Decision Procedures for Proving Inductive Theorems without Induction

Takahito Aoto, Sorin Stratulat

Decision Procedures for Proving Inductive Theorems without Induction

Takahito Aoto
RIEC, Tohoku University
email: aoto@nie.riec.tohoku.ac.jp

Sorin Stratulat
LITA, University of Lorraine
email: sorin.stratulat@univ-lorraine.fr

Abstract

Automated inductive reasoning for term rewriting has been extensively studied in the literature. Classes of equations and term rewriting systems (TRSs) with decidable inductive validity have been identified and used to automatize the inductive reasoning. We give procedures for deciding the inductive validity of equations in some standard TRSs on natural numbers and lists. Contrary to previous decidability results, our procedures can automatically decide *without* involving induction reasoning the inductive validity of *arbitrary* equations for these TRSs, that is, without imposing any syntactical restrictions on the form of equations. We also report on the complexity of our decision procedures. These decision procedures are implemented in our automated provers for inductive theorems of TRSs and experiments are reported.

Categories and Subject Descriptors F.3.1 [*Specifying and Verifying and Reasoning about Programs*]: Mechanical verification; F.4.1 [*Mathematical Logic*]: Mechanical theorem proving; I.2.3 [*Deduction and Theorem Proving*]: Deduction; F.4.2 [*Grammars and Other Rewriting Systems*]: Decision problems

Keywords Inductive Theorems, Term Rewriting Systems, Decision Procedure, Initial Algebra

1. Introduction

Inductive reasoning on recursively defined data structures is ubiquitous in the verification of formal specifications and software. In equational logic, the properties to be checked are formalized as *inductive theorems* of *term rewriting systems* (*TRS*s for short). It is known that the methods for automatically proving inductive theorems of TRSs easily diverge, the construction of effective inductive theorem provers still remaining a hard challenge [15].

In [21], Kapur and Subramaniam initiated the problem of identifying classes of conjectures and TRSs for which automated inductive proof methods provide *decision procedures*. More precisely, they gave syntactic conditions on structure of (recursive) function definitions and of conjectures, and showed that if one runs a (prefixed) *implicit* induction method in a (prefixed) particular strategy for any conjecture and TRS satisfying these conditions, then it never diverges and positive/negative answer is found always. This approach has been extended with other authors to more general TRSs and classes of conjectures in [11–14, 23].

Our work is motivated by strengthening the power of automated inductive reasoning, by invoking such decision procedures for inductive theorems, inside automated induction provers such as the authors' [2, 28]. It is well accepted that, often, a key ingredient of successful induction reasoning is the use of subsidiary lemmas [15], and thus various methods for automatically generating lemmas have been inspected [3, 26, 31, 32]. But, as one might expect, lemma generation methods often generate many incorrect conjectures. Even if decision procedures are only effective for restricted subclasses, and even if the given conjecture and TRS do not fall inside the scope of these classes, decision procedures could be helpful for solving these lemma candidates, often automatically generated while searching a successful inductive reasoning.

The decidability results obtained by the approach mentioned above, however, turned out to be not very helpful for this purpose. This is because usually conjectures satisfying the syntactic conditions of decision procedures can already be proved solely by the automated induction provers, as these decision procedures and the automated induction provers are basically based on similar induction methods. This motivates us to investigate different approaches for obtaining classes of equations and TRSs with decidable inductive validity.

In this paper, we propose a new approach for deciding inductive theorems of TRSs. Our essential idea is to use the validity in the *initial algebras* of TRSs, instead of the validity guaranteed by the existence of inductive proofs. For equations and TRSs, it is known that the inductive validity and the validity in initial algebras coincide. Thus, if we can decide the validity in initial algebras of TRSs, then we get a decision procedure for inductive theorems of TRSs. Furthermore, this approach is completely different from finding induction proofs and it does not suffer from the weakness of the Kapur and Subramaniam's approach when used inside the general automated induction proving methods.

Our approach seems very natural but, at the best of our knowledge, such approach for proving inductive theorems has not been investigated, albeit the usability of decidable arithmetic theories for building induction schemes has been investigated in [8, 20]. An obvious weakness of our approach is that it works only for specific TRSs. On the other hand, our decision procedures impose no syntactical conditions on the equations and do not require induction reasoning, contrary to the known decision procedures for inductive theorems. It may be also considered as a weakness that our approach does not provide induction proofs, which may be helpful to give a strategy for constructing proofs in formal proof systems such as Isabelle/HOL [24]. On the other hand, our approach may have a similarity to the *normalization by evaluation* technique, which

PPDP '14, September 8–10, 2014, Canterbury, UK.

http://dx.doi.org/10.1145/2643135.2643156

accomplishes the syntactic goal (normalization) using semantics (evaluation).

Because of the nature of our approach, our decision procedures consist in checking the validity of equations in some models of TRSs, i.e. in algebras. Hence, our decision procedures presented can be fallen in the more general category of automated proving methods. Naturally, the decidability of Presburger arithmetic (PA) turned out to be very useful. In fact, one of our decidability results is subsumed by the one using encoding to PA formulas theoretically. Throughout the paper, we also explain when known methods for proving the validity of (initial) algebras are available—but we would stress here that our central idea is rather not the introduction of the decision procedures for these algebras, but their application to obtain decision procedures for inductive theorems.

The rest of the paper is organized as follows. Section 2 covers preliminaries. In Section 3, we give an exponential procedure for deciding the inductive validity of the TRS consisting of the addition and multiplication on natural numbers. Then, we extend our decision procedure by incorporating some standard list functions such as *append*, *reverse* and *length* in Section 4. In Section 5, we present some decision procedures for the inductive theorems of the TRS with *max* and *min* functions on natural numbers. In Section 6, we report on the implementation and experiments. Section 7 concludes. Some of proofs have been put in the appendix.

2. Preliminaries

We assume basic familiarity with term rewriting and semantics of equational logic [5, 19].

A many-sorted signature $\Sigma = \langle \mathcal{S}, \mathcal{F} \rangle$ consists of the set $\mathcal{S}$ of sorts and the set $\mathcal{F}$ of many-sorted function symbols; $f : \alpha_1 \times \cdots \times \alpha_n \to \alpha_0$, with $\alpha_i \in \mathcal{S}$ and $i, n \geq 0$, denotes the signature of a function symbol $f \in \mathcal{F}$. If $\mathcal{S}$ is a singleton set, say $\{\alpha\}$, then the many-sorted signature is called a first-order signature. In this case, $\alpha_1 \times \cdots \times \alpha_n \to \alpha_0$ is abbreviated by n, and $f : \alpha_1 \times \cdots \times \alpha_n \to \alpha_0$ by $f^{(n)}$.

The $\mathcal{S}$-sorted variables (or variables) are $\mathcal{V} = \biguplus_{\alpha \in \mathcal{S}} \mathcal{V}^\alpha$, where each $\mathcal{V}^\alpha$ is disjoint from the others. The set $\mathrm{T}(\Sigma, \mathcal{V})^\alpha$ of Σ-terms (or *terms*) of sort $\alpha \in \mathcal{S}$ is inductively defined by (1) $\mathcal{V}^\alpha \subseteq \mathrm{T}(\Sigma, \mathcal{V})^\alpha$ and (1) if $f : \alpha_1 \times \cdots \times \alpha_n \to \alpha \in \mathcal{F}$ and $t_i \in \mathrm{T}(\Sigma, \mathcal{V})^{\alpha_i}$ for $i = 1, \ldots, n$, then $f(t_1, \ldots, t_n) \in \mathrm{T}(\Sigma, \mathcal{V})^\alpha$. The set of terms is given by $\mathrm{T}(\Sigma, \mathcal{V}) = \bigcup_{\alpha \in \mathcal{S}} \mathrm{T}(\Sigma, \mathcal{V})^\alpha$. The set of variables (function symbols) in a term t is denoted by $\mathcal{V}(t)$ ($\mathcal{F}(t)$, respectively). A term t is said to be *ground* if $\mathcal{V}(t) = \emptyset$. We denote an empty sequence by ϵ, and the *positions* in a term t, denoted by $\mathrm{Pos}(t)$, by sequences of natural numbers. The symbol at a position $p \in \mathrm{Pos}(t)$ is denoted by $t(p)$, the subterm at a position $p \in \mathrm{Pos}(t)$ by $t|_p$, and the term replacing $t|_p$ with a term s of the same sort by $t[s]_p$. A *context* is a term t possibly containing holes $\Box$. The term obtained from a context C by replacing the holes with terms $s_1, \ldots, s_n$ of appropriate sort from left to right is denoted by $C[s_1, \ldots, s_n]$. A *substitution* is a finite mapping $\sigma : \mathcal{V} \to \mathrm{T}(\Sigma, \mathcal{V})$ such that (1) $\mathrm{dom}(\sigma) = \{x \in \mathcal{V} \mid \sigma(x) \neq x\}$ is finite and (2) $x \in \mathcal{V}^\alpha$ implies $\sigma(x) \in \mathrm{T}(\Sigma, \mathcal{V})^\alpha$. Each substitution is identified with its homomorphic extension $\mathrm{T}(\Sigma, \mathcal{V}) \to \mathrm{T}(\Sigma, \mathcal{V})$. A substitution is said to be *ground* if $\sigma(x)$ is ground for any $x \in \mathrm{dom}(\sigma)$. Ground substitutions will be subscripted by g, for example θ_g. We write $t\sigma$ for $\sigma(t)$ and call it an *instance* of t. It is a *ground instance* if $t\sigma$ is ground. We assume that when we write $t\sigma_g$, $t\sigma_g$ is a ground instance, i.e., $\mathcal{V}(t) \subseteq \mathrm{dom}(\sigma_g)$.

A Σ-equation (or equation) $s \approx t$ is a pair of Σ-terms having the same sort. A Σ-equation $l \approx r$ satisfying $\mathcal{V}(r) \subseteq \mathcal{V}(l), l \notin \mathcal{V}$ is called a Σ-*rewrite rule* (or rewrite rule), in which case, $l \approx r$ may be written as $l \to r$. A *term rewriting system* (*TRS* for short) is a finite set of rewrite rules. Let $\mathcal{R}$ be a TRS. If $l \to r \in \mathcal{R}$, we write $s \to_{\mathcal{R}} t$ if there exist $p \in \mathrm{Pos}(s)$ and substitution σ such that $s|_p = l\sigma$ and $s[r\sigma]_p = t$. We call $s \to_{\mathcal{R}} t$ a *rewrite step* (from s to t). The reflexive transitive (equivalence) closure of $\to_{\mathcal{R}}$ is denoted by $\xrightarrow{*}_{\mathcal{R}}$ ($\overset{*}{\leftrightarrow}_{\mathcal{R}}$, respectively). A term s is said to be $\mathcal{R}$-*normal* if $s \to_{\mathcal{R}} t$ for no term t. The set of $\mathcal{R}$-normal terms is denoted by $\mathrm{NF}(\mathcal{R})$. If $s \xrightarrow{*}_{\mathcal{R}} t$ and $t \in \mathrm{NF}(\mathcal{R})$, then t is said to be the $\mathcal{R}$-*normal form* of s. A TRS $\mathcal{R}$ is *terminating* if $\to_{\mathcal{R}}$ is well-founded; $\mathcal{R}$ is *confluent* if $\xleftarrow{*}_{\mathcal{R}} \circ \xrightarrow{*}_{\mathcal{R}} \subseteq \xrightarrow{*}_{\mathcal{R}} \circ \xleftarrow{*}_{\mathcal{R}}$; $\mathcal{R}$ is *convergent* if it is terminating and confluent. If $\mathcal{R}$ is a convergent TRS, any term s has a unique $\mathcal{R}$-normal form, denoted by $s{\downarrow_{\mathcal{R}}}$. Let $\mathcal{D} = \{l(\epsilon) \mid l \to r \in \mathcal{R}\}$. A TRS $\mathcal{R}$ is *sufficiently complete* if, for any ground term t there exists a ground term s such that $t \overset{*}{\leftrightarrow}_{\mathcal{R}} s$ and $\mathcal{F}(s) \cap \mathcal{D} = \emptyset$. The subscript $\mathcal{R}$ will be omitted if no confusion arises.

The equation $s \approx t$ is an *inductive theorem* of a TRS $\mathcal{R}$, denoted by $\mathcal{R} \models_{ind} s \approx t$, if $s\theta_g \overset{*}{\leftrightarrow}_{\mathcal{R}} t\theta_g$, for any ground substitution θ_g. Extended to any set E of equations, we write $\mathcal{R} \models_{ind} E$ if $\mathcal{R} \models_{ind} s \approx t$, for all $s \approx t \in E$.

Given a many-sorted signature $\Sigma = \langle \mathcal{S}, \mathcal{F} \rangle$, a Σ-*algebra* is a pair $\mathcal{A} = \langle \langle A^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}} \rangle_{f \in \mathcal{F}} \rangle$ of tuples where A^α ($\alpha \in \mathcal{S}$) are mutually disjoint, and $f^{\mathcal{A}}$ is a mapping $A^{\alpha_1} \times \cdots \times A^{\alpha_n} \to A^{\alpha_0}$, for each $f : \alpha_1 \times \cdots \times \alpha_n \to \alpha_0 \in \mathcal{F}$. The set $A = \biguplus_{\alpha \in \mathcal{S}} A^\alpha$ is called the *carrier set* of the Σ-algebra $\mathcal{A}$ and denoted by $|\mathcal{A}|$. If $\mathcal{S} = \{\alpha_1, \ldots, \alpha_m\}$ and $\mathcal{F} = \{f_1, \ldots, f_k\}$, $\mathcal{A}$ is written like $\langle A^{\alpha_1}, \ldots, A^{\alpha_m}; f_1^{\mathcal{A}}, \ldots, f_k^{\mathcal{A}} \rangle$. The Σ-term algebra is a Σ-algebra $\mathcal{A} = \langle \langle A^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}} \rangle_{f \in \mathcal{F}} \rangle$ given by $A^\alpha = \mathrm{T}(\Sigma, \mathcal{V})^\alpha$ for each $\alpha \in \mathcal{S}$ and $f_i^{\mathcal{A}}(s_1, \ldots, s_n) = f_i(s_1, \ldots, s_n)$, for any $f_i \in \mathcal{F}$. The Σ-term algebra is denoted by $\mathcal{T}_\Sigma(\mathcal{V})$. Similarly, we can define a ground Σ-term algebra as $\mathcal{T}_\Sigma(\emptyset)$, which will be denoted by $\mathcal{T}_\Sigma$.

