the outermost function symbol of $\rho(r)$ occurs as a part of $t$.

(ii) for any rule $t = t' \in E$, $t$ does not overlap with itself in the following sense: there exist closed substitutions $\tau, \rho$ of $t$ such that $\tau(t)$ is a proper subterm of $\rho(t)$ and the outermost function symbol of $\tau(t)$ occurs as a part of $t$.

The term rewriting system $(\Sigma, E)$ is orthogonal if it is left linear and nonoverlapping.

The following is a basic fact about orthogonality; for a proof, see Section 3 of Klop [1992, Theorem 3.1.2].

LEMMA 3.4.5. If $(\Sigma, E)$ is an orthogonal TRS, then it is Church–Rosser.

3.5. Algebraic Specifications. Let $A$ be an algebra of signature $\Sigma_A$. Then $A$ is said to have a finite equational specification $(\Sigma, E)$ if $\Sigma = \Sigma_A$ and $E$ is a finite set of equations over $T(\Sigma, X)$ such that $T(\Sigma, E) \equiv A$. 

An algebra \( A \) of signature \( \Sigma_A \) is said to have a \textit{finite equational hidden enrichment specification} \((\Sigma, E)\) if \( \Sigma_A \subseteq \Sigma \) and \( E \) is a finite set of equations over \( T(\Sigma, X) \) such that

\[
T(\Sigma, E)|_{\Sigma_A} = \langle T(\Sigma, E) \rangle_{\Sigma_A} \cong A.
\]

The structural properties of a specification \((\Sigma, E)\), such as the Church–Rosser and normalization properties, are taken from those of its reduction relation \( \rightarrow_E \). For example:

**Definition 3.5.1.** An algebra \( A \) of signature \( \Sigma_A \) is said to have a \textit{finite equational complete TRS hidden enrichment specification} \((\Sigma, E)\) if \( \Sigma_A \subseteq \Sigma \) and \( E \) is a finite set of equations over \( T(\Sigma, X) \) such that \( \rightarrow_E \) is a complete TRS and

\[
T(\Sigma, E)|_{\Sigma_A} = \langle T(\Sigma, E) \rangle_{\Sigma_A} \cong A.
\]

4. **Computable and Semicomputable Algebra**

The definitions of a computable and semicomputable algebra have their origins in Rabin [1960] and Mal'cev [1961/1971], independent papers devoted to founding a general theory of computable algebraic systems and their computable morphisms. We will mention only those ideas and facts that contribute to the understanding or proofs of the theorems. In fact, the definitions and associated basic results (e.g., about invariance and the word problem) that are standard in computable algebra, and that we need here, can be found in Mal'cev [1961/1971].

For further information about the theory from the point of view of logic see the articles Mal'cev [1961/1971] and Ershov [1977]. For a view from computer science, where the subject is treated in the many-sorted case, see Meseguer and Goguen [1985] and Bergstra and Tucker [1987]. A survey of computable algebra, which includes details of its historical development, is Stoltenberg-Hansen and Tucker [1995].

4.1. **ALGEBRAS AND NUMBERINGS.** Let \( \Sigma \) be an \( S \) sorted signature. A many sorted algebra \( A \) of signature \( \Sigma \) is said to be \textit{effective} if for each \( s \in S \) there exists a recursive set \( \Omega_s \) of natural numbers and a surjection \( \alpha_s: \Omega_s \rightarrow A \) such that for each operation symbol \( \sigma \in \Sigma_{w,s} \) for \( w = w(1) \cdots w(k) \), and corresponding operation \( \sigma_A \) of \( A \), there corresponds a recursive \textit{tracking function} \( \bar{\sigma}: \Omega_{w(1)} \times \cdots \times \Omega_{w(k)} \rightarrow \Omega_s \) which commutes the following diagram,

\[
\begin{array}{ccc}
A_{w(1)} \times \cdots \times A_{w(k)} & \xrightarrow{\sigma_A} & A_s \\
\alpha^w \uparrow & & \uparrow \alpha \\
\Omega_{w(1)} \times \cdots \times \Omega_{w(k)} & \xrightarrow{\bar{\sigma}} & \Omega_s
\end{array}
\]

wherein \( \alpha^w(x_1, \ldots, x_k) = (\alpha_{w(1)}(x_1), \ldots, \alpha_{w(k)}(x_k)) \).
We combine the sets into the $S$ sorted family
$$\Omega = \langle \Omega_s : s \in S \rangle$$
which, along with the tracking functions, constitutes a recursive $\Sigma$ algebra $R$ of numbers. We combine the surjections into the $S$ sorted map
$$\alpha = \langle \alpha_s : s \in S \rangle$$
which is a $\Sigma$ epimorphism $\alpha : R \to A$. We refer to $\alpha$ as an effective numbering or coordinate system.

Consider the $S$ sorted relation $=_{a} = \langle =_{a_s} : s \in S \rangle$ on the number algebra $R$, defined for $x, y \in \Omega_s$ by
$$x =_{a_s} y \quad \text{if, and only if,} \quad \alpha_s(x) = \alpha_s(y) \text{ in } A.$$

The relation is a $\Sigma$ congruence on $R$.

**Definition 4.1.1.** Suppose the relation $=_{a}$ is recursive, that is, for each $s \in S$, $=_{a_s}$ is recursive on $\Omega_s$. Then, we say $A$ is computable under effective numbering $\alpha$.

Suppose the relation $=_{a_s}$ is recursively enumerable, that is, for each $s \in S$, $=_{a_s}$ is recursively enumerable on $\Omega_s$. Then, we say $A$ is semicomputable under effective numbering $\alpha$.

Both concepts are finiteness conditions, that is, isomorphism invariants possessed of all finite structures. Also noteworthy is this other invariance property first observed in Mal'cev [1961/1971].

**Lemma 4.1.2.** If $A$ is a finitely generated algebra computable or semicomputable, under both $\alpha : \Omega_{a} \to A$ and $\beta : \Omega_{b} \to A$, then $\alpha$ and $\beta$ are recursively equivalent in the sense that there exists recursive functions $f, g$ which commute the diagram:

$$\begin{array}{ccc}
\alpha & \Rightarrow & A \\
\downarrow f & & \downarrow \beta \\
\Omega_{a} & \xrightarrow{\rightarrow} & \Omega_{b}
\end{array} \quad \begin{array}{ccc}
\alpha & \Rightarrow & A \\
\downarrow g & & \downarrow \beta \\
\Omega_{a} & \xleftarrow{\leftarrow} & \Omega_{b}
\end{array}$$

Let $A$ be computable under $\alpha$. Using the recursiveness of $=_{a}$ and the observation that $\alpha$ is an epimorphism from $R$ to $A$, it is easy to prove this useful fact (see Bergstra and Tucker [1987]):

**Lemma 4.1.3.** Every computable algebra $A$ is isomorphic to a recursive number algebra $R$ whose carrier $R$ is the set $N$ of natural numbers, if $A$ is infinite, and is the set $\{0, 1, \ldots, m - 1\}$ of the first $m$ natural numbers, if $A$ is finite of cardinality $m$.

Obviously, no such isomorphic representation is possible for the semicomputable algebras for otherwise they would be computable.

If $A$ is computable under $\alpha$, then an $S$ sorted set $X \subseteq A^n$ is $(\alpha)$-computable or $(\alpha)$-semicomputable accordingly as
$$\alpha^{-1}(X) = \{(x_1, \ldots, x_k) \in \Omega^n : \alpha^n(x_1, \ldots, x_k) \in X\}$$
is recursive or recursively enumerable.
**Lemma 4.1.4.** Let $A$ be a computable algebra and $\equiv$ a congruence on $A$. If $\equiv$ is computable or semicomputable then the factor algebra $A/\equiv$ is computable or semicomputable accordingly.

**4.2. Computable Term Algebras.** The algebras $T(\Sigma)$ are computable under any of their standard Gödel numberings. This was implicit in Section 1 where we spoke of a data type $K$ being computable when its defining congruence $\equiv_K$ is decidable on $T(\Sigma)$. By Lemma 4.1.4 and isomorphism invariance, we can define equivalently a data type to be computable when its initial algebra is computable.

We will describe the computability properties of term algebras that we will need.

**Definition 4.2.1.** Let $\Sigma$ be an $S$ sorted signature and $X$ a countable set of variable names used to make $S$ sorted variables. Let $T(\Sigma, X)$ be the $\Sigma$ term algebra over $X$. Then $T(\Sigma, X)$ is a computable algebra.

Let $\gamma$ be a computable numbering for $T(\Sigma, X)$. Without loss of generality, we assume that $\gamma$ has the following properties.

(i) Let $G$ be a recursive $\Sigma$ algebra of numbers with $G_s = N$ for all $s \in S$, and let

$$
\gamma: G \to T(\Sigma, X) \quad \text{and} \quad \gamma^{-1}: T(\Sigma, X) \to G
$$

be $\Sigma$-isomorphisms.

(ii) Let $\gamma$ be standard in the sense of Mal'cev [1961/1971]; this means that we can decide when a term is a variable, compute subterms of a term, etc.

(iii) Let $\gamma$ satisfy the following monotonic property: for each $s \in S$, and context $t(x^u) \in T_s(\Sigma, X)$ with single variable $x^u$ of sort $u$, then for all $r_1, r_2 \in T_s(\Sigma, X)$,

$$
\gamma^{-1}_u(r_1) < \gamma^{-1}_u(r_2) \quad \text{implies} \quad \gamma^{-1}_u(t(r_1)) < \gamma^{-1}_u(t(r_2)).
$$

This means that the numbering induces an ordering on terms and that substitution into terms is monotonic with respect to this ordering. In a uniform way, for every minimal $\Sigma$ algebra, a transversal can be found by taking the smallest terms in this ordering to represent the elements of $A$.