A *valuation* on a Σ-algebra $\mathcal{A}$ is a tuple $\rho = \langle \rho_\alpha \rangle_{\alpha \in \mathcal{S}}$ of mappings $\rho_\alpha : \mathcal{V}^\alpha \to A^\alpha$. We abbreviate $\rho_\alpha(x)$ (with $x \in \mathcal{V}^\alpha$) as $\rho(x)$. Given a many-sorted signature $\Sigma = \langle \mathcal{S}, \mathcal{F} \rangle$ and a Σ-algebra $\mathcal{A} = \langle \langle A^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}} \rangle_{f \in \mathcal{F}} \rangle$, we define the interpretation $[\![t]\!]_{\mathcal{A},\rho}$ (which is abbreviated as $[\![t]\!]_\rho$ for brevity) of a Σ-term t on $\mathcal{A}$ w.r.t. a valuation ρ on $\mathcal{A}$ like this: $[\![x]\!]_\rho = \rho(x)$ and $[\![f(t_1, \ldots, t_n)]\!]_\rho = f^{\mathcal{A}}([\![t_1]\!]_\rho, \ldots, [\![t_n]\!]_\rho)$. It is easily shown that $[\![t]\!]_\rho \in A^\alpha$, for each $t \in \mathrm{T}(\Sigma, \mathcal{V})^\alpha$. A Σ-equation $s \approx t$ is *valid* on a Σ-algebra $\mathcal{A}$ (denoted by $\mathcal{A} \models s \approx t$) if $[\![s]\!]_\rho = [\![t]\!]_\rho$, for any valuation ρ on $\mathcal{A}$. For set E of equations, $\mathcal{A} \models E$ is defined by $\mathcal{A} \models s \approx t$, for all $s \approx t \in E$.

Let $\mathcal{A} = \langle \langle A^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}} \rangle_{f \in \mathcal{F}} \rangle$, $\mathcal{B} = \langle \langle B^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{B}} \rangle_{f \in \mathcal{F}} \rangle$ be Σ-algebras. A Σ-*homomorphism* σ from $\mathcal{A}$ to $\mathcal{B}$ is a tuple $\sigma = \langle \sigma_\alpha \rangle_{\alpha \in \mathcal{S}}$ of mappings $\sigma_\alpha : A^\alpha \to B^\alpha$ such that $\sigma_\alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\sigma_{\alpha_1}(a_1), \ldots, \sigma_{\alpha_n}(a_n))$, for each $f : \alpha_1 \times \cdots \times \alpha_n \to \alpha \in \mathcal{F}$. If $\mathcal{S} = \{\alpha\}$ then σ is identified with σ_α. Two Σ-algebras $\mathcal{A}$ and $\mathcal{B}$ are *isomorphic* (denoted by $\mathcal{A} \cong \mathcal{B}$) if there exists a Σ-homomorphism σ consisting of bijective mappings. Isomorphic Σ-algebras can be often identified.

Let $\Sigma = \langle \mathcal{S}, \mathcal{F} \rangle$ be a signature and $\mathcal{A} = \langle \langle A^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}} \rangle_{f \in \mathcal{F}} \rangle$ a Σ-algebra. An equivalence relation $\sim$ on A is said to be a *congruence* (on $\mathcal{A}$) if (1) $a \sim b$ implies $a, b \in A^\alpha$ for some $\alpha \in \mathcal{S}$, and (2) for any $f \in \mathcal{F}$ and $1 \leq i \leq n$, $a_i \sim b_i$ implies $f^{\mathcal{A}}(a_1, \ldots, a_n) \sim f^{\mathcal{A}}(b_1, \ldots, b_n)$. We denote the $\sim$-*equivalence class* of $a \in A$ by $[a]_\sim$. If $\sim$ is a congruence on $\mathcal{A}$ then we obtain its *quotient* Σ-*algebra* $\mathcal{A}/\sim = \langle \langle (A/\sim)^\alpha \rangle_{\alpha \in \mathcal{S}}, \langle f^{\mathcal{A}/\sim} \rangle_{f \in \mathcal{F}} \rangle$ by defining $(A/\sim)^\alpha = \{[a]_\sim \mid a \in A^\alpha\}$ and $f^{\mathcal{A}/\sim}([a_1]_\sim, \ldots, [a_n]_\sim) = [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\sim$.

Let $\mathcal{K}$ be a class of Σ-algebras. A Σ-algebra $\mathcal{A}$ is said to be *initial* in $\mathcal{K}$ if, for any $\mathcal{B} \in \mathcal{K}$, there exists a unique Σ-homomorphism $\mathcal{A} \to \mathcal{B}$. The initial algebras are unique up to isomorphism. Let $\mathcal{R}$ be a TRS, and $\mathcal{K}$ be the class of Σ-algebras satisfying $\mathcal{R}$, i.e., $\mathcal{K} = \{\mathcal{A} \mid \mathcal{A} \models \mathcal{R}\}$. Then the quotient ground Σ-term algebra $\mathcal{T}_\Sigma / \overset{*}{\leftrightarrow}_{\mathcal{R}}$ is initial in $\mathcal{K}$, which is called the *initial* Σ-*algebra* of $\mathcal{R}$,

and denoted by $\mathcal{I}_{\mathcal{R}}$. Validity on initial algebras and inductive theorems correspond in the following way.

PROPOSITION 2.1 (e.g., [19]). *Let $\mathcal{R}$ be a TRS over signature Σ and $s, t \in \mathrm{T}(\Sigma, \mathcal{V})$. An equation $s \approx t$ is an inductive theorem of $\mathcal{R}$ iff it is valid in the initial Σ-algebra of $\mathcal{R}$.*

3. Deciding Inductive Theorems on Natural Numbers with Addition and Multiplication

In this section, we consider a first-order signature $\Sigma_{(\times,+,\mathsf{s},0)} = \langle\{N\}, \mathcal{F}_{(\times,+,\mathsf{s},0)}\rangle$, where $\mathcal{F}_{(\times,+,\mathsf{s},0)} = \{\times^{(2)}, +^{(2)}, \mathsf{s}^{(1)}, \mathsf{0}^{(0)}\}$. Let $\mathcal{R}_{(\times,+)}$ be the following TRS over $\Sigma_{(\times,+,\mathsf{s},0)}$ that defines the multiplication and addition on natural numbers encoded by $\mathsf{0}$ and the successor function s.

$$\mathcal{R}_{(\times,+)} = \left\{ \begin{array}{lcl} +(\mathsf{0}, y) & \to & y \\ +(\mathsf{s}(x), y) & \to & \mathsf{s}(+(x, y)) \\ \times(\mathsf{0}, y) & \to & \mathsf{0} \\ \times(\mathsf{s}(x), y) & \to & +(\times(x, y), y) \end{array} \right\}$$

We present a decision procedure for $\mathcal{R}_{(\times,+)} \models_{ind} s \approx t$ with $s, t \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)}, \mathcal{V})$.

Let $\mathbb{N}_{(\times,+,\mathsf{s},0)} = \langle \mathbb{N}; \times^{\mathbb{N}}, +^{\mathbb{N}}, \mathsf{s}^{\mathbb{N}}, \mathsf{0}^{\mathbb{N}}\rangle$ be a $\Sigma_{(\times,+,\mathsf{s},0)}$-algebra, where $\mathbb{N}$ is the set of natural numbers, $\times^{\mathbb{N}}$ and $+^{\mathbb{N}}$ are multiplication and addition on natural numbers, respectively, and $\mathsf{s}^{\mathbb{N}}(n) = n + 1$ and $\mathsf{0}^{\mathbb{N}} = 0$.

A key fact of our decision procedure is the following.

LEMMA 3.1. *The initial $\Sigma_{(\times,+,\mathsf{s},0)}$-algebra of $\mathcal{R}_{(\times,+)}$ is isomorphic to $\mathbb{N}_{(\times,+,\mathsf{s},0)}$.*

Let us next consider a first-order signature $\Sigma_{(\times,+,1,0)} = \langle\{N\}, \mathcal{F}_{(\times,+,1,0)}\rangle$, where $\mathcal{F}_{(\times,+,1,0)} = \{\times^{(2)}, +^{(2)}, 1^{(0)}, 0^{(0)}\}$. The sets of natural numbers and integers equipped with the usual operations of multiplication, addition, 1 and 0 form $\Sigma_{(\times,+,1,0)}$-algebras $\langle\mathbb{N}; \times, +, 1, 0\rangle$ and $\langle\mathbb{Z}; \times, +, 1, 0\rangle$, which will be abbreviated as $\mathbb{N}$ and $\mathbb{Z}$, respectively, in what follows.

For $\Sigma_{(\times,+,1,0)}$-algebra $K = \langle |K|; \times, +, 1, 0\rangle$, the carrier set $|K|$ will be identified with K. Let $\Sigma_{(\times,+,1,0)}$-algebra $K = \langle |K|; \times, +, 1, 0\rangle$ be *commutative ring*. A *zero* ring is a ring with a singleton carrier set where we have $0 = 1$. A nonzero commutative ring K is said to be an *integral domain* if $a \times b \neq 0$ for any $a, b \in K$ such that $a \neq 0$ and $b \neq 0$.

The *polynomial ring* over a commutative ring K and *indeterminates* $x_1, \ldots, x_n$ is denoted by $K[x_1, \ldots, x_n]$. Elements of $K[x_1, \ldots, x_n]$ are called K-polynomials; each element has its *canonical expression* $C_1 x_1^{m_1^1} \cdots x_n^{m_n^1} + \cdots + C_k x_1^{m_1^k} \cdots x_n^{m_n^k}$, where $C_i \in K \setminus \{0\}$ and each tuple $(m_1^i, \ldots, m_n^i) \in \mathbb{N}^n$ is distinct, for all $1 \leq i \leq k$. (Here, we use the usual abbreviation of multiplication.) The set $K[x_1, \ldots, x_n]$ forms an integral domain with the usual multiplication and addition operations on K-polynomials, 1 and 0 from K. For any $a_1, \ldots, a_n \in K$ and any $\varphi \in K[x_1, \ldots, x_n]$, we denote by $\varphi(a_1, \ldots, a_n)$ the element in K obtained by replacing each x_i with a_i in the canonical expression of φ and applying operations over K according to the canonical expression. For example, if we take the ring $K = \mathbb{Z}$ of integers and $\varphi = 2x^2y + 3xy^2 + 1 \in \mathbb{Z}[x, y]$ then $\varphi(1, 1) = 2 \times 1^2 \times 1 + 3 \times 1 \times 1^2 + 1 = 6 \in \mathbb{Z}$. For any $a_1, \ldots, a_n \in K$, the mapping $\varphi \mapsto \varphi(a_1, \ldots, a_n)$ is a ring homomorphism $K[x_1, \ldots, x_n] \to K$.

For each $\Sigma_{(\times,+,1,0)}$-algebra $K = \langle |K|; \times, +, 1, 0\rangle$, we define its *counterpart* $\Sigma_{(\times,+,\mathsf{s},0)}$-algebra $K^\circ = \langle |K|; \times, +, \mathsf{s}^\circ, 0\rangle$ by putting $\mathsf{s}^\circ(x) = x + 1$. Then, clearly $\mathbb{N}^\circ \cong \mathbb{N}_{(\times,+,\mathsf{s},0)}$ and $\mathbb{Z}^\circ \cong \mathbb{Z}_{(\times,+,\mathsf{s},0)}$. The formal polynomial $(\!|t|\!)_K$ of t over the indeterminates $x_1, \ldots, x_n$ is an element in $K[x_1, \ldots, x_n]$ defined inductively as $(\!|\times(t_1, t_2)|\!)_K = (\!|t_1|\!)_K \times (\!|t_2|\!)_K$, $(\!|+(t_1, t_2)|\!)_K = (\!|t_1|\!)_K + (\!|t_2|\!)_K$, $(\!|\mathsf{s}(t)|\!)_K = (\!|t|\!)_K + 1$, $(\!|\mathsf{0}|\!)_K = 0$ and $(\!|x_i|\!)_K = x_i$. If obvious, the subscript K of $(\!|t|\!)_K$ is omitted. Note that $(\!|s|\!)(a_1, \ldots, a_n) \in K$ for any $a_1, \ldots, a_n \in K$.

LEMMA 3.2. *Let K be a commutative ring, $s \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)}, \{x_1, \ldots, x_n\})$, and $(\!|s|\!)_K$ the formal polynomial of s over the indeterminates $x_1, \ldots, x_n$. Then, for any valuation ρ on K°, we have $[\![s]\!]_{K^\circ,\rho} = (\!|s|\!)_K(\rho(x_1), \ldots, \rho(x_n))$.*

The correctness of our decision procedure is guaranteed by the following basic property on polynomials.

PROPOSITION 3.3 (e.g., [33]). *Let K be an integral domain and $\varphi, \psi \in K[x_1, \ldots, x_n]$. Suppose that there exist infinite sets $M_1, \ldots, M_n \subseteq K$ such that $\varphi(a_1, \ldots, a_n) = \psi(a_1, \ldots, a_n)$, for any $a_1 \in M_1, \ldots, a_n \in M_n$. Then, $\varphi = \psi$.*

Since $\mathbb{Z}$ is an integral domain and $\mathbb{N} \subseteq \mathbb{Z}$ is infinite, we have

LEMMA 3.4. *Suppose $s, t \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)}, \mathcal{V})$ and $\mathcal{V}(s) \cup \mathcal{V}(t) \subseteq \{x_1, \ldots, x_n\}$. Let $(\!|s|\!), (\!|t|\!) \in \mathbb{Z}[x_1, \ldots, x_n]$ be formal polynomials of s, t over the indeterminates $x_1, \ldots, x_n$, respectively. Then $\mathbb{N}_{(\times,+,\mathsf{s},0)} \models s \approx t$ iff $(\!|s|\!) = (\!|t|\!)$.*

THEOREM 3.5. *It is decidable in exponential time for given $s, t \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)}, \mathcal{V})$ whether the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\times,+)}$.*

Proof: From Proposition 2.1 and Lemma 3.1, it suffices to show $\mathbb{N}_{(\times,+,\mathsf{s},0)} \models_{ind} s \approx t$ is decidable in exponential time. Hence, by Lemma 3.4, it remains to give an exponential procedure to decide $(\!|s|\!)_{\mathbb{Z}} = (\!|t|\!)_{\mathbb{Z}}$ for given $s, t \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)}, \mathcal{V})$. First we translate $s \in \mathrm{T}(\{\mathsf{0}, \mathsf{s}, +, \times\}, \mathcal{V})$ to $\hat{s} \in \mathrm{T}(\{+, \times\} \cup \mathbb{N}, \mathcal{V})$ by replacing every subterm $\mathsf{s}^n(t)$ such that $t(\epsilon) \neq \mathsf{s}$ with $+(t, n)$ recursively, and eliminating $\mathsf{0}$. Clearly, the translation from s to $\hat{s}$ can be done in $\mathcal{O}(|s|)$, and we have $|\hat{s}| \leq 2 \times |s|$, where $|\cdot|$ is the *size* operator. Let a *monomial expression* be $\langle n, \{x_1, \ldots, x_p\}_m\rangle$, where $n, p \in \mathbb{N}$ and $\{x_1, \ldots, x_p\}_m$ is a multiset of variables. Then one can compute the list $\mathsf{Mono}(\hat{s})$ of monomial expressions from $\hat{s}$ recursively like this: $\mathsf{Mono}(x) = [\langle 1, \{x\}_m\rangle]$; $\mathsf{Mono}(n) = [\langle n, \{\}_m\rangle]$; $\mathsf{Mono}(+(u_1, u_2)) = \mathsf{Mono}(u_1)@\mathsf{Mono}(u_2)$, where @ is the concatenation operator for lists; $\mathsf{Mono}(\times(u_1, u_2)) = [\langle n \times m, N \uplus M\rangle \mid \langle n, N\rangle \in \mathsf{Mono}(u_1), \langle m, M\rangle \in \mathsf{Mono}(u_2)]$. Clearly this computation can be done in $\mathcal{O}(2^{|\hat{s}|})$ and $|\mathsf{Mono}(\hat{s})|$ is $\mathcal{O}(2^{|\hat{s}|})$. Finally, check whether $\mathsf{Mono}(\hat{s})$ and $\mathsf{Mono}(\hat{t})$ denote the same formal polynomial, i.e., $\sum\{n \mid \langle n, N\rangle \in \mathsf{Mono}(\hat{s})\} = \sum\{m \mid \langle m, N\rangle \in \mathsf{Mono}(\hat{t})\}$, for each N such that $\langle n, N\rangle \in \mathsf{Mono}(\hat{s}) \cup \mathsf{Mono}(\hat{t})$ for some n. This can be done in $\mathcal{O}((|\mathsf{Mono}(\hat{s})| + |\mathsf{Mono}(\hat{t})|)^2)$. Thus the overall procedure can be done in exponential time. □

The complexity of derivations in an equational proof system for showing the identity of two formal polynomials has been studied in [18]. Randomized algorithms for effectively checking the identity of formal polynomials have been studied, e.g., in [9, 25]. Thus, Theorem 3.5 may be folklore but we could not find any literature which reports on this. It is also known that even if we incorporate the exponential function, the validity of equations on natural numbers is decidable [10]. However, the underlying decision procedure given in [16], which checks that an equation is valid for all values lower than some (calculated) upper bounds, can be hardly used in practice (hence, to be used by inductive theorem provers).

EXAMPLE 3.6. *Let $s = \times(\mathsf{s}(x), \mathsf{s}(y))$ and $t = +(\mathsf{s}(+(y, x)), \times(y, x))$ Then we obtain $(\!|s|\!) = (x + 1) \times (y + 1)$ and $(\!|t|\!) = ((x + y) + 1) + (y \times x)$. Since $(x + 1) \times (y + 1) = xy + x + y + 1 = ((x + y) + 1) + (y \times x)$, we conclude from Theorem 3.5 that $\mathcal{R}_{(\times,+)} \models_{ind} s \approx t$ is valid.*

Let $\Sigma_{(+,\mathsf{s},0)} = \langle\{N\}, \mathcal{F}_{(+,\mathsf{s},0)}\rangle$, where $\mathcal{F}_{(+,\mathsf{s},0)} = \{+^{(2)}, \mathsf{s}^{(1)}, \mathsf{0}^{(0)}\}$, and $\mathcal{R}_{(+)} = \{l \to r \in \mathcal{R}_{(\times,+)} \mid l(\epsilon) = +\}$. It is also easy to see the following.

THEOREM 3.7. *It is decidable in polynomial time whether for given $s, t \in \mathrm{T}(\Sigma_{(+,\mathsf{s},0)}, \mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(+)}$.*

From the perspective of deciding the validity on natural numbers, the above results let us think that the situation is much nicer for equations than for general first-order formulas: for an arbitrary first-order formula φ over $\Sigma_{(\times,+,\mathsf{s},0)}$, $\mathbb{N}_{(\times,+,\mathsf{s},0)} \models \varphi$ (Peano arithmetic) is undecidable, and even for the one over the signature $\Sigma_{(+,\mathsf{s},0)}$, the complexity of deciding $\mathbb{N}_{(+,\mathsf{s},0)} \models \varphi$ (PA) is doubly exponential (e.g. [17]).

In fact, an exponential-time decision procedure for checking the validity of universal PA formulas is known [6, 27], and one can use this to decide $\mathbb{N}_{(+,\mathsf{s},0)} \models s \approx t$[1].

Similar to the Peano arithmetic case, one may be tempted to expect deciding the validity of equations on natural numbers is often decidable—but it is not true; in fact, extending $\mathbb{N}_{(\times,+,\mathsf{s},0)}$ with a simple function is enough to make the inductive validity of equations undecidable. This follows from the well-known result on the Hilbert 10th Problem [22]: it is undecidable whether $\exists a_1, \ldots, a_n \in \mathbb{Z}.\ \varphi(a_1, \ldots, a_n) = 0$ for given $\varphi \in \mathbb{Z}[x_1, \ldots, x_n]$. We now explain this, as the undecidability of inductive theorems seems to be folklore which we could not find in the literature.

Let us consider a first-order signature $\Sigma_{(\mathsf{eq},\times,+,\mathsf{s},0)} = \langle\{N\}, \{\mathsf{eq}^{(2)}\} \cup \mathcal{F}_{(\times,+,\mathsf{s},0)}\rangle$. Let $\mathcal{R}_{(\mathsf{eq},\times,+)}$ be the following TRS over $\Sigma_{(\mathsf{eq},\times,+,\mathsf{s},0)}$.

$$\mathcal{R}_{(\mathsf{eq},\times,+)} = \mathcal{R}_{(\times,+)} \cup \left\{ \begin{array}{lcl} \mathsf{eq}(\mathsf{0},\mathsf{0}) & \to & \mathsf{s}(\mathsf{0}) \\ \mathsf{eq}(\mathsf{s}(x),\mathsf{0}) & \to & \mathsf{0} \\ \mathsf{eq}(\mathsf{0},\mathsf{s}(x)) & \to & \mathsf{0} \\ \mathsf{eq}(\mathsf{s}(x),\mathsf{s}(y)) & \to & \mathsf{eq}(x,y) \end{array} \right\}$$

In the proof of Theorem 3.5, we showed that the equality of two formal polynomials $(\!|s|\!)$ and $(\!|t|\!)$ is decidable, for all natural numbers (i.e. $(\!|s|\!) = (\!|t|\!)$). The idea here is to use the fact that it is undecidable whether $(\!|s|\!)$ and $(\!|t|\!)$ are different for all natural numbers. By the additional eq-rules, this problem can be encoded as whether $\mathsf{eq}(s,t) \approx \mathsf{0}$ is an inductive theorem.

PROPOSITION 3.8 (Toyama [30]). *It is undecidable whether for given $s, t \in \mathrm{T}(\Sigma_{(\mathsf{eq},\times,+,\mathsf{s},0)}, \mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{eq},\times,+)}$.*

4. Deciding Inductive Theorems on Lists of Natural Numbers

In this section, we extend the decidability results of previous section to lists of natural numbers. For this, we assume a set $\mathcal{F}_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)} = \mathcal{F}_{(\times,+,\mathsf{s},0)} \cup \{\mathsf{len}^{L\to N}, \mathsf{rev}^{L\to L}, @^{L\times L\to L}, ::^{N\times L\to L}, \mathsf{nil}^{L}\}$ of function symbols and consider the many-sorted signature $\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)} = \langle\{N, L\}, \mathcal{F}_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}\rangle$. We define the following TRS $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$ over $\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}$ that encodes *append*, *reverse* and *length* functions on lists of natural numbers, where nil and :: are the list constructors: $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)} =$

$$\mathcal{R}_{(\times,+)} \cup \left\{ \begin{array}{lcl} @(\mathsf{nil}, ys) & \to & ys \\ @(::(x, xs), ys) & \to & ::(x, @(xs, ys)) \\ \mathsf{rev}(\mathsf{nil}) & \to & \mathsf{nil} \\ \mathsf{rev}(::(x, xs)) & \to & @(\mathsf{rev}(xs), ::(x, \mathsf{nil})) \\ \mathsf{len}(\mathsf{nil}) & \to & \mathsf{0} \\ \mathsf{len}(::(x, xs)) & \to & \mathsf{s}(\mathsf{len}(xs)) \end{array} \right\}$$

We are now going to present a procedure to decide whether $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)} \models_{ind} s \approx t$ for given terms $s, t \in \mathrm{T}(\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}, \mathcal{V})$. In the following, we will often abbreviate the subscripts $(\mathsf{len}, \mathsf{rev}, @, \times, +, ::, \mathsf{nil}, \mathsf{s}, \mathsf{0})$ and $(\mathsf{len}, \mathsf{rev}, @, \times, +)$ as $(\mathsf{len}, \ldots)$.

Let $\Sigma_{(::,\mathsf{nil},\mathsf{s},0)} = \langle\{N, L\}, \{::^{N\times L\to L}, \mathsf{nil}^{L}, \mathsf{s}^{N\to N}, \mathsf{0}^{N}\}\rangle$ be a many-sorted signature. Consider a $\Sigma_{(\mathsf{len},\ldots)}$-algebra with the set $\mathbb{L}^L$ of lists of natural numbers and natural numbers $\mathbb{L}^N$ as the carrier sets: $\mathbb{L}_{(\mathsf{len},\ldots)} = \langle\mathbb{L}; \mathsf{len}^{\mathbb{L}}, \mathsf{rev}^{\mathbb{L}}, @^{\mathbb{L}}, \times^{\mathbb{L}}, +^{\mathbb{L}}, ::^{\mathbb{L}}, \mathsf{nil}^{\mathbb{L}}, \mathsf{s}^{\mathbb{L}}, \mathsf{0}^{\mathbb{L}}\rangle$ where $\mathsf{len}^{\mathbb{L}}([\,]) = 0, \mathsf{len}^{\mathbb{L}}([a_1, \ldots, a_k]) = k, \mathsf{rev}^{\mathbb{L}}([a_1, \ldots, a_k]) = [a_k, \ldots, a_1]$, $@^{\mathbb{L}}([a_1, \ldots, a_k], [a_{k+1}, \ldots, a_l]) = [a_1, \ldots, a_l]$, $\times^{\mathbb{L}}(x, y) = x \times y$, $+^{\mathbb{L}}(x, y) = x + y$, $::^{\mathbb{L}}(a_0, [a_1, \ldots, a_l]) = [a_0, \ldots, a_l]$, $\mathsf{nil}^{\mathbb{L}} = [\,]$, $\mathsf{s}^{\mathbb{L}}(x) = x + 1$ and $\mathsf{0}^{\mathbb{L}}(x) = 0$.

Again, a key fact of our decision procedure is the following.

LEMMA 4.1. *The initial $\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}$-algebra of $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$ is isomorphic to $\mathbb{L}_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}$.*

We now present a decision procedure for the validity on $\mathbb{L}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$.

In the rest of this subsection, $\mathbb{L}_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}$ is abbreviated as $\mathbb{L}$. In our decision procedure, we consider normal form defined in terms of the function symbol single instead of ::. The term $\mathsf{single}(x)$ is

interpreted as the singleton list $::(x, \mathsf{nil})$. Thus we consider a signature $\Sigma_{(\mathsf{single},\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)} = \langle\{N, L\}, \{\mathsf{single}^{N\to L}\} \cup \mathcal{F}_{(\mathsf{len},\ldots)}\rangle$. We abbreviate $\{\mathsf{single}^{N\to L}\} \cup \mathcal{F}_{(\mathsf{len},\ldots)}$ as $\mathcal{F}_{(\mathsf{single},\ldots)}$ and $\Sigma_{(\mathsf{single},\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)}$ as $\Sigma_{(\mathsf{single},\ldots)}$.