All standard numberings are recursively equivalent, by Lemma 4.1.2. Recall that $A \approx T(\Sigma)/\equiv_A$. The following result states the equivalence between the classes of computable and semicomputable algebras and those of algebras with decidable or semidecidable generalised word problems, respectively. A proof of this can be found in Mal'cev [1961/1971].

**Theorem 4.2.2.** Let $A$ be a finitely generated algebra. Then $A$ is computable or semicomputable if, and only if, $\equiv_A$ is computable or semicomputable on $T(\Sigma)$, respectively.

From $\gamma$ we can computably number the set $Eqn(\Sigma, X)$ of equations in an obvious way: $\gamma_{\equiv}: [G_\equiv \to Eqn(\Sigma, X)]$ is obtained from $\gamma$ by pairing.

We may define $E \subset Eqn(\Sigma, X)$ to be recursively enumerable if $\gamma_{\equiv}^{-1}(E)$ is recursively enumerable.

We note that if $E$ is recursively enumerable then the closure $\hat{E}$ is recursively enumerable.
However, we define $E \subseteq \text{Eqn}({\Sigma}, {X})$ to be recursive if $\gamma^{-1}(E)$ is recursive and if $\gamma^{-1}(\overline{E})$ is recursive.

A starting point for the investigation of effectivity are these facts:

**Lemma 4.2.3.** Let $({\Sigma}, {E})$ be a finite equational term rewriting system specification. Then

(i) the basis set $D_{{\Sigma}}$ and the one-step reduction relation $\rightarrow_{{\Sigma}(1)}$ are computable;
(ii) the reduction system $\rightarrow_{{\Sigma}}$ and the congruence $=_{E}$ are semicomputable;
(iii) the set $\text{NF}(\Sigma, E)$ of normal forms is computable.

In particular, $T(\Sigma, E)$ is a semicomputable algebra. If $({\Sigma}, E)$ is recursive or recursively enumerable, then (i) and (ii) hold, but the set $\text{NF}(\Sigma, E)$ is cosemicomputable.

Notice that $\text{NF}(\Sigma, E)$ need not be a transversal for $=_{E}$. We may now trivially prove the following:

**Lemma 4.2.4.** Let $({\Sigma}, {E})$ be a finite equational term rewriting system specification which is Church–Rosser and weakly terminating. Then $T(\Sigma, E)$ is a computable algebra.

**Proof.** Given $t \in T(\Sigma)$, we can interleave the algorithms enumerating $\text{NF}(\Sigma, E)$ and $=_{E}$ to seek the normal form of $t$ which is guaranteed to exist from the weak termination hypothesis. Given $t, t' \in T(\Sigma)$, to decide $t =_{E} t'$ we calculate their normal forms $n, n'$ and, using the uniqueness property of Church–Rosser systems, we have only to check whether or not $n = n'$. Q.E.D.

The argument of Lemma 4.2.4 is also that of this companion lemma to Lemma 4.1.4.

**Lemma 4.2.5.** Let $A$ be a semicomputable algebra with semicomputable congruence $=_{E}$. If there exists a semicomputable transversal for $=_{E}$, then the factor algebra $A/_{=}$ is a computable algebra.

4.3. Theorems on Recursive Specifications. We will now prove some first results about specifications of algebras without hidden functions.

**Theorem 4.3.1.** Let $A$ be a minimal $X$ algebra. If $A$ is computable, then $A$ possesses a possibly infinite recursive equational specification $({\Sigma}, E')$ that is an orthogonal complete term rewriting system.

**Proof.** Now $\Sigma \cong T(\Sigma)/=_{\Sigma}$ and since $A$ is computable we have that $=_{A}$ is recursive in the numbering $\gamma$. Let $nf_{\gamma}: T(\Sigma) \rightarrow T(\Sigma)$ compute the smallest normal forms for $=_{A}$ as determined by the enumeration $\gamma$; it is defined by

$\text{nf}_{\gamma}(t) = \gamma((\text{least } i)[t \equiv_{A} \gamma(i)])$.

Define

$E_{A} = \{ t = nf_{\gamma}(t) : t \neq nf_{\gamma}(t) \text{ and for each proper subterm } r \text{ of } t, nf_{\gamma}(r) \equiv r \}$.

Let $T_{\gamma} = \text{im}(nf_{\gamma})$, the image of $nf_{\gamma}$, be a transversal for $=_{A}$. We claim that $T_{\gamma}$ is the set of normal forms for the TRS $({\Sigma}, E_{A})$. First, note that the terms in $T_{\gamma}$ do not reduce since neither they nor their subterms occur on a LHS. This is because each subterm $r$ has the property that $r = nf_{\gamma}(r)$, for if not, then there is a contradiction with the enumeration property (iii) of the computable
numbering $\gamma$ as formulated in 4.2.1 above. Next, note that the terms not in $T_\gamma$ can be reduced. To see this, let $t \not\in T_\gamma$ and let $r$ be the smallest subterm of $t$ such that $r \in T_\gamma$ (perhaps $r$ is $t$). Then $r$ occurs on a LHS of an equation in $E_A$, and we may reduce $t$.

Thus, $NF(\Sigma, E_A) = T_\gamma$.

Next we show that $(\Sigma, E_A)$ is strongly terminating. Because the Gödel numbering $\gamma$ of $T(\Sigma)$ is monotonic, any reduction of $t \rightarrow t'$ entails $\gamma^{-1}(t) > \gamma^{-1}(t')$. Thus, an infinitely long reduction cannot occur because $(N, <)$ is well founded.

We show that $(\Sigma, E_A)$ is an orthogonal TRS. Clearly, since each rule has no variables, there is no rule with duplicated variables on its LHS, that is, the TRS is left-linear. If two rules overlap then, since the rules have closed terms on the LHS, one of the LHS must be a subterm of the other. By inspection of $E_A$, we see this is not the case. Thus, the TRS is nonoverlapping.

Thus, $(\Sigma, E_A)$ is complete since it is strongly terminating and orthogonal.

Now, $(\Sigma, E_A)$ is recursive since $E_A$ is recursive using the computability of syntactic identity $\equiv$, $nf_\gamma$ and subterm decomposition, and $E_A$ is trivially closed under the renaming of its variables.

Finally, since $NF(\Sigma, E_A) = T_\gamma$ is a transversal for $\equiv_A$ and trivially $A \in \text{Alg}(\Sigma, E_A)$, we deduce that

$$A \equiv T(\Sigma, E_A)$$

by Lemma 3.4.3. Q.E.D.

**Corollary 4.3.2.** Let $A$ be a $\Sigma$ minimal algebra. If $A$ is finite, then $A$ possesses a finite orthogonal complete TRS specification $(\Sigma, E)$.

**Proof.** To see this note that $\text{im}(nf_\gamma)$ is finite, its cardinality is that of $A$, and each LHS in $E_A$ is of the form $g(t_1, \ldots, t_k)$ with $g$ a function symbol in $\Sigma$ and $t_i \in \text{im}(nf_\gamma)$ for $1 \leq i \leq k$. Since $\Sigma$ is finite, we know that $E_A$ is finite. Q.E.D.

Consider the size of $(\Sigma, E)$ in the case of the corollary. Let

$$l = \max\{|A_s| : s \in S\}$$

$$k = \max\{|w| : \Sigma_{w,s} \neq \emptyset\}$$

$$m = |\Sigma| = |S| + |\bigcup \{\Sigma_{w,s} : w \in S^*, s \in S\}|.$$

Then $|E| < ml^k$.

5. **Proof of Theorem 1.1**

Let us restate the first theorem.

**Theorem 1.1.** Let $A$ be a finitely generated minimal $\Sigma$ algebra. Then the following are equivalent:

1. $A$ is computable.
2. There is a finite equational specification $(\Sigma_0, E_0)$ such that
   (i) $\text{Sort}(\Sigma) = \text{Sort}(\Sigma_0)$ and $\Sigma \subseteq \Sigma_0$;
   (ii) $(\Sigma_0, E_0)$ is a complete term rewriting system;
   (iii) $I(\Sigma_0, E_0) |_{\Sigma} \equiv A$. 

Furthermore, the \((\Sigma_0, E_0)\) may be taken to be an orthogonal term rewriting system, and the sizes \(|\Sigma_0|\) and \(|E_0|\) depend upon the algebra \(A\).

The fact that statement (2) implies statement (1) was established in Lemma 4.2.4; we prove that (1) implies (2).

Let \(S = \{1, 2, \ldots, n\}\) be a set of \(n\) sorts. Let \(\Sigma\) be an \(S\) sorted signature with \(p\) constants and \(q\) operations. Let \(A\) be any computable minimal \(2\) algebra.

If \(A\) is finite then there exists an appropriate finite equational specification \((\Sigma, E)\) for \(A\) by Corollary 4.3.2.

Here is the idea of the proof in the case that \(A\) is infinite.

Suppose \(A\) is infinite with \(l\) infinite carriers

\[A_1, \ldots, A_l\]

and \(n - l\) finite carriers

\[A_{l+1}, \ldots, A_n.\]

We suppose that for \(i = l + 1, \ldots, n\)

\[|A_i| = b_i + 1.\]

Of course, \(A\) need not have finite carriers and \(l = n.\)

Since \(A\) is computable, by Lemma 4.1.3, we can take \(A\) to be isomorphic to a recursive algebra \(R\) of numbers and we can concentrate on building an appropriate finite equational specification for \(R\), which will also be a specification for \(A.\)

First, we build an expansion \(R_0\) of \(R\) by adding constants and functions such that

\[R_0|_\Sigma = R.\]

The design of \(R_0\) involves coding all the carriers into one of the infinite carriers and simulating the algebraic operations using recursive functions and the Kleene T-predicate.

Next, we build a finite equational specification \((\Sigma_0, E_0)\) for \(R_0\) that we will prove is a complete TRS. Here, we exploit algebraic aspects of the definition of the recursive functions by recursion schemes. This equational specification of \(R_0\) does not involve hidden sorts or functions.

The specification \((\Sigma_0, E_0)\) serves as an appropriate specification for \(R\) that does involve hidden functions.

5.1. CONSTRUCTION OF \(R_0\). Using Lemma 4.1.3, let \(R \cong A\) and for \(i = 1, \ldots, l\)

\[R_i = \mathbb{N}\]

and \(i = l + 1, \ldots, n\)

\[R_i = \{0, 1, \ldots, b_i\} \subset \mathbb{N}.\]

We assume that each of the \(p\) constants has the form

\[c \in R.\]
for some \( s \in S \), and that each of the \( q \) operations are total recursive functions on \( N \) having the form

\[
f: R_{w(1)} \times \cdots \times R_{w(k)} \to R_s
\]

for some \( w(1), \ldots, w(k), s \in S \).

To make \( R_0 \), we add to \( R \) the following constants and functions:

5.1.1. Counting. For \( i = 1, \ldots, n \) we add the constant zero

\[
i_0 \in R_i
\]

and the successor function

\[
i_{\text{succ}}: R_i \to R_i
\]

defined as follows: for infinite sorts \( i = 1, \ldots, l \)

\[
i_{\text{succ}}(x) = x + 1,
\]

and for finite sorts \( i = l + 1, \ldots, n \)

\[
i_{\text{succ}}(x) = x + 1 \quad \text{if} \quad x < b_i
\]

\[
= b_i \quad \text{if} \quad x = b_i.
\]

5.1.2. Coding. We add functions that code all the carriers into the first

infinite carrier \( R_1 \), namely: for \( i = 1, \ldots, n \)

\[
i_{\text{fold}}: R_i \to R_1
\]

is defined by

\[
i_{\text{fold}}(x) = x
\]

for \( x \in N. \) We add functions that decode from \( R_1 \), namely:

\[
i_{\text{unfold}}: R_1 \to R_i
\]

defined for \( i = 1, \ldots, l \) by

\[
i_{\text{unfold}}(x) = x
\]

for \( x \in N, \) and for \( i = l + 1, \ldots, n \) by

\[
i_{\text{unfold}}(x) = \min(x, b_i).
\]

for \( x \in N. \)

5.1.3. Tracking Functions. For each operation \( f: R_{w(1)} \times \cdots \times R_{w(k)} \to R_s \) of \( R \) we add a recursive function \( f': R_1 \times \cdots \times R_1 \to R_1 \) that simulates \( f \) on \( R_1. \) This \( f' \) is defined by

\[
f'(x_1, \ldots, x_k) = i_{\text{fold}}(f(w(1)_{\text{unfold}}(x_1), \ldots, w(k)_{\text{unfold}}(x_k)))
\]

for \( x_1, \ldots, x_k \in R_1. \)

5.1.4. Enumeration Functions. We add new functions designed to compute

each tracking function \( f' \) on \( R_1 \) in a special way as follows: let \( \phi: \mathbb{N}^k \to \mathbb{N} \) be any total recursive function. Then, by the Kleene Normal Form Theorem, this may be written

\[
\phi(x) = U(\mu z \cdot T^k(e, x, z)),
\]
where $U$ and $T$ are the so called Kleene computation function and $T$ predicate, respectively, and $e$ is some index for $\phi, x \in \mathbb{N}^k$, and $z \in \mathbb{N}$. Since $U$ and $T^k$ are primitive recursive so are the functions
\[ h(z, x) = U(\mu z' \leq z \cdot [z' = z \text{ or } T^k(e, x, z')]) \]
\[ g(z, x) = 0 \quad \text{if } \exists z' \leq z \cdot T^k(e, x, z') \]
\[ = 1 \quad \text{otherwise}. \]
From these functions we can define a recursive function
\[ t(z, x, 0) = h(z, x) \]
\[ t(z, x, y + 1) = t(z + 1, x, g(z + 1, x)) \]
to simulate the least number operator. Thus, $\phi$ is factorized into $t, h, g$ in the sense that
\[ \phi(x) = t(0, x, 1). \]
(The reader may care to consult Cutland [1980].)

We apply this method for $\phi$ to each tracking function $f'$ on $R_i$ and add the constructed functions $h, g, t$.

5.1.5. Subfunctions. Finally, for each tracking map $f'$, we add each primitive recursive subfunction $\Lambda$ of its primitive recursive enumeration functions $g, h$. Let $\Delta$ be this list of all the subfunctions of the enumeration functions $g$ and $h$. Such a list is added for each of the $q$ tracking maps.

5.1.6. Size. Now $R_0$ is the many sorted algebra obtained by adding all the above functions. Clearly,
\[ R_0|_{\Sigma} = R. \]
It is instructive to count these additions. Since $\Sigma$ has $p$ constants and $q$ functions, to make the signature $\Sigma_0$, we must add the following:
\begin{align*}
\text{n constants} \\
\text{n successors} \\
\text{n folds} \\
\text{n unfolds} \\
q \text{ tracking functions} \\
3q \text{ enumeration functions} \\
\Pi \text{ subfunctions}
\end{align*}
where $\Pi = \Pi_1 + \cdots + \Pi_q$ and $\Pi_i$ is the number of subfunctions in some primitive recursive definitions of $g$ and $h$ associated with the $i$th tracking operation $f'$. Note that $\Pi$ is dependent on the algebra, whereas the other numbers are independent of the algebra and dependent only on the number of sorts, constants and functions in $\Sigma$.

5.2. CONSTRUCTION OF $(\Sigma_0, E_0)$. We now define specification $(\Sigma_0, E_0)$ for $R_0$. Let $\Sigma$ have the form
\[
\begin{align*}
\text{constants} & \quad \cdots \\
\xi: \rightarrow s \\
\cdots
\end{align*}
\]
Equational Specifications

operations

\[ F : w(1) \times \cdots \times w(k) \to s \]

where there are \( p \) constants and \( q \) operations.

Then \( \Sigma_0 \) has the form of \( \Sigma \) with the following adjoined:

| constants  | \( i^0 : \to i \) |
| operations | \( \forall i < n \) |

\begin{align*}
\text{SUCC}: i &\to i \\
\text{FOLD}: i &\to 1 \\
\text{UNFOLD}: 1 &\to i \\
\end{align*}

\[ F' : 1^k \to 1 \]

\[ G : 1 \times 1^k \to 1 \] for each operation \( F \) of \( \Sigma \)

\[ H : 1 \times 1^k \to 1 \]

\[ T : 1 \times 1^k \times 1 \to 1 \]

\[ \Lambda \]

\[ \ldots \]

We will often use \( \lambda \) for a notation naming a function \( \lambda \) in \( R_0 \).

The equations of \( E_0 \) are constructed as follows:

5.2.1. Counting. For finite sorts \( i = 1 + 1, \ldots, n \)

\[
\text{SUCC}^i(\text{SUCC}^i(0)) = \text{SUCC}^i(0).
\] (1)

5.2.2. Coding. For infinite sorts \( i = 1, \ldots, l \)

\[
\text{FOLD}^i(0) = i^0 \\
\text{FOLD}^i(\text{SUCC}^i(X)) = \text{SUCC}^i(\text{FOLD}^i(X)).
\] (2) (3)

For finite sorts \( i = 1 + 1, \ldots, n \)

\[
\text{FOLD}^i(0) = i^0 \\
\text{FOLD}^i(\text{SUCC}^k(0)) = \text{SUCC}^k(i^0)
\] (4) (5)

and for \( k = 1, \ldots, b_i \).

For all sorts, \( i = 1, \ldots, n \)

\[
\text{UNFOLD}^i(0) = 0^n \\
\text{UNFOLD}^i(\text{SUCC}^i(X)) = \text{SUCC}^i(\text{UNFOLD}^i(X)).
\] (6) (7)

5.2.3. Tracking. For each constant \( c \) of sort \( s \) naming \( c \in R_i \),

\[
c = \text{SUCC}^c(0).
\] (8)

For each operation symbol \( F \in \Sigma_{w,s} \),

\[
F((w(1)X_1), \ldots, (w(k)X_k))
= \text{UNFOLD}^i(F'(w(1)\text{FOLD}^i(w(1)X_1), \ldots, w(k)\text{FOLD}^i(w(k)X_k))).
\] (9)
5.2.4. Enumeration and Subfunctions. For each tracking function \( f' \) for each function \( f \) we add equations for the \( g, h, \) and \( t, \) and primitive subfunctions \( \Delta \) of \( g \) and \( h, \) as follows:

For \( t \) we add

\[
T(Z, X, 1^0) = H(Z, X) \\
T(Z, X, 1\text{SUCC}(Y)) = T(1\text{SUCC}(Z), X, G(1\text{SUCC}(Z), X))
\]

and

\[
F'(X) = T(1^0, X, 1\text{SUCC}(1^0))
\]

For each primitive recursive function \( \lambda \in \Delta \cup \{ g, h \}, \) we add equations for its name \( \lambda, \) using a case distinction on the defining equations for \( \lambda: \)

If \( \lambda(x_1, \ldots, x_k) = x_i, \) then add \( \lambda(X_1, \ldots, X_k) = X_i \)

If \( \lambda(y) = y + 1, \) then add \( \lambda(Y) = \text{SUCC}(Y) \)

If \( \lambda(x) = \mu(\mu_1(x), \ldots, \mu_n(x)) \), then add \( \lambda(X) = \mu(\mu_1(X), \ldots, \mu_n(X)) \)

where \( x = (x_1, \ldots, x_k) \) and \( X = (X_1, \ldots, X_k). \)

If \( \lambda(0, x) = \mu_1(x) \) and \( \lambda(y + 1, x) = \mu_2(y, x, \lambda(y, x)) \)

then add

\[
\lambda(0, X) = \mu_1(X) \\
\lambda(1\text{SUCC}(Y), X) = \mu_2(Y, X, \lambda(Y, X))
\]

where, again, \( x \) and \( X \) are possibly vectors.