Procedure `list-check(s,t)`

1. Normalize s and t by the following TRS: $\mathcal{S}_{(\mathsf{len},\mathsf{rev},::,@)} =$

$$\left\{ \begin{array}{lcl} @(xs, \mathsf{nil}) & \to & xs \\ @(\mathsf{nil}, ys) & \to & ys \\ ::(x, xs) & \to & @(\mathsf{single}(x), xs) \\ \mathsf{rev}(\mathsf{nil}) & \to & \mathsf{nil} \\ \mathsf{rev}(\mathsf{single}(x)) & \to & \mathsf{single}(x) \\ \mathsf{rev}(\mathsf{rev}(xs)) & \to & xs \\ \mathsf{rev}(@(xs, ys)) & \to & @(\mathsf{rev}(ys), \mathsf{rev}(xs)) \\ \mathsf{len}(\mathsf{nil}) & \to & \mathsf{0} \\ \mathsf{len}(\mathsf{single}(x)) & \to & \mathsf{s}(\mathsf{0}) \\ \mathsf{len}(\mathsf{rev}(xs)) & \to & \mathsf{len}(xs) \\ \mathsf{len}(@(xs, ys)) & \to & +(\mathsf{len}(xs), \mathsf{len}(ys)) \end{array} \right\}$$

   Note that $\mathcal{S}_{(\mathsf{len},\mathsf{rev},::,@)}$ is convergent and each term has a unique $\mathcal{S}_{(\mathsf{len},\mathsf{rev},::,@)}$-normal form. In the rest of this section, we will abbreviate $\mathcal{S}_{(\mathsf{len},\mathsf{rev},::,@)}$ as $\mathcal{S}$, and the $\mathcal{S}_{(\mathsf{len},\mathsf{rev},::,@)}$-normal form of a term u as $u{\downarrow}$.

   As we will see, if $\mathsf{len}(u)$ is a subterm of a $\mathcal{S}_{(\mathsf{len},\ldots)}$-normal term of sort N then $u \in \mathcal{V}^L$. To deal with such terms, let $\mathsf{len}(\mathcal{V}^L) = \{\mathsf{len}(xs) \mid xs \in \mathcal{V}^L\}$, and $\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})} = \langle\{N, L\}, \mathcal{F}_{(\times,+,\mathsf{s},0)} \cup \{\mathsf{len}^{L\to N}\}\rangle$.

2. Define (elem)-terms and (list)-terms by the following (extended) BNF.

(elem)-terms	$v_i ::= xs \mid \mathsf{single}(u) \mid \mathsf{rev}(xs)$
(list)-terms	$w_i ::= \mathsf{nil} \mid v_1 @ \cdots @ v_k$

[1] Note that, as implied from the definition of the interpretation, $\mathbb{N}_{(+,\mathsf{s},0)} \models s \approx t$ should be understood as $\mathbb{N}_{(+,\mathsf{s},0)} \models \forall x_1, \ldots, x_n.\ s \approx t$, where $\{x_1, \ldots, x_n\} = \mathcal{V}(s) \cup \mathcal{V}(t)$.

where xs ranges over $\mathcal{V}^L$, and u ranges over $\mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$. Here, @ is assumed to be associative. As we will see, $s{\downarrow}, t{\downarrow}$ are either terms in $\mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$ (if they have sort N) or (list)-terms (if they have sort L).

3. Consider a set $\mathcal{V}'^N$ of new variables that is bijective to $\mathsf{len}(\mathcal{V}^L)$. Let $\delta : \mathsf{len}(\mathcal{V}^L) \to \mathcal{V}'^N$ be a bijection. Furthermore, for any $u \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$, let $\mathsf{Abs}(u)$ be the term in $\mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)},\mathcal{V}^N \cup \mathcal{V}'^N)$ obtained by replacing every $\mathsf{len}(xs) \in \mathsf{len}(\mathcal{V}^L)$ in u with $\delta(\mathsf{len}(xs))$.

   If $s{\downarrow}, t{\downarrow}$ have sort N, then check $(\!|\mathsf{Abs}(s{\downarrow})|\!) = (\!|\mathsf{Abs}(t{\downarrow})|\!)$, i.e. whether $\mathsf{Abs}(s{\downarrow})$ and $\mathsf{Abs}(t{\downarrow})$ are the same formal polynomial, and use Theorem 3.5.

4. Consider now the remaining case when $s{\downarrow}, t{\downarrow}$ have the sort L.

   For any (list)-term w, let $\mathsf{List}(w)$ be the list of its (elem)-terms, i.e. if $w = \mathsf{nil}$ then $\mathsf{List}(w) = [\,]$ and if $w = v_1 \mathbin{@} \cdots \mathbin{@} v_k$ then $\mathsf{List}(w) = [v_1, \ldots, v_k]$.

   Take $l_1 = \mathsf{List}(s{\downarrow})$ and $l_2 = \mathsf{List}(t{\downarrow})$. Then, check l_1 and l_2 have equal lengths, and that, for each pairs $\langle v_i, v'_i\rangle$ of i-the elements of l_1 and l_2, either $v_i = v'_i \in \mathcal{V}^L$, $v_i = \mathsf{rev}(xs) = v'_i$ for some $xs \in \mathcal{V}^L$, or $v_i = \mathsf{single}(u_i), v'_i = \mathsf{single}(u'_i)$ for some u_i, u'_i and $(\!|\mathsf{Abs}(u_i)|\!) = (\!|\mathsf{Abs}(u'_i)|\!)$ holds.

LEMMA 4.2. *Let $s \in \mathrm{T}(\Sigma_{(\mathsf{single},\ldots)},\mathcal{V})$. (1) If s has sort N then $\mathsf{Abs}(s{\downarrow})$ can be computed in polynomial time. (2) If s has sort L then $\mathsf{List}(s{\downarrow})$ can be computed in polynomial time.*

It is easy to show that $\rhd \cup \to_{\mathcal{S}}$ is terminating, where $\rhd$ is the proper subterm relation. This fact is a basis of the proof of the following Lemma.

LEMMA 4.3. *Let $s \in \mathrm{T}(\Sigma_{(\mathsf{single},\ldots)},\mathcal{V})$. (1) If s has sort N then $s{\downarrow} \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$. (2) If s has sort L then $s{\downarrow}$ is a* (list)*-term.*

Note in the next lemma that it follows from Lemma 4.3 and $\mathrm{T}(\Sigma_{(\mathsf{len},\ldots)},\mathcal{V})^N \subseteq \mathrm{T}(\Sigma_{(\mathsf{single},\ldots)},\mathcal{V})^N$ that (1) for any $s \in \mathrm{T}(\Sigma_{(\mathsf{len},\ldots)},\mathcal{V})^N$, $s{\downarrow} \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$, and hence $\mathsf{Abs}(s{\downarrow})$ is defined, and (2) for any $s \in \mathrm{T}(\Sigma_{(\mathsf{len},\ldots)},\mathcal{V})^L$, $s{\downarrow}$ is a (list)-term and thus $\mathsf{List}(s{\downarrow})$ is defined.

LEMMA 4.4. *1. For $s,t \in \mathrm{T}(\Sigma_{(\mathsf{len},\ldots)},\mathcal{V})^N$, $\mathbb{L} \models s \approx t$ iff $\mathbb{N} \models \mathsf{Abs}(s{\downarrow}) \approx \mathsf{Abs}(t{\downarrow})$.*

2. Let $s,t \in \mathrm{T}(\Sigma_{(\mathsf{len},\ldots)},\mathcal{V})^L$, $\mathsf{List}(s{\downarrow}) = [u_1,\ldots,u_k]$ and $\mathsf{List}(t{\downarrow}) = [v_1,\ldots,v_l]$. Then $\mathbb{L} \models s \approx t$ iff $k = l$ and for every $i = 1,\ldots,k$, either (i) $u_i = v_i \in \mathcal{V}^L$, (ii) $u_i = \mathsf{rev}(xs) = v_i$ for some $xs \in \mathcal{V}^L$, or (iii) $u_i = \mathsf{single}(\hat{u}_i)$ and $v_i = \mathsf{single}(\hat{v}_i)$ with $\mathbb{N} \models \mathsf{Abs}(\hat{u}_i) \approx \mathsf{Abs}(\hat{v}_i)$.

Now we arrive at the main theorem of this section, claiming the decidability of inductive validity of $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$.

THEOREM 4.5. *It is decidable in exponential time whether for given $s,t \in \mathrm{T}(\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},0)},\mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$.*

Proof: We first claim `list-check(`s`,`t`)` can be done in exponential time. If s,t have sort N, then, by Lemma 4.2, $\mathsf{Abs}(s{\downarrow}), \mathsf{Abs}(t{\downarrow})$ can be computed in polynomial time. Then, $\mathbb{N} \models \mathsf{Abs}(s{\downarrow}) \approx \mathsf{Abs}(t{\downarrow})$ can be checked in exponential time by Theorem 3.5. If s,t have sort L, then, by Lemma 4.2, $\mathsf{List}(s{\downarrow}), \mathsf{List}(t{\downarrow})$ can be computed in polynomial time and the size of their elements is $\mathcal{O}(s)$ or $\mathcal{O}(t)$. Thus, the condition of Lemma 4.4 can be checked in exponential time by Theorem 3.5. Thus, `list-check(`s`,`t`)` can be done in exponential time. The correctness follows from Lemmas 4.1 and 4.4 and Proposition 2.1. □

EXAMPLE 4.6. *Let $s = \mathsf{rev}(@(\mathsf{rev}(::(+(\mathsf{len}(ys),\mathsf{len}(xs)), xs)), ys))$ and $t = @(\mathsf{rev}(ys), @(::(\mathsf{len}(@(xs,ys)), xs), \mathsf{nil}))$. Our decision procedure for $\mathcal{R}_{(\mathsf{len},\ldots)} \models_{ind} s \approx t$ works as follows. First, normalize s,t by $\mathcal{S}_{(\mathsf{len},\ldots)}$ to obtain $\mathsf{List}(s{\downarrow}) = [\mathsf{rev}(ys),\ \mathsf{single}(+(\mathsf{len}(ys),\mathsf{len}(xs))),\ xs]$ and $\mathsf{List}(t{\downarrow}) = [\mathsf{rev}(ys), \mathsf{single}(+(\mathsf{len}(xs),\mathsf{len}(ys))), xs]$. Next, we compare each components. Since the first and third components are identical, it remains to check $\mathbb{N} \models \mathsf{Abs}(+(\mathsf{len}(ys),\mathsf{len}(xs))) \approx \mathsf{Abs}(+(\mathsf{len}(xs),\mathsf{len}(ys)))$. This is done in the procedure presented in the proof of Theorem 3.5, and 'yes' is returned as $(\!|+(y,x)|\!) = y+x = x+y = (\!|+(x,y)|\!)$. Hence, we conclude from Theorem 4.5 that $\mathcal{R}_{(\mathsf{len},\ldots)} \models_{ind} s \approx t$ is valid.*

We now focus on a fragment of $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$ having a more efficient decision procedure. For this, we consider a many-sorted signature $\Sigma_{(\mathsf{len},\mathsf{rev},@,+,::,\mathsf{nil},\mathsf{s},0)} = \langle\{N,L\}, \mathcal{F}_{(\mathsf{len},\ldots)} \setminus \{\times\}\rangle$, and $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,+)} = \{l \to r \in \mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)} \mid l(\epsilon) \neq \times\}$.

THEOREM 4.7. *It is decidable in polynomial time whether for given $s,t \in \mathrm{T}(\Sigma_{(\mathsf{len},\mathsf{rev},@,+,::,\mathsf{nil},\mathsf{s},0)},\mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,+)}$.*

5. Deciding Inductive Theorems on Natural Numbers with Max and Min

In this section, we consider the decidability of inductive theorems of TRSs for other important functions defined on natural numbers, namely the maximum max and minimum min functions. In contrast to the previous sections, our results only cover the cases without multiplication $\times$. Also, the complexity of the decision procedures are exponential if max/min are combined with addition $+$.

In Section 5.1 we consider the case with both of max and min, and in Section 5.2 (5.3) we consider the case with only max (mix, respectively). Our presentation goes from broader classes to narrower classes.

5.1 Decidability with Max and Min

Let $\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)} = \langle\{N\}, \mathcal{F}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}\rangle$ be a first-order signature, where $\mathcal{F}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)} = \{\mathsf{max}^{(2)}, \mathsf{min}^{(2)}\} \cup \mathcal{F}_{(+,\mathsf{s},0)}$. Let us consider

$$\mathcal{R}_{(\mathsf{max},\mathsf{min})} = \left\{ \begin{array}{lcl} \mathsf{max}(0,y) & \to & y \\ \mathsf{max}(x,0) & \to & x \\ \mathsf{max}(\mathsf{s}(x),\mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{max}(x,y)) \\ \mathsf{min}(0,y) & \to & 0 \\ \mathsf{min}(x,0) & \to & 0 \\ \mathsf{min}(\mathsf{s}(x),\mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{min}(x,y)) \end{array} \right\}$$

that encodes the maximum/minimum operations on natural numbers, and the TRS $\mathcal{R}_{(\mathsf{max},\mathsf{min},+)} = \mathcal{R}_{(\mathsf{max},\mathsf{min})} \cup \mathcal{R}_{(+)}$ over $\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$. It is easy to check that $\mathcal{R}_{(\mathsf{max},\mathsf{min},+)}$ is convergent and sufficiently complete [5].