Let us count the equations:

\[
\begin{align*}
n - 1 & \quad \text{counting} \\
2l + 2(b_1,\ldots, b_n) + 2n & \quad \text{coding} \\
p & \quad \text{tracking constants} \\
q & \quad \text{tracking operations} \\
3q & \quad t \text{ and tracking functions} \\
\Pi_\epsilon & \quad g, h, \text{ and } \Delta
\end{align*}
\]

The method for primitive recursive functions adds at most two equations per function; in previous notation, we note

\[
\Pi_\epsilon < 2.2q + 2. \Pi = 2(2q + \Pi).
\]

Thus, the number of equations depends on the size of the finite carriers and the structure of (the enumeration of) the operations.

**Lemma 5.2.4.1.** The finite equational specification \((\Sigma_0, E_0)\) is an initial algebra specification of \(R_0,\) that is,

\[
R_0 \cong T(\Sigma_0, E_0).
\]
Equational Specifications

As a TRS, \((\Sigma_0, E_0)\) has the following properties:

(i) it is orthogonal;
(ii) it is strongly terminating;
(iii) the sets of normal forms are, for infinite sorts \(i = 1, \ldots, l\),

\[ NF_i(\Sigma_0, E_0) = \{ \text{SUCC}^k(\text{\texttt{0}}): k = 0, 1, \ldots \} \]

and for finite sorts \(i = l + 1, \ldots, n\)

\[ NF_i(\Sigma_0, E_0) = \{ \text{SUCC}^k(\text{\texttt{0}}): k = 0, 1, \ldots, b_i \} \].

From (i) and (ii), it follows that \((\Sigma_0, E_0)\) is a complete TRS.

**Proof.** Clearly, \(R_0\) satisfies \(E_0\) by construction. We will prove these statements in the order (i) followed by (iii). Then we will assume (ii) and deduce that \(R_0 \equiv T(\Sigma_0, E_0)\). Finally, we prove (ii) in the next subsection 5.3.

(i) The TRS \((\Sigma_0, E_0)\) is left linear and nonoverlapping by inspection.

(iii) For \(i = 1, \ldots, l\) define

\[ T_i = \{ \text{SUCC}^k(\text{\texttt{0}}): k = 0, 1, \ldots \} \]

and for \(i = l + 1, \ldots, n\) define

\[ T_i = \{ \text{SUCC}^k(\text{\texttt{0}}): k = 0, 1, \ldots, b_i \} \].

Clearly, for each \(i = 1, \ldots, n\),

\[ T_i \subseteq NF_i(\Sigma_0, E_0) \]

because no equation of \(E_0\) has a LHS that matches with the numerals of \(T_i\).

Next we consider the converse inclusion. Let \(t \notin T_i\) we show that \(t\) reduces and so is not a normal form.

Let \(r\) be the smallest subterm of \(t\) such that \(r \notin T_i\). There are three cases:

(a) If \(i\) is a finite sort and \(r = \text{SUCC}^k(\text{\texttt{0}})\) for \(k > b_i\). Then there is a reduction of \(r\) by means of eq. (1) for counting in 4.2.1, and so \(t\) is not a normal form.

(b) If \(r = \text{\texttt{c}}\), then there is a reduction by eq. (8) for constants in 5.2.3.

(c) If \(r = \Lambda(t_1, \ldots, t_k)\) for \(\Lambda\) any function symbol, then \(t_1, \ldots, t_k\) must be numerals by the minimality of \(r\). For each choice of \(\Lambda\), there is a reduction of \(r\) by means of an equation of \(E_0\) and so \(t\) is not a normal form.

We prove isomorphism using 5.2.4.1(ii); we define a map \(\phi: R_0 \rightarrow T(\Sigma_0, E_0)\) which is a family of maps

\[ \phi_i: R_i \rightarrow T_i(\Sigma_0, E_0) \]

for \(i = 1, \ldots, n\), where

\[ \phi_i(x) = \{ \text{SUCC}^x(\text{\texttt{0}}) \} \]

for all \(x \in R_i\). Since the numerals are normal forms 5.2.4.1(iii); the map is injective. If the strong termination property 5.2.4.1(ii) holds then every term has a normal form that is a numeral and so the map is surjective.

We show \(\phi\) is a homomorphism.
Let \( \Lambda \) be any operation symbol in \( \Sigma_0 \) of type \( u(1) \times \cdots \times u(k) \to \nu \) naming the operation \( \Lambda \) in \( T(\Sigma_0, E_0) \) and the operation \( \lambda \) in \( R_0 \); we show that
\[
\phi(x_1, \ldots, x_k) = \Lambda(\phi_{u(1)}(x_1), \ldots, \phi_{u(k)}(x_k)).
\]
The LHS is
\[
[\nu\text{SUCC}^{x_1, \ldots, x_k}](\nu(0)).
\]
The RHS is
\[
\Lambda[\nu\text{SUCC}^{x_1}((\nu(1)))], \ldots, \nu\text{SUCC}^{x_k}((\nu(0)))]
\]
by definition of \( \Lambda \) in \( T(\Sigma_0, E_0) \).

To show that these terms are equivalent in \( E_0 \) we reason as follows: Note that since \( R_0 \) is an algebra of numbers,
\[
R_0 \models \nu\text{SUCC}^{x_1, \ldots, x_k}(\nu(0)) = \Lambda[\nu\text{SUCC}^{x_1}((\nu(1)))], \ldots, \nu\text{SUCC}^{x_k}((\nu(0)))]
\]
If the strong termination property 5.2.5(ii) holds, since the numerals are the normal forms, we have
\[
E_0 \models \Lambda[\nu\text{SUCC}^{x_1}((\nu(1)))], \ldots, \nu\text{SUCC}^{x_k}((\nu(0)))] = \nu\text{SUCC}^y(\nu(0))
\]
for some \( y \in N \). Thus, because \( R_0 \) satisfies \( E_0 \),
\[
R_0 \models \nu\text{SUCC}^y(\nu(0)) = \nu\text{SUCC}^{x_1, \ldots, x_k}(\nu(0))
\]
and, by uniqueness, \( y = \lambda(x_1, \ldots, x_k) \). Therefore,
\[
E_0 \models \Lambda[\nu\text{SUCC}^{x_1}((\nu(1)))], \ldots, \nu\text{SUCC}^{x_k}((\nu(0)))] = \nu\text{SUCC}^{y}(\nu(0)),
\]
and the equivalence classes are identified, and \( \phi \) is a homomorphism. Q.E.D.

5.3. PROOF OF STRONG TERMINATION. We prove (ii) of Lemma 5.2.4.1, that each \( t \in T(\Sigma_0) \) is strongly terminating, by induction on the complexity of \( t \).

As basis, we consider all constant symbols. If \( t = \text{0} \), then we know that no reduction is possible from \( E_0 \) because it is a normal form.

If \( t = c \) of sort \( s \) names the constant \( c \in R_s \), then, by inspection of \( E_0 \), there is at most one reduction possible, by means of eq. 8, and this leads to a normal form \( \nu\text{SUCC}^c(\nu(0)) \).

We formulate the induction step as follows:

**Lemma 5.3.1.** Let \( s_1, \ldots, s_k \in T(\Sigma_0) \) be strongly terminating and let \( \Lambda \) be a \( k \)-ary function symbol of \( \Sigma_0 \). Then \( \Lambda(s_1, \ldots, s_k) \) is strongly terminating.

**Proof.** We prove this by induction on an ordering of the function symbols.

First, we order the signature \( \Sigma_0 \) by ordering the operations of \( R_0 \). For each operation \( f_i \) of \( R \) let \( h_i, g_i, t_i \) be the functions factoring \( f_i \) and let \( \Delta_i \) be the list of primitive recursive functions used in the definitions of the \( h_i \) and \( g_i \), those of \( h_i \) preceding those of \( g_i \) and each of these two lists ordered by the complexity of the primitive recursive definitions of the \( h_i \) and \( g_i \), respectively. Thus, we order the constants and operations of \( R_0 \) into the list
\[
\nu\text{suc}, \ldots, \nu\text{suc}, \nu\text{fold}, \ldots, \nu\text{fold}, \nu\text{unfold}, \ldots, \nu\text{unfold}, \Delta_1, \ldots, \Delta_q, h_1, \ldots, h_q, g_1, \ldots, g_q, t_1, \ldots, t_q, f'_1, \ldots, f'_q, f_1, \ldots, f_q
\]
and let the signature $\Sigma_0$ of $R_0$ be ordered in this way. We shall now prove the
lemma by induction on the position of $\lambda$ in this ordering of $\Sigma_0$.

The proof divides into a basis case, and an induction step involving nine
cases, many of which split into subcases. In every case, we argue by contradic-
tion. We assume that an infinite reduction

$$t \rightarrow t_1 \rightarrow t_2 \rightarrow \cdots \rightarrow t_N \rightarrow t_{N+1} \rightarrow \cdots$$

exists for $t = \lambda(s_1, \ldots, s_k)$ and $s_1, \ldots, s_k$ strongly terminating. We assume that
$t_N \rightarrow t_{N+1}$ is the first reduction where a rule is used that involves the outer-
most function symbol $\lambda$. Such an $N$ must exist for otherwise the infinite
reduction would contradict the assumption that the $s_1, \ldots, s_k$ are strongly
terminating. Thus, $t_1, \ldots, t_N$ have the forms

$$t_i = \lambda(r_{i1}, \ldots, r_{ik})$$
for $i = 1, \ldots, N$, and for some $1 \leq \alpha(i) \leq k$

$$r_{ij} = r_{i+1j} \quad \text{for} \quad j \neq \alpha(i)$$
$$r_{ij} \rightarrow r_{i+1j} \quad \text{for} \quad j = \alpha(i).$$

Note that $t_N = \lambda(r_{N1}, \ldots, r_{Nk})$ and that the subterms $r_{N1}, \ldots, r_{Nk}$ are
strongly terminating because the $s_1, \ldots, s_k$ are.

We will consider such reduction sequences for every type of operator $\lambda$ in
the ordered list. For convenience, we would like to assume that $N = 1$ and that
the first reduction involves $\lambda$; this is possible:

**Lemma 5.3.2.** The following are equivalent:

(a) For all strongly terminating terms $r_1, \ldots, r_k$, each reduction sequence of
$\lambda(r_1, \ldots, r_k)$ is finite and $\lambda(r_1, \ldots, r_k)$ is strongly terminating.

(b) For all strongly terminating terms $r_1, \ldots, r_k$ each reduction sequence of
$\lambda(r_1, \ldots, r_k)$ that begins with a reduction involving $\lambda$ is finite.

**Proof.** That (a) implies (b) is immediate. Consider the converse. Consider
the arbitrary infinite reduction sequence

$$t \rightarrow t_1 \rightarrow t_2 \rightarrow \cdots \rightarrow t_N \rightarrow t_{N+1} \rightarrow \cdots$$

If this is infinite, then the reduction sequence

$$t_N \rightarrow t_{N+1} \rightarrow \cdots$$

is infinite and involves $\lambda$ at the first step. By (b), we deduce that this is
impossible. Hence, $t$ is strongly terminating. Q.E.D.

Thus, in each argument, we will examine the reduction

$$t \rightarrow t_1$$
and show that $t_1$ is strongly terminating (often it cannot be further reduced).

We now begin the proof by induction on the position of $\lambda$ in the list.

**Basis 5.3.3.** $\lambda$ is $^1Succ$ and $t = ^1Succ(s)$.

There is no equation in $E_0$ that allows us to rewrite $^1Succ$, so an infinite
reduction sequence from $t$ starting with such a rewrite is impossible.
Induction Steps 5.3.4. We assume the Lemma 5.3.1 is true for all function symbols preceding $\lambda$ in the list. There are nine cases and several subcases.

Case 1. $\lambda$ is 'Succ for $1 < i \leq n$.

Subcase 1a. The sort $i = 2, \ldots, l$ is infinite. Then, the argument is exactly the same as in the basis case above.

Subcase 1b. The sort $i = l + 1, \ldots, n$ is finite. Consider a $\lambda$ first step reduction sequence

$$t \rightarrow t_1 \rightarrow \cdots .$$

Only eq. (1) allows $\lambda$ to be reduced and this leads to a normal form that cannot be reduced further. Thus, no infinite reduction sequence exists.

Case 2. $\lambda$ is 'Fold for $1 \leq i \leq n$ and $t = \text{fold}(s)$.

Subcase 2a. The sort $i = 1, \ldots, l$ is infinite.

Only rules (2) and (3) can be applied to the reduction $t \rightarrow t_1$ in a $\lambda$ first step reduction sequence. We show that $t$ is strongly terminating by induction on the value $\text{val}(s)$ of $s$ in $R_0$.

If $\text{val}(s) = 0$, then eq. (3) cannot be applied because otherwise $s$ must have the form 'Succ($z$), for some $z$, which contradicts that $\text{val}(s) = 0$, by definition of $\text{val}$. So eq. (2) is applied which entails $s = 0$ and hence $t_1 = 0$ and a normal form. Hence, the sequence terminates.

For the induction step, suppose that for all strongly terminating $s$ such that $\text{val}(s) = d$, the term $t = \text{fold}(s)$ is strongly terminating.

Consider some $s$ that is strongly terminating and $\text{val}(s) = d + 1$. In the reduction $t \rightarrow t_1$, eq. (2) cannot be applied because $\text{val}(s) \neq 0$ and so $s$ is not $0$. Thus, eq. (3) is applied whence $s = \text{Succ}(z)$, for some $z$, and $t_1 = \text{Succ}(' \text{fold}(z))$. Now $\text{val}(z) = d$ so by the induction hypothesis on $d$ we know that 'fold($z$) is strongly terminating. By the basis case of induction on the list, we know $t_1$ is strongly terminating.

Subcase 2b. The sort $i = l + 1, \ldots, n$ is finite.

Only rules (4) and (5) can be applied to the reduction $t \rightarrow t_1$ and in both cases $t_1$ must be a normal form.

Case 3. $\lambda$ is 'Unfold for $1 \leq i \leq n$ and $t = \text{unfold}(s)$.

In the reduction $t \rightarrow t_1$ only eq. (6) and (7) can be applied. The argument that $t$ is strongly normalising follows that of subcase 2a and uses induction on $\text{val}(s)$ in $R_0$.

Case 4. $\lambda$ names a primitive recursive function on $R_1$ from

$$\Delta_1, \ldots, \Delta_q, h_1, \ldots, h_q, g_1, \ldots, g_q$$

Note that $\lambda$ is constructed from functions earlier in the list. There are five subcases corresponding with the five parts of the definition of primitive recursion. We will classify these cases using the function named by $\lambda$.

Subcase 4a. Constant function. $\lambda$ names $\lambda(x_1, \ldots, x_k) = 10$.

If $t = \lambda(s_1, \ldots, s_k)$, then the only equation that applies is (13i) and so $t_1 = 10$ and is a normal form. The sequence halts and $t$ is strongly terminating.
Subcase 4b. Projection. $\lambda$ names $\lambda(x_1, \ldots, x_k) = x_j$.
If $t = \lambda(s_1, \ldots, s_k)$, then the only equation that applied is (13ii). Hence,
$t_1 = s_j$, which is strongly terminating by hypothesis.

Subcase 4c. Successor. $\lambda$ names $\lambda(x) = ^1SUCC(x)$.
If $t = \lambda(s)$, then the only equation that applied is (13iii). Hence, $t_1 = ^1SUCC(s)$, which is strongly terminating by the earlier basis case of this lemma.
Hence, $t$ is strongly terminating.

Subcase 4d. Composition $\lambda$ names
$$
\lambda(x) = \mu_1(x_1, \ldots, \mu_n(x))
$$
where $x = (x_1, \ldots, x_k)$.
If $t = \lambda(s)$, where $s = (s_1, \ldots, s_k)$, then the only equation that applies is (13iv). Then
$$
t_1 = \mu_1(\mu_1(s), \ldots, \mu_n(s)),
$$
where $\mu, \mu_1, \ldots, \mu_n$ name the subfunctions of $\lambda$. Since the $\mu_1, \mu_2, \ldots, \mu_n$ precede $\lambda$ in the list, by the main induction hypothesis we know that $\mu_1(s), \ldots, \mu_n(s)$ are strongly terminating and, further, that $t_1$ is strongly terminating, hence so is $t$.

Subcase 4e. Primitive recursion. $\lambda$ names the function
$$
\lambda(0, x) = \mu_1(x)
$$
$$
\lambda(y + 1, x) = \mu_2(y, x, \lambda(y, x))
$$
where $x = (x_1, \ldots, x_k)$.
Let $t = \lambda(r, s)$ where $s$ is $(s_1, \ldots, s_k)$. The only equations that apply are (13v) and (13vi). We show that $t$ is strongly terminating by induction on the value $val(r)$ in $R_0$.

If $val(r) = 0$ then the only equation that applies is (13v) and $t_1 = \mu_1(s)$. Since $\mu_1$ occurs before $\lambda$ we know that $\mu_1(s)$ is strongly terminating and so is $t$.

If $val(r) > 0$, then we take as induction hypothesis the following: for all strongly terminating $r, s$ such that $val(r) = d$ the term $\lambda(r, s)$ is strongly terminating.

Let $t = \lambda(r, s)$ for $val(r) = d + 1$. The only equation that applies is (13vi). Thus, $r = ^1SUCC(z)$ for some $z$ and
$$
t_1 = \mu_2(z, s, \lambda(z, s)).
$$
By the induction hypothesis on $val(r)$, we know that $\lambda(z, s)$ is strongly terminating, because $val(z) = d$. Therefore, by the main induction hypothesis of 5.3, since $\mu_2$ precedes $\lambda$ in the list, and $z, s, \lambda(z, s)$ are strongly terminating, we know that $t_1$ and hence $t$ are strongly terminating.