Let $\mathbb{N}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)} = \langle\mathbb{N}; \mathsf{max}^{\mathbb{N}}, \mathsf{min}^{\mathbb{N}}, +^{\mathbb{N}}, \mathsf{s}^{\mathbb{N}}, 0^{\mathbb{N}}\rangle$ be a $\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$-algebra where the operations are defined in a similar way to $\mathbb{N}_{(\times,+,\mathsf{s},0)}$ with additionally defining $\mathsf{max}^{\mathbb{N}}$ and $\mathsf{min}^{\mathbb{N}}$ as: $\mathsf{max}^{\mathbb{N}}(n,m) = n$ ($\mathsf{min}^{\mathbb{N}}(n,m) = m$) if $n \geq m$, and $\mathsf{max}^{\mathbb{N}}(n,m) = m$ ($\mathsf{in}^{\mathbb{N}}(n,m) = n$, respectively), otherwise.

Again, a key fact of our decision procedure is the following.

LEMMA 5.1. *The initial $\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$-algebra of $\mathcal{R}_{(\mathsf{max},\mathsf{min},+)}$ is isomorphic to $\mathbb{N}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$.*

We now explain that any validity of equations in $\mathbb{N}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$ can be encoded in that of first-order (universally quantified) PA formulas. (Universal quantification will be implicit below.)

For this, let consider a formula φ of the form $x_1 \approx \delta_1(u_1,v_1) \wedge \cdots \wedge x_k \approx \delta_k(u_k,v_k) \to s \approx t$, where

$s, t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}, \mathcal{V})$ and $\delta_i \in \{\mathsf{max}, \mathsf{min}\}, u_i, v_i \in \mathrm{T}(\Sigma_{(+,\mathsf{s},0)}, \mathcal{V})$ for $i = 1, \ldots, k$. Select a subterm occurrence of $\delta(u', v')$ in $s \approx t$ with $\delta \in \{\mathsf{max}, \mathsf{min}\}$ and $u', v' \in \mathrm{T}(\Sigma_{(+,\mathsf{s},0)}, \mathcal{V})$, and the replace this occurrence with a fresh variable z—let the result be $s' \approx t'$. Let the translation Pre be replacing φ by $x_1 \approx \delta_1(u_1, v_1) \wedge \cdots \wedge x_k \approx \delta_k(u_k, v_k) \wedge z \approx \delta(u', v') \to s' \approx t'$. Clearly, the translation Pre is terminating and the final result $\mathsf{Pre}^n(\varphi)$ is of the form $x_1 \approx \delta_1(u_1, v_1) \wedge \cdots \wedge x_k \approx \delta_k(u_k, v_k) \to s \approx t$ with $s, t \in \mathrm{T}(\Sigma_{(+,\mathsf{s},0)}, \mathcal{V})$. Next, replace each $x_i \approx \mathsf{max}(u_i, v_i)$ in $\mathsf{Pre}^n(\varphi)$ by $(u_i \leq v_i \to x_i \approx v_i) \wedge (v_i < u_i \to x_i \approx u_i)$ and $x_i \approx \mathsf{min}(u_i, v_i)$ in $\mathsf{Pre}^n(\varphi)$ by $(u_i \leq v_i \to x_i \approx u_i) \wedge (v_i < u_i \to x_i \approx v_i)$ for each $i = 1, \ldots, k$. Clearly, the result thus obtained is a PA formula and the translation preserves validity. Furthermore, the whole translation can be done in polynomial time. Thus, by the fact that the validity of universal PA formula[2]is decidable in exponential time [6, 27], the following corollary is obtained.

COROLLARY 5.2. *It is decidable in exponential time whether for given $s, t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}, \mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{max},\mathsf{min},+)}$.*

In the rest of this subsection, we show another decision procedure for a subclass of the problems in the hope that the procedure performs more efficiently experimentally, albeit in exponential time complexity—namely, a decision procedure for the fragment without addition $+$ and successor function s. Thus, we present a decision procedure of $\mathcal{R}_{(\mathsf{max},\mathsf{min})} \models_{ind} s \approx t$ for $s, t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},0)}, \mathcal{V})$, where $\Sigma_{(\mathsf{max},\mathsf{min},0)} = \langle\{N\}, \mathcal{F}_{(\mathsf{max},\mathsf{min})}\rangle$ with $\mathcal{F}_{(\mathsf{max},\mathsf{min})} = \{\mathsf{max}^{(2)}, \mathsf{min}^{(2)}, \mathsf{0}^{(0)}\}$ and $\mathcal{R}_{(\mathsf{max},\mathsf{min})} = \{l \to r \in \mathcal{R}_{(\mathsf{max},\mathsf{min},+)} \mid l(\epsilon) \in \{\mathsf{max}, \mathsf{min}\}\}$.

Let $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)} = \langle \mathbb{N}; \mathsf{max}^{\mathbb{N}}, \mathsf{min}^{\mathbb{N}}, \mathsf{s}^{\mathbb{N}}, \mathsf{0}^{\mathbb{N}}\rangle$ be a $\Sigma_{(\mathsf{max},\mathsf{min},\mathsf{s},0)}$-algebra, defined in a similar way to $\mathbb{N}_{(\mathsf{max},\mathsf{min},+,\mathsf{s},0)}$. Note here that the successor function s is necessary to construct $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)}$.

LEMMA 5.3. *The initial $\Sigma_{(\mathsf{max},\mathsf{min},\mathsf{s},0)}$-algebra of $\mathcal{R}_{(\mathsf{max},\mathsf{min})}$ is isomorphic to $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)}$.*

We are now going to present a decision procedure for $\mathcal{R}_{(\mathsf{max},\mathsf{min})} \models_{ind} s \approx t$ for $s, t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},0)}, \mathcal{V})$, where $\Sigma_{(\mathsf{max},\mathsf{min},0)} = \langle\{N\}, \{\mathsf{max}^{(2)}, \mathsf{min}^{(2)}, \mathsf{0}^{(0)}\}\rangle$.

Let us denoted by $\mathcal{P}(X)$ the powerset of a set X.

Procedure `max-min-check(s,t)`

1. Normalize s and t by the following TRS: $\mathcal{S}_{(\mathsf{max},\mathsf{min})} =$

$$\left\{ \begin{array}{lcl} \mathsf{min}(\mathsf{max}(x, y), z) & \to & \mathsf{max}(\mathsf{min}(x, z), \mathsf{min}(y, z)) \\ \mathsf{min}(x, \mathsf{max}(y, z)) & \to & \mathsf{max}(\mathsf{min}(x, y), \mathsf{min}(x, z)) \end{array} \right\}$$

   Note that $\mathcal{S}_{(\mathsf{max},\mathsf{min})}$ is convergent and each term has a unique $\mathcal{S}_{(\mathsf{max},\mathsf{min})}$-normal form. In the rest of this subsection, $s{\downarrow_{\mathcal{S}_{(\mathsf{max},\mathsf{min})}}}$ is abbreviated as $s{\downarrow}$.

2. We define (min)-terms and (max)-terms by the following BNF.

$$\begin{array}{ll} (\mathsf{min})\text{-terms} & v_i ::= \mathsf{0} \mid x \mid \mathsf{min}(v_1, v_2) \\ (\mathsf{max})\text{-terms} & w_i ::= v_1 \mid \mathsf{max}(w_1, w_2) \end{array}$$

   where x ranges over variables. Obviously, $s{\downarrow}, t{\downarrow}$ are (max)-terms. For each (min)-term v, define a set $[v]_{min} \in \mathcal{P}(\mathcal{V}) \cup \{\top\}$ as follows: $[v]_{min} = \top$ if v is a (min)-term containing $\mathsf{0}$, and $[v]_{min} = \mathcal{V}(v)$, otherwise. For each (max)-term v, define a set $[v]_{max} \subseteq \mathcal{P}(\mathcal{V}) \cup \{\top\}$ as follows: by $[v]_{max} = \{[v]_{min}\}$ for (min)-terms v, or by $[\mathsf{max}(w_1, w_2)]_{max} = [w_1]_{max} \cup [w_2]_{max}$, otherwise. Compute $U = [s{\downarrow}]_{max}$ and $V = [t{\downarrow}]_{max}$.

3. For each $X, Y \in \mathcal{P}(\mathcal{V}) \cup \{\top\}$, define $X \subseteq^\circ Y$ by $X^\circ \subseteq Y^\circ$, where $X^\circ = X$ for $X \subseteq \mathcal{V}$ and $\top^\circ = \mathcal{V}$. For each set $A \subseteq \mathcal{P}(\mathcal{V}) \cup \{\top\}$, let $\mathcal{M}in(A)$ be the set of minimal elements of A w.r.t. the set inclusion $\subseteq^\circ$, i.e.

$$\mathcal{M}in(A) = \{X \in A \mid \forall Y \in A.\ (Y \subseteq^\circ X \Rightarrow X = Y)\}$$

   Compute the sets of variables $S = \mathcal{M}in(U)$ and $T = \mathcal{M}in(V)$. Then return 'yes' if $S = T$ and 'no' otherwise.

LEMMA 5.4. `max-min-check(s,t)` *can be done in exponential time.*

To show the correctness of the procedure, we need some technical definitions and lemmas. To interpret (min)-terms, we introduce a function Min_ρ.

DEFINITION 5.5. *For any valuation $\rho : \mathcal{V} \to \mathbb{N}$, we define $\mathsf{Min}_\rho : \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\} \cup \{\top\} \to \mathbb{N}$ as follows: (1) $\mathsf{Min}_\rho(\top) = 0$, and (2) $\mathsf{Min}_\rho(A) = \min\{\rho(x) \mid x \in A\}$, for finite non-empty $A \subseteq \mathcal{V}$.*

Some properties of Min_ρ follow.

LEMMA 5.6. *Let $\rho : \mathcal{V} \to \mathbb{N}$ be a valuation, and $A, B \subseteq \mathcal{V}$ finite non-empty sets. Then, (1) $\mathsf{Min}_\rho(A \cup B) = \min\{\mathsf{Min}_\rho(A), \mathsf{Min}_\rho(B)\}$, and (2) $A \subseteq B$ implies $\mathsf{Min}_\rho(B) \leq \mathsf{Min}_\rho(A)$.*

LEMMA 5.7. *Let $A, B \in \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\} \cup \{\top\}$. Then $A \subseteq^\circ B$ implies $\mathsf{Min}_\rho(B) \leq \mathsf{Min}_\rho(A)$.*

The correspondence of the function Min_ρ and the interpretation of (min)-terms is expressed like this:

LEMMA 5.8. *Let $\rho : \mathcal{V} \to \mathbb{N}$ be a valuation. Then, for any (min)-term v, $\mathsf{Min}_\rho([v]_{min}) = [\![v]\!]_\rho$.*

Next, we introduce a function Max_ρ to interpret (max)-terms.

DEFINITION 5.9. *Let $\rho : \mathcal{V} \to \mathbb{N}$ be a valuation. For any finite $S \subseteq \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\} \cup \{\top\}$, define $\mathsf{Max}_\rho(S) = \max\{\mathsf{Min}_\rho(X) \mid X \in S\}$.*

The correspondence of the function Min_ρ and the interpretation of (min)-terms is extended to that of Max_ρ and the interpretation of (max)-terms.

LEMMA 5.10. *Let $\rho : \mathcal{V} \to \mathbb{N}$ be a valuation. Then, for any (max)-term w, $\mathsf{Max}_\rho([w]_{max}) = [\![w]\!]_\rho$.*

Some properties of Max_ρ follow.

LEMMA 5.11. *Let $\rho : \mathcal{V} \to \mathbb{N}$ be a valuation. Then, for any finite non-empty $S \subseteq \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\} \cup \{\top\}$, $\mathsf{Max}_\rho(S) = \mathsf{Max}_\rho(\mathcal{M}in(S))$.*

LEMMA 5.12. *Let $S, T \subseteq \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\} \cup \{\top\}$ be finite and non-empty. Suppose that S (T) consists of elements minimal w.r.t. $\subseteq^\circ$, i.e. $X \subseteq^\circ Y$ implies $X = Y$ for any $X, Y \in S$ (for any $X, Y \in T$, respectively). Then $S = T$ iff $\forall \rho.\ \mathsf{Max}_\rho(S) = \mathsf{Max}_\rho(T)$*

Now we can prove the correctness of the procedure.

LEMMA 5.13. *For any $s, t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},0)}, \mathcal{V})$, `max-min-check(s,t)` returns 'yes' iff $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)} \models s \approx t$.*

[2]Note that one has to check the validity of formulas of the form $\forall x_1, \ldots, x_k.\ \psi$ for quantifier-free ψ, and not that of the form $\exists x_1, \ldots, x_k.\ \psi$ (satisfiability problem of quantifier-free PA formula), which is in NP.