Case 5. $\lambda$ is $T_j$ and $t = T_j(r, s, u)$ where $s$ is $(s_1, \ldots, s_k)$.
The only equations that can be applied to the first reduction are (10) and (11). Define
$$
\chi(r, s) = (\mu z)[g(z, val(s)) = 0] - val(r).
$$
We argue using induction on $\chi(r, s)$. 

Basis. \( \chi(r, s) = 0 \).

Subcase a. \( \text{val}(u) = 0 \). Then \( u = 0 \) and the equation used is (10), and \( t_1 = H_j(r, s) \). Since \( H_j \) preceeds \( T_j \) in the list, by induction, since \( r \) and \( s \) are strongly terminating so \( t_1 \) and (hence) \( t \) are strongly terminating.

Subcase b. \( \text{val}(u) \neq 0 \). Then the equation used is (11) and

\[ t_1 = T_j\left(1\text{SUCC}(r), s, G_j(1\text{SUCC}(r), s)\right). \]

First, note that

\[ 1\text{SUCC}(r), s \text{ and } G_j(1\text{SUCC}(r), s) \]

are strongly normalising by hypothesis and/or by induction on the list. It follows that an infinite reduction of \( t_1 \) must involve a further application of eqs. (10) and (11). For this to happen \( G_j(1\text{SUCC}(r), s) \) must reduce to either \( 0 \) or to \( 1\text{SUCC}(z) \) for some \( z \).

Claim. \( \text{val}(G_j(1\text{SUCC}(r), s)) = 0 \).

Proof of Claim. Let \( z_0 = (\mu z)[g_j(z, \text{val}(s)) = 0] \). Since \( \chi(r, s) = 0 \), we have

\[ z_0 < \text{val}(r) < \text{val}(1\text{SUCC}(r)). \]

Now, if \( z_0 < z \) and \( g_j(z_0, x) = 0 \), then \( g_j(z, x) = 0 \). Thus, \( g_j(1\text{SUCC}(r), s) = 0 \) and the claim follows.

By the claim, the subterm of \( t_1 \) reduces to \( 0 \), and \( t_1 \) reduces by (10) to

\[ H_j(\text{SUCC}(r), s), \]

which is strongly terminating by induction on the list.

Induction step. We suppose as induction hypothesis that for any \( r, s, \) and \( u \) that are strongly terminating and \( \chi(r, s) = d, t = T_j(r, s, u) \) is strongly terminating.

Suppose \( \chi(r, s) = d + 1 \).

Case a. \( \text{val}(u) = 0 \). Then the argument is as for case (a) of the basis of this case 5.

Case b. \( \text{val}(u) \neq 0 \). Then the equation used is (11) and

\[ t_1 = T_j\left(1\text{SUCC}(r), s, G_j(1\text{SUCC}(r), s)\right). \]

All subterms are strongly terminating and we note that

\[ \chi^{1\text{SUCC}(r), s} = d \]

by definition of \( \chi \). Thus, by the induction hypothesis on \( \chi(r, s) \) we have that \( t_1 \) and (hence) \( t \) are strongly terminating.

This concludes the case 5.
Case 6. \( \lambda \) is \( F' \) and \( t = F'(s_1, \ldots, s_k) \)

The only equation that applies is (12) which means that

\[
t_1 = T_f(1^0, s_1, \ldots, s_k, 1\text{SUCC}(1^0)),
\]

which is strongly terminating by case 5.

Case 7. \( \lambda \) is \( F \) and \( t = F(s_1, \ldots, s_k) \)

The only equation that applies is (9) which means that

\[
t_1 \equiv \text{UNFOLD}(F'(w^{(1)} \text{FOLD}(s_1), \ldots, w^{(k)} \text{FOLD}(s_k))).
\]

By the previous cases 1, 2, and 6, we deduce that \( t_1 \) and (hence) \( t \) are strongly terminating. Q.E.D.

Up to case 5, where \( T_f \) appears, our proof could be replaced by a shorter but more advanced argument based on the recursive path ordering.

6. Examples of Term Rewriting Specifications

Theorem 1.1 shows that any computable algebra has a finite equational complete TRS specification, but that the number of equations in it may be large (in relation to earlier results) and involves hidden functions. We will show that these features are necessary.

6.1. An Example of a Family of Finite Algebras such that All Complete TRS Equational Specifications Are Dependent on the Size of the Algebras.

Let \( n > 1 \) and \( \Sigma_n \) be the signature

- \text{sort} \quad s
- \text{constants} \quad c_1, \ldots, c_n : s

and consider the \( \Sigma_n \) algebra

\[
A_n = (\{a\} : a, \ldots, a)
\]

wherein the \( n \) constants of \( \Sigma_n \) are identified.

**Theorem 6.1.1.** Let \((\Sigma, E)\) be a finite equational TRS such that \( \Sigma_n \subseteq \Sigma \), \((\Sigma, E)\) is complete and

\[
|E| > n - 1.
\]

**Proof.** Let \( t \in T(\Sigma) \) be the normal form of \( c_1 \). Then, for \( 1 \leq j \leq n \), \( t \) is the normal form of \( c_j \). To see this note that

\[
A_n \models c_1 = c_j
\]

and, because \( A_n \) is specified by \((\Sigma, E)\),

\[
E \models c_1 = c_j
\]

so \( c_1 \) and \( c_j \) have a common reduct because \((\Sigma, E)\) is confluent. Thus, we deduce that at most one of \( c_1, \ldots, c_n \) could be the normal form \( t \).
Suppose that $c_j$ is not the normal form $t$. Then, there must be a rule

$$e_j = l(X) = r(X)$$

that applies to $c_j$ for $X = X_1, \ldots, X_l$. Thus, $l(X) \equiv X_j$ or $l(X) \equiv c_j$.

If $l(X) \equiv X_j$, then the TRS $(\Sigma, E)$ cannot be terminating and indeed according to the definitions $(\Sigma, E)$ does not qualify as a TRS, so we exclude this case and assume that $l(X) \equiv c_j$.

Now for the $n - 1$ cases, where $c_j$ is not a normal form, we obtain $n - 1$ equations $e_j$ with LHS $c_j$. Thus, $|E| > n - 1$. Q.E.D.

6.2. AN EXAMPLE OF AN ALGEBRA SUCH THAT FOR ALL FINITE COMPLETE TRS EQUATIONAL SPECIFICATIONS WITH HIDDEN FUNCTIONS THE NORMAL FORMS MUST INVOLVE THOSE HIDDEN FUNCTIONS. Let $\Sigma_0$ be the signature

- **sorts**
  - nat
  - set

- **constants**
  - $0 : \text{nat}$
  - $\emptyset : \text{set}$

- **operations**
  - $S : \text{nat} \rightarrow \text{nat}$
  - $\text{INS} : \text{nat} \times \text{set} \rightarrow \text{set}$

and let $E_0$ be the set of equations

$$\text{INS}(X, \text{INS}(Y, Z)) = \text{INS}(Y, \text{INS}(X, Z))$$

$$\text{INS}(X, \text{INS}(X, Z)) = \text{INS}(X, Z).$$

The initial algebra of $(\Sigma_0, E_0)$ is isomorphic with

$$F = (N, P_{\text{fin}}(N); 0, \emptyset, n + 1, \text{ins})$$

where $P_{\text{fin}}(N)$ is the set of finite subsets of $N$ and

$$\text{ins} : N \times P_{\text{fin}}(N) \rightarrow P_{\text{fin}}(N)$$

$$\text{ins}(n, A) = \{n\} \cup A.$$ 

This example is taken from Bergstra et al. [1989].

**Theorem 6.2.1.** Let $(\Sigma, E)$ be a finite equational complete TRS specification for the $\Sigma_0$ algebra $F$, so that

$$T(\Sigma, E)|_{\Sigma_0} \equiv F.$$ 

Then there is a $t \in T(\Sigma_0)$ whose normal form $t_1 \in T(\Sigma)$ with respect to $(\Sigma, E)$ does not lie in $T(\Sigma_0)$.

**Proof.** First consider the terms of $T(\Sigma_0)$. Any $t \in T_{\text{nat}}(\Sigma_0)$ has the form $S^l(0)$. Any $t \in T_{\text{set}}(\Sigma_0)$ has the following form:

$$t = \text{INS}(S^{(1)}(0), S^{(2)}(0), \ldots, \text{INS}(S^{(d)}(0), \emptyset), \ldots);$$

we abbreviate $t$ by

$$\text{INS}(l(1), \ldots, l(d), \emptyset),$$

or by $\text{INS}(l, \emptyset)$ for $l = (l(1), \ldots, l(d))$, when convenient.
Now let \((\Sigma, E)\) be a complete TRS specification for the algebra \(F\). Notice that \(E\) cannot contain any rule \(l(X) = r(X)\) where \(l(X)\) and \(r(X)\) are terms of sort \(\text{nat}\). This is because \(T_{\text{nat}}(\Sigma, E)\) is the free term algebra on \(0\) and \(S\), and any rule that is an equation valid in \(F\) would be a syntactic identity that leads to nonterminating derivations using \((\Sigma, E)\).

We define a term \(t \in T_{\text{sep}}(\Sigma_0)\) that will satisfy the conclusion of the theorem. Let \(k = \max(|\text{lhs}(e)| : e \in E) + 1\). Define

\[
t = \text{INS}(S^k(0), \text{INS}(S^{2k}(0), \emptyset)).
\]

Let \(t_1 \in T(\Sigma)\) be the normal form of \(t\).

Suppose for a contradiction \(t_1 \in T(\Sigma_0)\). Let

\[
t_1 = \text{INS}(l(1), \ldots, l(d), \emptyset).
\]

Notice that for \(i = 1, \ldots, d\)

\[
l(i) = k \quad \text{or} \quad l(i) = 2k.
\]

We now take \(t_2 \in T(\Sigma_0)\) to be \(t_1\) with \(S^k(0)\) and \(S^{2k}(0)\) everywhere interchanged, that is,

\[
t_2 = \text{INS}(3k - l(1), \ldots, 3k - l(d), \emptyset).
\]

We know that

\[
F \vdash t_1 = t_2
\]

and so

\[
E \vdash t_1 = t_2
\]

but \(t_2\) is not a normal form of \((\Sigma, E)\) because \(t_1\) is, and \((\Sigma, E)\) is complete.

Hence, there must be a rule that reduces \(t_2\). Let this rule be

\[
l(X_1, \ldots, X_p, Z) \rightarrow r(X_1, \ldots, X_p, Z)
\]

where \(X_1, \ldots, X_p\) are variables of sort \(\text{nat}\) and \(Z\) is a variable of sort \(\text{set}\). The term \(l(X_1, \ldots, X_p, Z)\) matches with \(t_2\) to make the reduction.

CLAIM 6.2.2. \(l(X, Z) = l(X_1, \ldots, X_p, Z)\) matches \(t_1\) and hence \(t_1\) is not a normal form.

PROOF. We claim that the term \(l(X_1, \ldots, X_p, Z)\) must have the form

\[
\text{INS}(S^{M(i)}(X_{\pi(i)}), \ldots, S^{M(q)}(X_{\pi(q)}), Z),
\]

where there are \(q\) locations where \(\text{INS}\) is applied and

\[
\pi: [1, q] \rightarrow [1, p]
\]

defines which variable \(X_{\pi(i)}\) occurs at location \(i\).

To see this structure, note that the alternative is that some \(S^{M(i)}(0)\) occurs at location \(i\). If this occurs in \(l(X_1, \ldots, X_p, Z)\), then it also occurs in \(t_2\), because of the matching. Now \(M(i) < k\) since \(k\) bounds the left hand sides of the rules in \(E\). But every subterm of \(t_2\) of type \(\text{nat}\) is either \(S^k(0)\) or \(S^{2k}(0)\), which is a contradiction.
Now suppose that $\sigma$ is a substitution such that $\sigma(l(X, Z))$ is a subterm of $t_2$. Let

$$\sigma(X_i) = S^{m(i)}(0)$$
$$\sigma(Z) = INS(S^{r(1)}(0), \ldots, S^{r(e)}(0), \emptyset)$$

for $i = 1, \ldots, p$. Note that since $\sigma(Z)$ is a subterm of $t_2$

$$r(i) = k \quad \text{or} \quad r(i) = 2k$$

for $i = 1, \ldots, e$, by the construction of $t_2$ from $t_1$.

We will construct a substitution $\sigma'$ such that $\sigma'(l(X, Z))$ is a subterm of $t_1$. Define $\lambda:[1, p] \rightarrow \mathbb{N}$ by

$$\lambda(i) = m(i) - k \quad \text{if} \quad k < m(i) \leq 2k$$
$$\lambda(i) = m(i) + k \quad \text{otherwise}$$

and set

$$\sigma'(X_i) = S^{\lambda(i)}(0)$$
$$\sigma'(Z) = INS(S^{3k-r(1)}(0), \ldots, S^{3k-r(e)}(0), \emptyset).$$

Thus, in the case of $\sigma'(Z)$, the $S^k(0)$ and $S^{2k}(0)$ in $\sigma(Z)$ are interchanged.

We know that $\sigma(l(X, Z))$ is a subterm of $t_2$. Then we can compare these terms starting from the innermost subterm $Z$. This leads to the following identities between the powers of the numerals: first by matching the subterm $\sigma(Z)$,

$$r(e) = 3k - l(d)$$

$$\vdots$$

$$r(1) = 3k - l(d - e + 1)$$

and next by matching the remainder of $\sigma(l(X, Z))$,

$$M(q) + m(\pi(q)) = 3k - l(d - e)$$

$$\vdots$$

$$M(1) + m(\pi(1)) = 3k - l(d - e - q + 1).$$

To prove the claim, we must prove that $\sigma'(l(X, Z))$ matches $t_1$. This occurs if, and only if, the following identities hold

$$3k - r(e) = l(d)$$

$$\vdots$$

$$3k - r(1) = l(d - e + 1)$$

and

$$M(q) + \lambda(m(\pi(q))) = l(d - e)$$

$$\vdots$$

$$M(q) + \lambda(m(\pi(1))) = l(d - e - q + 1).$$

The set of identities $A_2$ are immediately derivable from $A_1$. Consider the first identity of $B_2$. We will show it is derivable from the first identity of $B_1$, which is

$$M(q) + m(\pi(q)) = 3k - l(d - e).$$
There are two cases:

\[ l(d - e) = k \quad \text{or} \quad l(d - e) = 2k \]

(i) \( l(d - e) = k \). Now \( M(q) + m(\pi(q)) = 2k \). Since \( M(q) < k \) (\( k \) bound LHS of equations) we know \( 2k \geq m(\pi(q)) > k \). Thus, by definition of \( \lambda \),

\[ \lambda(m(\pi(q))) = m(\pi(q)) - k. \]

So substituting,

\[
M(q) + \lambda(m(\pi(q))) = M(q) + m(\pi(q)) - k \\
= 2k - k \\
= k \\
= l(d - e).
\]

(ii) \( l(d - e) = 2k \). Now \( M(q) + m(\pi(q)) = k \). Again \( M(q) < k \) implies \( m(\pi(q)) < k \). So

\[ \lambda(m(\pi(q))) = m(\pi(q)) + k. \]

Substituting

\[
M(q) + \lambda(m(\pi(q))) = M(q) + m(\pi(q)) + k \\
= k + k \\
= 2k \\
= l(d - e).
\]

The other identities of \( B_2 \) follow similarly from corresponding identities of \( B_1 \). Q.E.D.

7. Results on Semicomputable Algebras

We now consider the situation for semicomputable algebras.

7.1. Recursive and RE Specifications of Semicomputable Algebras

**Theorem 7.1.1.** Let \( A \) be a minimal \( \Sigma \) algebra. Then \( A \) is semicomputable if, and only if, \( A \) possesses a recursively enumerable complete TRS specification \( (\Sigma, E) \).

**Proof.** If \( A \) has a recursively enumerable equational specification, then it is semicomputable (Lemma 4.2.3). The argument for the converse follows that of Theorem 4.3.1. Using similar notation, define

\[ E_A = \{ t_1 = t_2 | \gamma^{-1}(t_1) > \gamma^{-1}(t_2) \text{ and } t_1 \equiv_A t_2 \}. \]

Clearly, \( E_A \) is recursively enumerable since \( A \) is semicomputable.

Let \( T_r = \text{im}(nf_r) \) be a transversal for \( \equiv_A \). We claim \( T_r \) is the set of normal forms for the TRS \( (\Sigma, E_A) \). First, the terms in \( T_r \) do not reduce, since neither they nor their subterms occur on the LHS since they are minimal in size (with respect to \( \gamma \)). Any term \( t \notin T_r \) can be reduced since \( t = nf_r(t) \in E_A \).

Thus, \( \text{NF}(\Sigma, E_A) = T_r \).

The TRS \( (\Sigma, E_A) \) is strongly terminating because the monotonic property of \( \gamma \) implies that any reduction \( t \to t' \) entails \( \gamma^{-1}(t) > \gamma^{-1}(t') \).
Ground confluence follows immediately from the fact that every closed term \( t \) can reduce in one step to its normal form \( n(t) \). In order to prove confluence one may use the critical pairs theorem of Knuth and Bendix. Indeed all critical pairs of \((\Sigma, E_A)\) are convergent and \((\Sigma, E_A)\) is terminating, because all reductions lead to shorter terms. See the survey [Klop 1992, 2.4.14].

Since \((\Sigma, E_A)\) is strongly terminating and confluent, it is complete.

Finally, since \(NF(\Sigma, E_A) = T_y\) is a transversal for \( \equiv_A \) and trivially \( A \in ALG(\Sigma, E_A) \) we deduce that

\[
A \equiv T(\Sigma, E_A)
\]

by Lemma 3.4.3. Q.E.D.

**THEOREM 7.1.2.** There is a semicomputable single sorted \( \Sigma \) algebra \( A \) that does not possess a recursive complete TRS specification.

**PROOF.** By Theorem 6.5 in Bergstra and Tucker [1987], there is a semicomputable algebra \( A \) that does not possess a recursive equational specification under initial algebra semantics; this \( A \) does not possess a recursive equational complete TRS specification (Lemma 4.2.3). Q.E.D.

### 7.2. ORTHOGONAL SPECIFICATIONS

**THEOREM 7.2.1.** There is a semicomputable single sorted \( \Sigma \) algebra \( A \) that does not possess a recursively enumerable, complete, orthogonal TRS specification \( (\Sigma, E)\).

**PROOF.** Let \( \{0, 1\}^* \) be the set of finite sequences over \( \{0, 1\} \) and \( \epsilon \in \{0, 1\}^* \) be the empty sequence. Let \( \perp \) be a new symbol.