Proof: In the following, let us abbreviate $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)}$ as $\mathbb{N}$. First, note that we have $\mathbb{N} \models \mathsf{min}(\mathsf{max}(x,y),z) \approx \mathsf{max}(\mathsf{min}(x,z),\mathsf{min}(y,z))$ and $\mathbb{N} \models \mathsf{min}(x,\mathsf{max}(y,z)) \approx \mathsf{max}(\mathsf{min}(x,y),\mathsf{min}(x,z))$. Thus, $\mathbb{N} \models s \approx t$ iff $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$ holds. Thus it remains to show that `max-min-check(`s`,`t`)` returns 'yes' iff $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$.
($\Rightarrow$) Suppose `max-min-check(`s`,`t`)` returns 'yes'. Then, by definition of the procedure, $\mathit{Min}([s{\downarrow}]_{max}) = \mathit{Min}([t{\downarrow}]_{max})$. Clearly, $[s{\downarrow}]_{max}$ and $[t{\downarrow}]_{max}$ are finite and non-empty. Thus, using Lemmas 5.11 and 5.10, for any valuation $\rho : \mathcal{V} \to \mathbb{N}$, $[\![s{\downarrow}]\!]_\rho = \mathsf{Max}_\rho([s{\downarrow}]_{max}) = \mathsf{Max}_\rho(\mathit{Min}([s{\downarrow}]_{max})) = \mathsf{Max}_\rho(\mathit{Min}([t{\downarrow}]_{max})) = \mathsf{Max}_\rho([t{\downarrow}]_{max}) = [\![t{\downarrow}]\!]_\rho$. Hence, $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$.
($\Leftarrow$) Suppose $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$. Again, using Lemmas 5.11 and 5.10, we know that, for any valuation $\rho : \mathcal{V} \to \mathbb{N}$, $\mathsf{Max}_\rho(\mathit{Min}([s{\downarrow}]_{max})) = \mathsf{Max}_\rho(\mathit{Min}([t{\downarrow}]_{max}))$ holds. Since each of $\mathit{Min}([s{\downarrow}]_{max})$ and $\mathit{Min}([t{\downarrow}]_{max})$ consists of elements minimal w.r.t. $\subseteq^\circ$, by Lemma 5.12, $\mathit{Min}([s{\downarrow}]_{max}) = \mathit{Min}([t{\downarrow}]_{max})$. Thus, `max-min-check(`$s$`,`$t$`)` returns 'yes'. □

THEOREM 5.14. *It is decidable in exponential time whether for given $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{min},0)},\mathcal{V})$, the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{max},\mathsf{min})}$.*

EXAMPLE 5.15. *Let $s = \mathsf{max}(\mathsf{min}(y,0),\mathsf{max}(\mathsf{min}(y,z),x))$ and $t = \mathsf{max}(x,\mathsf{min}(\mathsf{max}(x,y),z))$. Then we can establish that $[s{\downarrow}]_{max} = [s]_{max} = \{\top,\{y,z\},\{x\}\}$ and $[t{\downarrow}]_{max} = [\mathsf{max}(x,\mathsf{max}(\mathsf{min}(x,z),\mathsf{min}(y,z)))]_{max} = \{\{x\},\{x,z\},\{y,z\}\}$.*
`max-min-check(`s`,`t`)` returns 'yes', as $\mathit{Min}(\{\top,\{y,z\},\{x\}\}) = \{\{y,z\},\{x\}\} = \mathit{Min}(\{\{x\},\{x,z\},\{y,z\}\})$. Hence, we conclude from Theorem 5.14 that $\mathcal{R}_{(\mathsf{max},\mathsf{min})} \models_{ind} s \approx t$ is valid.

5.2 Decidability with Max

In the previous subsection, we considered the case that both of max and min are presented. In this section, we consider the case that only max is presented, i.e. decidability of inductive theorems of $\mathcal{R}_{(\mathsf{max},+)} = \{l \to r \in \mathcal{R}_{(\mathsf{max},\mathsf{min},+)} \mid l(\epsilon) \in \{\mathsf{max},+\}\}$. [3]

We first explain a corollary that follows from an existing work. In [1], an exponential decision procedure for $\mathbb{N}_{(\mathsf{max},+,0)} \models s \approx t$ for $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},+,0)},\mathcal{V})$ is presented, where $\mathbb{N}_{(\mathsf{max},+,0)}$ and $\Sigma_{(\mathsf{max},+,0)}$ are given in the obvious way.

We now briefly explain the decision procedure of [1]. Given an equation $s \approx t$ of $\Sigma_{(\mathsf{max},+,0)}$, normalize s,t by the following TRS:

$$\left\{\begin{array}{l} +(\mathsf{max}(x,y),z) \to \mathsf{max}(+(x,z),+(y,z)) \\ +(z,\mathsf{max}(x,y)) \to \mathsf{max}(+(z,x),+(z,y)) \\ \mathsf{max}(x,0) \to x \\ \mathsf{max}(0,y) \to y \end{array}\right\}$$

Let $s' \approx t'$ be an arbitrary but fixed result. Let (max)-contexts be given by the following BNF.

$$(\mathsf{max})\text{-contexts} \qquad v_i ::= \Box \mid \mathsf{max}(v_1,v_2)$$

Then s' and t' are 0 or of the from $C[u_1,\ldots,u_m]$ for some (max)-contexts C and $u_1,\ldots,u_n \in \mathrm{T}(\Sigma_{(+)},\mathcal{V})$. The case either $s' = 0$ or $t' = 0$ is clear, so we suppose otherwise. Clearly, $C[u_1,\ldots,u_m] \approx C'[u'_1,\ldots,u'_n]$ is valid if and only if $u_i \le C'[u'_1,\ldots,u'_n]$ is valid for all $1 \le i \le m$ and $u'_j \le C[u_1,\ldots,u_m]$ is valid for all $1 \le j \le n$. Thus, it suffices to decide the validity of inequations $u \le C[v_1,\ldots,v_m]$, for any (max)-context C and $u,v_1,\ldots,v_n \in \mathrm{T}(\Sigma_{(+)},\{x_1,\ldots,x_n\})$. Let the formal polynomials of $u,v_1,\ldots,v_m$ be $(\!|u|\!) = c_1x_1+\cdots+c_nx_n$ and $(\!|v_i|\!) = d_{i1}x_1+\cdots+d_{in}x_n$ $(1 \le i \le m)$. Corollary 3.17 of [1] shows that the inequation $u \le C[v_1,\ldots,v_m]$ is valid if and only if there exist the non-negative real numbers $\lambda_1,\ldots,\lambda_m$ and $\gamma_1,\ldots,\gamma_n$ such that $\sum_i \lambda_i = 1$ and, for each $j = 1,\ldots,n$, $(\sum_i d_{ij}\lambda_i) - \gamma_j = c_j$. The latter is a linear programming problem, which is known to be solvable in polynomial time.

Thus, the next corollary immediately follows from [1].

COROLLARY 5.16. *It is decidable in exponential time whether for given $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},+,0)},\mathcal{V})$, the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{max},+)}$.*

In the rest of this section, we show that by replacing addition $+$ with successor function s, one can obtain a *polynomial* decision procedure, i.e. $\mathcal{R}_{(\mathsf{max})} \models_{ind} s \approx t$ is decidable in polynomial time for $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{s},0)},\mathcal{V})$, where $\Sigma_{(\mathsf{max},\mathsf{s},0)} = \langle\{N\},\mathcal{F}_{(\mathsf{max},\mathsf{s},0)}\rangle$, $\mathcal{F}_{(\mathsf{max},\mathsf{s},0)} = \{\mathsf{max}^{(2)},\mathsf{s}^{(1)},0^{(0)}\}$ and $\mathcal{R}_{(\mathsf{max})} = \{l \to r \in \mathcal{R}_{(\mathsf{max},\mathsf{min},+)} \mid l(\epsilon) = \mathsf{max}\}$. Note that since $\mathbb{N}_{(\mathsf{max},+,0)}$ cannot encode s and $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)}$ cannot encode $+$, this result does not follow from Corollary 5.16.

LEMMA 5.17. *The initial $\Sigma_{(\mathsf{max},\mathsf{s},0)}$-algebra of $\mathcal{R}_{(\mathsf{max})}$ is isomorphic to $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)}$.*

We now present a decision procedure for the validity on $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)}$.

Procedure `max-check(`s`,`t`)`

1. Normalize s,t by the following TRS:
$$\mathcal{S}_{(\mathsf{max})} = \{\ \mathsf{s}(\mathsf{max}(x,y)) \to \mathsf{max}(\mathsf{s}(x),\mathsf{s}(y))\ \}$$
Note that $\mathcal{S}_{(\mathsf{max})}$ is convergent and each term has a unique $\mathcal{S}_{(\mathsf{max})}$-normal form. In the rest of this subsection, $s{\downarrow}_{\mathcal{S}_{(\mathsf{max})}}$ is abbreviated as $s{\downarrow}$.
2. We define (s)-terms and (max)-terms by the following BNF.
$$\begin{array}{ll} (\mathsf{s})\text{-terms} & u_i ::= x \mid 0 \mid \mathsf{s}(u_1) \\ (\mathsf{max})\text{-terms} & v_i ::= u_1 \mid \mathsf{max}(v_1,v_2) \end{array}$$
where x ranges over variables. Obviously, $s{\downarrow},t{\downarrow}$ are (max)-terms. From each (max)-term v, define a set $[v]$ of (s)-terms by $[u] = \{u\}$ if u is an (s)-term, $[\mathsf{max}(v_1,v_2)] = [v_1] \cup [v_2]$ otherwise. Compute the sets $U = [s{\downarrow}]$ and $V = [t{\downarrow}]$ of (s)-terms.
3. Define a relation $\prec$ on (s)-terms by $s \prec t$ if either (1) $\mathsf{s}^n(u) \prec \mathsf{s}^m(u)$, for some $n < m$ and $u \in \mathcal{V} \cup \{0\}$, or (2) $\mathsf{s}^n(0) \prec \mathsf{s}^m(x)$, for some $n \le m$ and variable $x \in \mathcal{V}$. For each set X of (s)-terms, let $\mathcal{M}ax_\prec(X)$ be the set of maximal elements of X w.r.t. $\prec$:
$$\mathcal{M}ax_\prec(X) = \{s \in X \mid s \prec t \text{ for no } t \in X\}$$
Compute the sets $S = \mathcal{M}ax_\prec(U)$ and $T = \mathcal{M}ax_\prec(V)$ of (s)-terms. Then return 'yes' if $S = T$ and 'no' otherwise.

LEMMA 5.18. `max-check(`s`,`t`)` *can be done in polynomial (quadratic) time.*

LEMMA 5.19. *For any $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{s},0)},\mathcal{V})$, `max-check(`$s$`,`$t$`)` returns 'yes' iff $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)} \models s \approx t$.*

THEOREM 5.20. *It is decidable in polynomial time whether for given $s,t \in \mathrm{T}(\Sigma_{(\mathsf{max},\mathsf{s},0)},\mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{max})}$.*

EXAMPLE 5.21. *Let $s = \mathsf{max}(\mathsf{s}(x),x)$ and $t = \mathsf{max}(\mathsf{s}(0),\mathsf{s}(x))$. Then `max-check(`$s$`,`$t$`)` returns 'yes', as we have $\mathcal{M}ax_\prec([s{\downarrow}_{\mathcal{S}_{(\mathsf{max})}}]) = \mathcal{M}ax_\prec(\{\mathsf{s}(x),x\}) = \{\mathsf{s}(x)\}$ and $\mathcal{M}ax_\prec([t{\downarrow}_{\mathcal{S}_{(\mathsf{max})}}]) = \mathcal{M}ax_\prec(\{\mathsf{s}(0),\mathsf{s}(x)\}) = \{\mathsf{s}(x)\}$. Thus, we conclude from Theorem 5.20 that $\mathcal{R}_{(\mathsf{max})} \models_{ind} s \approx t$ is valid.*

[3] A decision procedure for Min can be built similarly.

It is not difficult to give a decision procedure and obtain the next theorem in the similar way to Theorem 5.20.

THEOREM 5.22. *It is decidable in polynomial time whether for given $s, t \in \mathrm{T}(\Sigma_{(\mathsf{min},\mathsf{s},\mathsf{0})}, \mathcal{V})$ the equation $s \approx t$ is an inductive theorem of $\mathcal{R}_{(\mathsf{min})}$.*

6. Experiments

The decision procedures of the paper have been implemented in the SPIKE[4] prover [7, 28].

For the experiments, we take into account some categories and construct collections of conjectures randomly for each category. Each collection gathers equalities of same inductive validity and built over one of the following signatures:

- $\Sigma_{(+,\mathsf{s})}$ and its extension with $\mathsf{0}$, $\Sigma_{(+,\mathsf{s},\mathsf{0})}$,
- $\Sigma_{(\times,+,\mathsf{s})}$ and its extension with $\mathsf{0}$, $\Sigma_{(\times,+,\mathsf{s},\mathsf{0})}$,
- $\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},\mathsf{s},\mathsf{0})}$ by considering equalities between terms of list sort,
- $\Sigma_{(\mathsf{max},\mathsf{min},\mathsf{0})}$,
- $\Sigma_{(\mathsf{max},\mathsf{s},\mathsf{0})}$ and similarly $\Sigma_{(\mathsf{min},\mathsf{s},\mathsf{0})}$.

For each category, we excluded trivial equations and equations whose roots of both sides of the equation is s. All equalities have at most three distinct variales of each sort and the depth of both sides is smaller than five. The number of examples widely varies between each category. Furthermore, since most of the randomly generated conjectures are not inductive theorems, we have additionally incorporated several ad-hoc heuristics to generate a sufficient number of inductive theorems to reach a target of 100 examples (we failed for only one category).

The numbers of examples and the summary of experiments are shown in Table 1. Each test was performed on a PC with one 2.50GHz CPU and 4G of memory. For any information of the form $a(b)$ in the table, a (resp. b) represents the number of examples that has (resp. has not) been successfully checked within the 10 seconds.

Our decision procedures successfully solved all these examples, as shown in the column entitled "SPIKE + direct". For comparison, we also tested the examples with SPIKE integrating an incomplete solver for PA, as previously described in [4, 29]. The figures from the column entitled "SPIKE + PA (Cor. 5.2)" (resp., "SPIKE + PA([4])") give the statistics about the use of the PA solver with a prior encoding of equalities to PA, according to Corollary 5.2, (resp., without encoding). In the categories to which our decision procedures and the PA solver are applicable, the first are 2–6 times faster; the latter failed at some examples due to lack of additional resources.

When the decision procedures and the PA solver are disabled, SPIKE acts as an implicit induction theorem prover, able to perform several induction and rewrite steps during a proof session. We used a unique proof strategy for all tests and no additional lemmas (0-knowledge proofs). Apart from the TRS and the conjecture to be proved, we additionally provided a unique precedence suitable for ensuring the termination of the input TRS. For some categories, SPIKE inductively proved/disproved most of the examples, as shown in the column "SPIKE (induction) [28]". However, for some categories more than half of the examples have not been solved or require more than 10s to be solved. A special category, involving equations over the extended signature $\Sigma_{(\mathsf{max},\mathsf{min},+,\mathsf{s},\mathsf{0})}$, helped to better compare with the PA solver. '-' means that the TRS category cannot be solved by the corresponding SPIKE configuration, hence it matches the values from the last column. We can safely conclude that SPIKE has become more effective by incorporating our decision procedures.

The collection of examples and details of the experiments are available on the webpage `http://www.nue.riec.tohoku.ac.jp/tools/experiments/ppdp14/`.

[4] `https://code.google.com/p/spike-prover/`

7. Conclusion

We have given decision procedures for checking the inductive validity of equations built over common function symbols defined on natural numbers and lists. Our results are summarized in Table 2. In contrast to the line of research from [11–14], our decidability results do not impose any syntactical conditions on the equations or induction reasoning albeit specific to some TRSs. Experiments show that our decision procedures are effective for enhancing inductive theorem provers.

Our strong restriction on TRSs can be slightly relaxed. For example, the decidability result for $\mathcal{R}_{(\times,+)}$ also applies to the following variation $\mathcal{R}'_{(\times,+)}$, which is convergent, sufficiently complete and has the same initial algebra as $\mathcal{R}_{(\times,+)}$:

$$\mathcal{R}'_{(\times,+)} = \left\{ \begin{array}{lcl} +(x,\mathsf{0}) & \to & x \\ +(x,\mathsf{s}(y)) & \to & +(\mathsf{s}(x),y) \\ \times(x,\mathsf{0}) & \to & \mathsf{0} \\ \times(x,\mathsf{s}(y)) & \to & +(x,\times(x,y)) \end{array} \right\}$$

As future works, we would like to tackle some problems which are left open in the current contribution: extending the decision procedure of [1] to equations over $\Sigma_{(\mathsf{max},+,\mathsf{s},\mathsf{0})}$ and to equations over $\Sigma_{(\mathsf{min},+,\mathsf{0})}$, obtaining a decision procedure for equations over $\Sigma_{(\mathsf{max},\times,+)}$. We also intend to find other standard TRSs for which our approach works, and how to (semi-)automatically find inductively valid equations that sufficiently characterize the validity in initial algebras. We also intend to apply our approach for classes of conditional TRSs and (conditional) equations.

Acknowledgements

Thanks are due to Yoshihito Toyama for kindly allowing us to include his unpublished result [30]. We also thank Yuki Chiba, Nao Hirokawa and Michio Oyamaguchi for helpful comments. We are also grateful to our anonymous reviewers for their time and comments.

References

[1] L. Aceto, Z. Ésik, and A. Ingólfsdóttir. The max-plus algebra of the natural numbers has no finite equational basis. *Theoretical Computer Science*, 293:169–188, 2003.

[2] T. Aoto. Designing a rewriting induction prover with an increased capability of non-orientable equations. In *Proc. of 1st SCSS*, volume 08-08 of *RISC Technical Report*, pages 1–15, 2008.

[3] T. Aoto. Sound lemma generation for proving inductive validity of equations. In *Proc. of 28th FSTTCS*, volume 2 of *LIPIcs*, pages 13–24. Schloss Dagstuhl, 2008.

[4] A. Armando, M. Rusinowitch, and S. Stratulat. Incorporating decision procedures in implicit induction. *Journal of Symbolic Computation*, 34:241–258, 2002.

[5] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[6] W. W. Bledsoe. A new method for proving certain Presburger formulas. In *Proc. of 4th IJCAI*, pages 15–21, 1975.

[7] A. Bouhoula, E. Kounalis, and M. Rusinowitch. Automated mathematical induction. *Journal of Logic and Computation*, 5(5):631–668, 1995.

[8] R. S. Boyer and J. S. Moore. Integrating decision procedures into heuristic theorem provers: a case study of linear arithmetic. In *Ma-*

Table 1. Summary of Experiments

TRS	signature / complexity	inductive validity	number of problems	SPIKE + direct	SPIKE + PA(Cor. 5.2)	SPIKE + PA([4])	SPIKE (induction) [28]
$\mathcal{R}_{(+)}$	$\Sigma_{(+,s)}$ /	yes	101	101(0)	101(0)	101(0)	30(71)
	polynomial	no	1197	1197(0)	1197(0)	1197(0)	887(310)
$\mathcal{R}_{(+)}$	$\Sigma_{(+,s,0)}$ /	yes	101	101(0)	101(0)	101(0)	75(26)
	polynomial	no	536	536(0)	536(0)	536(0)	407(129)
$\mathcal{R}_{(\times,+)}$	$\Sigma_{(\times,+,s)}$ /	yes	60	60(0)	-	-	2(58)
	exponential	no	1670	1670(0)	-	-	992(678)
$\mathcal{R}_{(\times,+)}$	$\Sigma_{(\times,+,s,0)}$ /	yes	244	244(0)	-	-	145(199)
	exponential	no	1204	1204(0)	-	-	910(294)
$\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$	$\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},s,0)}$ /	yes	213	213(0)	-	-	24(189)
	exponential	no	1777	1777(0)	-	-	1068(709)
$\mathcal{R}_{(\mathsf{max},\mathsf{min},+)}$	$\Sigma_{(\mathsf{max},\mathsf{min},+,s,0)}$ /	yes	104	-	102(2)	-	51(53)
	exponential	no	1741	-	1719(22)	-	1164(547)
$\mathcal{R}_{(\mathsf{max},\mathsf{min})}$	$\Sigma_{(\mathsf{max},\mathsf{min},0)}$ /	yes	153	153(0)	148(5)	-	121(32)
	exponential	no	1528	1528(0)	1478(50)	-	1285(243)
$\mathcal{R}_{(\mathsf{max})}$	$\Sigma_{(\mathsf{max},s,0)}$ /	yes	116	116(0)	116(0)	-	114(2)
	polynomial	no	1107	1107(0)	1107(0)	-	1061(46)
$\mathcal{R}_{(\mathsf{min})}$	$\Sigma_{(\mathsf{min},s,0)}$ /	yes	115	115(0)	115(0)	-	114 (1)
	polynomial	no	1081	1081(0)	1081(0)	-	1032(49)

Table 2. Summary of Results

TRS	signature	complexity	reference
$\mathcal{R}_{(\mathsf{exp},\times,+)}$	$\Sigma_{(\mathsf{exp},\times,+,s,0)}$	decidable	([10])
$\mathcal{R}_{(\mathsf{eq},\times,+)}$	$\Sigma_{(\mathsf{eq},\times,+,s,0)}$	undecidable	([30])
$\mathcal{R}_{(\times,+)}$	$\Sigma_{(\times,+,s,0)}$	exponential	Thm. 3.5
$\mathcal{R}_{(+)}$	$\Sigma_{(+,s,0)}$	polynomial	Thm. 3.7
$\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$	$\Sigma_{(\mathsf{len},\mathsf{rev},@,\times,+,::,\mathsf{nil},s,0)}$	exponential	Thm. 4.5
$\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,+)}$	$\Sigma_{(\mathsf{len},\mathsf{rev},@,+,::,\mathsf{nil},s,0)}$	polynomial	Thm. 4.7
$\mathcal{R}_{(\mathsf{max},\mathsf{min},+)}$	$\Sigma_{(\mathsf{max},\mathsf{min},+,s,0)}$	exponential	(validity of QFP [6, 27])
$\mathcal{R}_{(\mathsf{max},\mathsf{min})}$	$\Sigma_{(\mathsf{max},\mathsf{min},0)}$	exponential	Thm. 5.14
$\mathcal{R}_{(\mathsf{max},+)}$	$\Sigma_{(\mathsf{max},+,0)}$	exponential	(Cor. 3.17 of [1])
$\mathcal{R}_{(\mathsf{max})}$	$\Sigma_{(\mathsf{max},s,0)}$	polynomial	Thm. 5.20
$\mathcal{R}_{(\mathsf{min})}$	$\Sigma_{(\mathsf{min},s,0)}$	polynomial	Thm. 5.22

chine Intelligence, volume 11, pages 83–124. Oxford University Press, 1988.

[9] Z.-Z. Chen and M.-Y. Kao. Reducing randomness via irrational numbers. In *Proc. of 29th STOC*, pages 200–209. ACM, 1997.

[10] R. D. Cosmo and T. Dufour. The equational theory of $\langle \mathbb{N}, 0, 1, +, \times, \uparrow \rangle$ is decidable, but not finitely axiomatisable. In *Proc. of 11th LPAR*, volume 3452 of *LNAI*, pages 240–256. Springer-Verlag, 2004.

[11] S. Falke and D. Kapur. Inductive decidability using implicit induction. In *Proc. of 13th LPAR*, volume 4246 of *LNAI*, pages 45–59. Springer-Verlag, 2006.

[12] S. Falke and D. Kapur. Rewriting induction + linear arithmetic = decision procedure. In *Proc. of 6th IJCAR*, volume 7364 of *LNAI*, pages 241–255, 2012.

[13] J. Giesl and D. Kapur. Decidable classes of inductive theorems. In *Proc. of 1st IJCAR*, volume 2083 of *LNAI*, pages 469–484, 2001.

[14] J. Giesl and D. Kapur. Deciding inductive validity of equations. In *Proc. of CADE-19*, volume 2741 of *LNAI*, pages 17–31, 2003.

[15] B. Gramlich. Strategic issues, problems and challenges in inductive theorem proving. *Electronic Notes in Theoretical Computer Science*, 125(2):5–43, 2005.

[16] R. Gurevič. Equational theory of positive numbers with exponentiation. *AMS*, 94(1):135–141, 1985.

[17] J. Harrison. *Handbook of Practical Logic and Automated Reasoning*. Cambridge University Press, 2009.

[18] P. Hrubes and I. Tzameret. The proof complexity of polynomial identities. In *Proc. of CCC*, pages 41–51. IEEE, 2009.

[19] G. Huet and D. C. Oppen. Equations and rewrite rules: a survey. Technical report, Stanford University, Stanford, CA, USA, 1980.

[20] D. Kapur and M. Subramaniam. New uses of linear arithmetic in automated theorem proving by induction. *Journal of Automated Reasoning*, 1–2:81–111, 1991.

[21] D. Kapur and M. Subramaniam. Extending decision procedures with induction schemes. In *Proc. of CADE-17*, volume 1831 of *LNAI*, pages 324–345, 2000.

[22] Y. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Dokl. AN SSSR*, 191(2):278–282, 1970. English translation in: Soviet Math. Doklady, 11(2):354–358, 1970.

[23] T. Nakazima, T. Aoto, and Y. Toyama. Decidability of inductive theorems based on rewriting induction. *JSSST Computer Software*, 31(3):294–306, 2014. In Japanese.

[24] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.

[25] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. of the Association for Computing Machinery*, 27(4):701–717, 1980.

[26] S. Shimazu, T. Aoto, and Y. Toyama. Automated lemma generation for rewriting induction with disproof. *JSSST Computer Software*, 26(2):41–55, 2009. In Japanese.

[27] R. E. Shostak. On the SUP-INF method for proving Presburger formulas. *J. of the Association for Computing Machinery*, 24(4):529–543, 1977.

[28] S. Stratulat. A general framework to build contextual cover set induction provers. *Journal of Symbolic Computation*, 32:403–445, 2001.

[29] S. Stratulat. Implementing reasoning modules in implicit induction theorem provers. In *Proc. of 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2014)*, to appear.

[30] Y. Toyama. Private communication.

[31] P. Urso and E. Kounalis. Sound generalizations in mathematical induction. *Theoretical Computer Science*, 323:443–471, 2004.

[32] T. Walsh. A divergence critic for inductive proof. *J. of Artificial Intelligence Research*, 4:209–235, 1996.

[33] Y. Yamazaki. *Ring and Module (in Japanese)*. Iwanami, 1990.