Consider the algebra

\[
A = (\{0, 1\}^* \cup \{\perp\}, \epsilon, \perp, f, g)
\]

whose unary operations are defined by

\[
f(\perp) = \perp
\]

\[
f(x) = x \cdot 0 \quad \text{if} \quad x \neq \perp
\]

and

\[
g(\perp) = \perp
\]

\[
g(x) = x \cdot 1 \quad \text{if} \quad x \neq \perp.
\]

Let \( Z \subset \{0, 1\}^* \) and assume that

(i) \( Z \) is suffix-closed, that is, for any \( x, y \in \{0, 1\}^* \)

\[
x \in Z \implies x \cdot y \in Z;
\]

(ii) \( Z = \{0, 1\}^* - Z \) is infinite.

Note that from (i) and (ii) it follows that \( \epsilon \notin Z \). If \( Z \) is nonempty, then \( Z \) is infinite.

We define a congruence \( \equiv_Z \) on \( A \) by

\[
x \equiv_Z y \quad \text{if, and only if,} \quad x, y \in Z \cup \{\perp\} \text{ or } x = y.
\]
Let $A_z = A / \equiv_z$.

**Lemma 7.2.2.** $Z$ is recursively enumerable if, and only if $A_z$ is semicomputable.

**Proof.** Immediate. Q.E.D.

We want to choose $Z$ satisfying (i) and (ii) such that

(iii) $Z$ is recursively enumerable
(iv) If $V \subset \{0, 1\}^*$ is infinite and recursively enumerable, then $V \cap Z \neq \emptyset$.

**Lemma 7.2.3.** A $Z$ satisfying (i)–(iv) exists.

**Proof.** Let $\gamma : N \rightarrow \{0, 1\}^*$ be a bijective enumeration of finite strings. Let $\langle W_e, e \in N \rangle$ be an enumeration of the recursively enumerable subsets of $N$ and take $\gamma(W_e), e \in N$ to be an enumeration of the recursively enumerable subsets of $\{0, 1\}^*$. Let

$$Z = \bigcup_n Z_n,$$

where $Z_n$ is defined uniformly in $n$ to be a semicomputable set such that

$$\gamma(W_n) \text{ infinite implies } \gamma(W_n) \cap Z_n \neq \emptyset.$$

The algorithm for $Z_n$ is defined as follows: let

$$c(n) = (\text{least } k | k \in W_n \text{ and } ||\gamma(k)|| > 2n + 1)$$

and set

$$x \in Z_n \iff x \text{ extends the string } \gamma(c(n))$$

for $x \in \{0, 1\}^*$.

First note that $Z$ is infinite and recursively enumerable. Next note, by definition of when $c(n)$ is defined, $Z \cap \gamma(W_n) \neq \emptyset$ for all $n$ such that $W_n$ is infinite.

Finally, we show that $Z^c$ is infinite. Recall the measure $\mu$ on subsets of $\{0, 1\}^*$ defined from

$$\mu(B_x) = \frac{1}{2^{|x|}},$$

where $B_x = \{y \in \{0, 1\}^* | y \text{ extends } x\}$.

Then

$$\mu(Z^c) = 1 - \sum_{n=0}^{\infty} \mu(Z_n)$$

$$= 1 - \sum_{n=0}^{\infty} \frac{1}{2^{2n+1}}$$

$$> 0.$$

Thus, $Z^c$ is infinite. Q.E.D.

Let $\Sigma$ be the signature of $A$:

```
sort s
constants ε, ⊥ : s
operations F : s → s
 G : s → s
```
LEMMA 7.2.4. The algebra $A_z$ does not possess a recursively enumerable orthogonal TRS equational specification which is strongly terminating for ground terms.

PROOF. Suppose for a contradiction that such a specification $(\Sigma, E)$ exists. First note that $E$ is infinite for if $E$ is finite then $(\Sigma, E)$ is a finite complete TRS specification of $A_z$ and this implies $A_z$ is computable, which contradicts the choice of $Z$.

Now let $t_\perp$ be a normal form for $\perp$.

We divide the equations into two sets $E_1$ and $E_2$: let $E = E_1 \cup E_2$ where the equations of $E_2$ are precisely those of $E$ whose LHS have the following forms:

$$\perp, F(t_\perp) \text{ and } G(t_\perp).$$

Notice that $|E_2| \leq 3$ because $E$ is orthogonal and its equations may not overlap.

Hence, we know that $E_1$ is infinite. We will construct from $E_1$ an infinite recursively enumerable subset $X$ of $Z^c$. This will contradict clause (iv) in the definition of $Z$.

We define for $s \in \{0, 1\}^*$ a term $\tau_s(X) \in T(\Sigma, X)$ in the single variable $X$ as follows:

$$\tau_s(X) = X$$
$$\tau_{s.0}(X) = F(\tau_{s.0}(X)) \quad \text{if} \quad s = r \cdot 0$$
$$\tau_{s.1}(X) = G(\tau_{s.1}(X)) \quad \text{if} \quad s = r \cdot 1$$

Now each equation $e \in E_1$ has a LHS of one of the following forms

$$(1) \quad F(\tau_s(X))$$
$$(2) \quad G(\tau_s(X))$$
$$(3) \quad F(\tau_s(e))$$
$$(4) \quad G(\tau_s(e))$$
$$(5) \quad F(\tau_s(\perp))$$
$$(6) \quad G(\tau_s(\perp))$$

for some $s$. In the case of closed terms (3)–(6) we note that $\tau_s(e)$ and $\tau_s(\perp)$ are not syntactically identical to $\perp$. To see this notice that $\tau_s(e)$ or $\tau_s(\perp)$ can only be syntactically identical to $\perp$ if $s = e$; so let us assume this. There are two cases.

(i) If $\perp = t_\perp$, then an equation $e$ with LHS $F(\tau_s(\perp))$ or $G(\tau_s(\perp))$ is in $E_2$ and hence not in $E_1$.

(ii) If $\perp$ is not $t_\perp$, then suppose that $\tau_s(\perp) = \perp$. Now let equation $e$ have $F(\tau_s(\perp)) = F(\perp)$ as a LHS. Then equation $e$ shows an overlap with a rule that allows $\perp$ to reduce which must exist since $\perp$ is not syntactically equal to its normal form $t_\perp$. This contradicts the orthogonality of $E$.

Further, we note that $e$ cannot be a LHS of $e \in E_1$, since it is a normal form; this follows from the fact that no other term has value $[e] \in A/\equiv_Z$. Q.E.D.

CLAIM 7.2.5. If $e \in E_1$ has a form (1)–(6) with index $s \in \{0, 1\}^*$, then $s \notin Z$.

Assuming this claim, we can complete the argument of Lemma 7.2.4 as follows: Let

$$X = \{s \in \{0, 1\}^*: s \text{ is an index for an equation } e \in E_1 \text{ of form (1)–(6)}\}.$$
Since $E_1$ is infinite and recursively enumerable, we have that $X$ is infinite and recursively enumerable. By claim, $X \subseteq Z^c$. This is the desired contradiction of clause (iv).

**Proof of Claim 7.2.5.** We argue by contradiction: Suppose $e \in E_1$. There are six cases, depending on the form of $e \in E_1$.

First, we show that forms (5) and (6) cannot arise with index $s$ in $Z$; we consider case (5) only, as (6) is similar. Observe that

$$A_Z \models \tau_s(\bot) = \bot \quad \text{and} \quad A_Z \models \bot = t_\bot.$$  

Hence, $\tau_s(\bot)$ and $t_\bot$ have a common reduct $t_\bot$; a rewriting is necessary because $\tau_s(\bot)$ is not $\bot$. The equation that performs this rewrite must overlap with the equation $e$ of type (5). Thus, $e$ does not exist.

Now, we show that the forms (3) and (4) cannot arise with index $s$ in $Z$; we consider case (3) only, as (4) is similar. Since $s \in Z$

$$A_Z \models \tau_s(e) = \bot \quad \text{and} \quad A_Z \models \bot = t_\bot.$$  

Hence, $\tau_s(e)$ and $t_\bot$ have a common reduct. Again the existence of a rewrite implies that an equation overlaps $e$ and contradicts orthogonality. So $e$ with index $s \in Z$ does not exist.

Finally, we consider forms (1) and (2); (2) is similar to (1). If $s \in Z$, then on substituting $e$ in $\tau_s(X)$ we obtain

$$A_Z \models \tau_s(e) = \bot \quad \text{and} \quad A_Z \models \bot = t_\bot.$$  

Thus there is a reduction of $\tau_s(e)$ to $t_\bot$ and, since $e$ is a normal form, this rewrite involves function symbols in $\tau_s(X)$. It follows that the first reduction of $\tau_s(e)$ is performed by an equation that overlaps with $e$, which is the desired contradiction. Q.E.D.

8. **Concluding Remarks**

We conclude that complete term rewriting systems are adequate for the equational specification of computable data types. Hidden functions will often be needed and the use of hidden functions in normal forms cannot, in general, be avoided. An open question is this: Under what conditions can a computable data type be specified using a complete equational term rewriting system involving hidden functions and whose normal forms do not use the hidden functions?

We think that the development of many sorted term rewriting is an interesting and useful project. Arising in our work is the topic of the relationship between term rewriting systems over many sorted signatures with common subsignatures. Perhaps, new many sorted modularity results for term rewriting systems could lead to an easy and satisfying proof of many sorted case of Theorem 1.1 from a proof of the single sorted case.

**References**


RECEIVED AUGUST 1992; REVISED NOVEMBER 1994; ACCEPTED JUNE 1995