A. Proofs

Proof: [of Lemma 3.1] First, it is easy to check that $\mathcal{R}_{(\times,+)}$ is convergent and sufficiently complete [5]. Hence any ground term $t \in \mathrm{T}\left(\Sigma_{(\times,+,\mathsf{s},0)}\right)$ has a unique normal form $t{\downarrow} \in \mathrm{T}\left(\Sigma_{(\mathsf{s},0)}\right)$. Thus the mapping given by $\varphi : [t] \mapsto t{\downarrow}$ is a bijection from $\mathrm{T}\left(\Sigma_{(\times,+,\mathsf{s},0)}\right)/{\overset{*}{\leftrightarrow}_{\mathcal{R}_{(\times,+)}}}$ to $\mathrm{T}\left(\Sigma_{(\mathsf{s},0)}\right)$. Let $\mathcal{N}_{(\times,+,\mathsf{s},0)} = \langle \mathrm{T}\left(\Sigma_{(\mathsf{s},0)}\right); \times^{\mathcal{N}}, +^{\mathcal{N}}, \mathsf{s}^{\mathcal{N}}, \mathsf{0}^{\mathcal{N}}\rangle$ be a $\Sigma_{(\times,+,\mathsf{s},0)}$-algebra, where operations are given by $\times^{\mathcal{N}}(s,t) = \times(s,t){\downarrow}$, $+^{\mathcal{N}}(s,t) = +(s,t){\downarrow}$, $\mathsf{s}^{\mathcal{N}}(t) = \mathsf{s}(t)$ and $\mathsf{0}^{\mathcal{N}} = \mathsf{0}$. Then it is easy to check that φ is a $\Sigma_{(\times,+,\mathsf{s},0)}$-homomorphism, and thus, $\mathcal{I}_{\mathcal{R}_{(\times,+)}} \cong \mathcal{N}_{(\times,+,\mathsf{s},0)}$. Since $\mathbb{N}_{(\times,+,\mathsf{s},0)}$ is isomorphic to $\mathcal{N}_{(\times,+,\mathsf{s},0)}$ via an obvious bijection $\{n \mapsto \mathsf{s}^n(\mathsf{0}) \mid n \in \mathbb{N}\}$, the claim follows. □

Proof: [of Lemma 3.2] By induction on s. □

Proof: [of Lemma 3.4] ($\Rightarrow$) Suppose $\mathbb{N}_{(\times,+,\mathsf{s},0)} \models s \approx t$. Then, for any valuation $\rho : \mathcal{V} \to \mathbb{N}$, we have $[\![s]\!]_{\mathbb{N}_{(\times,+,\mathsf{s},0)},\rho} = [\![t]\!]_{\mathbb{N}_{(\times,+,\mathsf{s},0)},\rho}$. Since $\mathbb{N}^\circ$ is a subalgebra of $\mathbb{Z}^\circ$, it follows that, for any valuation $\rho : \mathcal{V} \to \mathbb{N}$, $[\![s]\!]_{\mathbb{Z}^\circ,\rho} = [\![t]\!]_{\mathbb{Z}^\circ,\rho}$. Hence by Lemma 3.2, $(\!|s|\!)_{\mathbb{Z}}(a_1,\ldots,a_n) = (\!|t|\!)_{\mathbb{Z}}(a_1,\ldots,a_n)$ for any $a_1,\ldots,a_n \in \mathbb{N}$. Since $\mathbb{N} \subseteq \mathbb{Z}$ is an infinite set and $\langle \mathbb{Z}; \times, +, 1, 0\rangle$ is an integral domain, we have $(\!|s|\!) = (\!|t|\!)$ by Proposition 3.3.
($\Leftarrow$) If $(\!|s|\!) = (\!|t|\!)$ then $(\!|s|\!)(a_1,\ldots,a_n) = (\!|t|\!)(a_1,\ldots,a_n)$ for any $a_1,\ldots,a_n \in \mathbb{Z}$. Hence, by Lemma 3.2, $[\![s]\!]_{\mathbb{Z}^\circ,\rho} = [\![t]\!]_{\mathbb{Z}^\circ,\rho}$ for any valuation ρ on $\mathbb{Z}^\circ$. In particular, $[\![s]\!]_{\mathbb{N}_{(\times,+,\mathsf{s},0)},\rho} = [\![t]\!]_{\mathbb{N}_{(\times,+,\mathsf{s},0)},\rho}$ for any valuation ρ on $\mathbb{N}^\circ$, as $\mathbb{N}_{(\times,+,\mathsf{s},0)} \cong \mathbb{N}^\circ$ is a subalgebra of $\mathbb{Z}^\circ$. □

Proof: [of Theorem 3.7] As for Theorem 3.5 but taking into account that the computation of the list of monomial expressions $\mathsf{Mono}(\hat{s})$ can be done in $\mathcal{O}(|\hat{s}|)$ if the term $\hat{s}$ does not contain the multiplication $\times$. □

Proof: [of Proposition 3.8] Let us denote by $\mathbb{Z}_+[x_1,\ldots,x_n]$ the set of formal polynomials over the indeterminates $x_1,\ldots,x_n$ with natural number coefficients. First note that $\exists a_1,\ldots,a_n \in \mathbb{Z}.\ \varphi(a_1,\ldots,a_n) = 0$ iff $\exists a_1,\ldots,a_n \in \mathbb{N}.\ \varphi(\delta_1 a_1,\ldots,\delta_n a_n) = 0$ for some $\delta_1,\ldots,\delta_n \in \{-1,1\}$, where $\varphi \in \mathbb{Z}[x_1,\ldots,x_n]$; thus, it is a corollary of the undecidability of Hilbert's 10th problem that it is undecidable whether $\exists a_1,\ldots,a_n \in \mathbb{N}.\ \varphi(a_1,\ldots,a_n) = 0$ for given $\varphi \in \mathbb{Z}[x_1,\ldots,x_n]$ (†). For any $\varphi \in \mathbb{Z}[x_1,\ldots,x_n]$, there exist $\varphi_{\mathsf{p}}, \varphi_{\mathsf{n}} \in \mathbb{Z}_+[x_1,\ldots,x_n]$ such that $\varphi = \varphi_{\mathsf{p}} - \varphi_{\mathsf{n}}$. Since $\exists a_1,\ldots,a_n \in \mathbb{N}.\ \varphi(a_1,\ldots,a_n) = 0$ iff $\exists a_1,\ldots,a_n \in \mathbb{N}.\ \varphi_{\mathsf{p}}(a_1,\ldots,a_n) = \varphi_{\mathsf{n}}(a_1,\ldots,a_n)$, it follows from (†) that it is undecidable whether $\exists a_1,\cdots,a_n \in \mathbb{N}.\ \varphi(a_1,\ldots,a_n) = \psi(a_1,\ldots,a_n)$ for given $\varphi,\psi \in \mathbb{Z}_+[x_1,\ldots,x_n]$ (‡). Let $u,v \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)},\mathcal{V})$. It is easy to check that $\mathcal{R}_{(\mathsf{eq},\times,+)}$ is convergent and sufficiently complete [5], and hence $\mathcal{R}_{(\mathsf{eq},\times,+)} \models_{ind} \mathsf{eq}(u,v) \approx \mathsf{0}$ iff $(\!|u|\!)(a_1,\ldots,a_n) \neq (\!|v|\!)(a_1,\ldots,a_n)$ for any $a_1,\ldots,a_n \in \mathbb{N}$. If it is decidable whether $\mathcal{R}_{(\mathsf{eq},\times,+)} \models_{ind} \mathsf{eq}(u,v) \approx \mathsf{0}$, then so is whether $\forall a_1,\ldots,a_n \in \mathbb{N}.\ (\!|u|\!)(a_1,\ldots,a_n) \neq (\!|v|\!)(a_1,\ldots,a_n)$ and so is $\exists a_1,\ldots,a_n \in \mathbb{N}.\ \varphi(a_1,\ldots,a_n) = \psi(a_1,\ldots,a_n)$ for given $\varphi,\psi \in \mathbb{Z}_+[x_1,\ldots,x_n]$. This contradicts (‡). □

Proof: [of Lemma 4.1] Similar to Lemma 3.1. Note that it is easy to check that $\mathcal{R}_{(\mathsf{len},\mathsf{rev},@,\times,+)}$ is convergent and sufficiently complete [5]. □

Proof: [of Lemma 4.2] Let $s \in \mathrm{T}(\Sigma_{(\mathsf{single},\ldots)},\mathcal{V})$. First, eliminate all occurrences of :: by the third rule. The size of the term is at most doubled by this. Then, normalize recursively using len-rules the outermost subterms of the form $\mathsf{len}(u)$ with $u \notin \mathcal{V}$. Next, normalize using rev-rules by counting the number k of occurrences of rev along the path, swapping arguments of @ if k is odd and eliminating rev. Finally, if s has sort N replace each $\mathsf{len}(xs)$ with $\delta(\mathsf{len}(xs))$, else (i.e. if s has sort L) change the final (list)-term to a list of (elem)-terms by listing up all non-nil (elem)-terms from left to right. Clearly, $\mathsf{Abs}(s{\downarrow})$ (or $\mathsf{List}(s{\downarrow})$) is obtained, and each step can be done in $\mathcal{O}(|s|)$. Thus overall computation can be done in polynomial time. □

Proof: [of Lemma 4.3] We show (1) and (2) simultaneously by Noetherian induction on s w.r.t. $\rhd \cup \to_{\mathcal{S}}$.
(1) All cases satisfying $s(\epsilon) \neq \mathsf{len}$ are straightforward by the induction hypothesis. Suppose $s = \mathsf{len}(ts)$. By induction hypothesis, $ts{\downarrow}$ is a (list)-term. If $ts{\downarrow} = xs \in \mathcal{V}$ then $s{\downarrow} = \mathsf{len}(xs) \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$ and the claim follows. Otherwise, $s = \mathsf{len}(ts) \overset{*}{\to}_{\mathcal{S}} \mathsf{len}(ts{\downarrow}) \to_{\mathcal{S}} s'$ for some s'. Then, by induction hypothesis, $s{\downarrow} = s'{\downarrow} \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$.
(2) We distinguish six cases:

1. $s \in \mathcal{V}^L$. Then $s{\downarrow}\,(= s)$ is an (elem)-term, which is a (degenerated) (list)-term.
2. $s = \mathsf{nil}$. Then $s{\downarrow}\,(= s)$ is a (list)-term.
3. $s = ::(t_1,t_2)$. Then $s \to_{\mathcal{S}} @(\mathsf{single}(t_1),t_2) = s'$. By induction hypothesis, $t_1{\downarrow}$ and $t_2{\downarrow}$ are (list)-terms, so $s{\downarrow}\,(= s'{\downarrow})$ is a (list)-term.
4. $s = \mathsf{single}(t)$. Then, by induction hypothesis, $t{\downarrow} \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0)},\mathcal{V}^N \cup \{\mathsf{len}(xs) \mid xs \in \mathcal{V}^L\})$. Since $s{\downarrow} = \mathsf{single}(t{\downarrow})$, $s{\downarrow}$ is a (list)-term by definition.
5. $s = \mathsf{rev}(ts)$. Then by induction hypothesis $ts{\downarrow}$ is a (list)-term. If $ts{\downarrow} \notin \mathcal{V}$ then $s = \mathsf{rev}(ts) \overset{*}{\to}_{\mathcal{S}} \mathsf{rev}(ts{\downarrow}) \to_{\mathcal{S}} s'$ for some s'. By induction hypothesis, $s'{\downarrow}$ is a (list)-term, so $s{\downarrow}$ is it, too. If $ts{\downarrow} \in \mathcal{V}$ then, by definition, $\mathsf{rev}(ts{\downarrow})$ (hence $s{\downarrow}$) is a (list)-term.
6. $s = @(t_1,t_2)$. By induction hypothesis, for each $i = 1,2$, $t_i{\downarrow} = w_i$ is a (list)-term.

   We distinguish two cases.

   (a) $w_1 = \mathsf{nil}$ or $w_2 = \mathsf{nil}$. Then $s \overset{*}{\to}_{\mathcal{S}} @(w_1,w_2) \to_{\mathcal{S}} s'$ for some s'. The claim follows from $s{\downarrow} = s'{\downarrow}$ and the induction hypothesis.

   (b) Otherwise, for $i = 1,2$, either $w_i = @(w_i',w_i'')$, $w_i = xs \in \mathcal{V}^L$, $w_i = \mathsf{single}(u_i)$ for some $u_i \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},0,\mathsf{len})},\mathcal{V})^N$, or $w_i = \mathsf{rev}(xs)$. In either cases, $@(w_1,w_2)$ is a (list)-term.

□

Proof: [of Lemma 4.4] For any $l \to r \in \mathcal{S}$ and valuation ρ on $\mathbb{L}$, $[\![l]\!]_\rho = [\![r]\!]_\rho$. Hence $\mathbb{L} \models s \approx s\!\downarrow$ and $\mathbb{L} \models t \approx t\!\downarrow$. Thus $\mathbb{L} \models s\!\downarrow \approx t\!\downarrow$ iff $\mathbb{L} \models s \approx t$.

1. Let $s, t \in \mathrm{T}(\Sigma_{(\mathsf{len},\ldots)}, \mathcal{V})^N$. Let $u \in \mathrm{T}(\Sigma_{(\times,+,\mathsf{s},\mathsf{0},\mathsf{len})}, \mathcal{V})^N$. Since the length of lists ranges over natural numbers, for any valuation ρ on $\mathbb{N}$, there exists a valuation ρ' on $\mathbb{L}$ such that $[\![\mathsf{Abs}(u)]\!]_\rho = [\![u]\!]_{\rho'}$ and vice versa. Thus, it follows from Lemma 4.3 and $\mathrm{T}(\Sigma_{(\mathsf{len},\ldots)}, \mathcal{V})^N \subseteq \mathrm{T}(\Sigma_{(\mathsf{single},\ldots)}, \mathcal{V})^N$ that if $[\![s\!\downarrow]\!]_\rho \neq [\![t\!\downarrow]\!]_\rho$ then $[\![\mathsf{Abs}(s\!\downarrow)]\!]_{\rho'} \neq [\![\mathsf{Abs}(t\!\downarrow)]\!]_{\rho'}$ for some ρ', and if $[\![\mathsf{Abs}(s\!\downarrow)]\!]_\rho \neq [\![\mathsf{Abs}(t\!\downarrow)]\!]_\rho$ then $[\![s\!\downarrow]\!]_{\rho'} \neq [\![t\!\downarrow]\!]_{\rho'}$ for some ρ'. Thus the claim follows.

2. ($\Rightarrow$) If $k \neq l$, then take a valuation ρ such that $\rho(xs) = [0]$ for all $xs \in \mathcal{V}^L$. Then, for any (elem)-term v, $[\![v]\!]_\rho$ is a singleton list, and thus the length of $[\![s\!\downarrow]\!]_\rho$ equals to k and that of $[\![t\!\downarrow]\!]_\rho$ equals to l. Hence, $[\![s\!\downarrow]\!]_\rho \neq [\![t\!\downarrow]\!]_\rho$. Next, suppose otherwise, i.e. $k = l$. We show if there exists some i such that none of (i), (ii), (iii) holds, then $[\![u_i]\!]_\rho \neq [\![v_i]\!]_\rho$ (and hence $[\![s\!\downarrow]\!]_\rho \neq [\![t\!\downarrow]\!]_\rho$) holds for some ρ. We distinguish six cases, where we omit the symmetric case.

1. $u_i = xs$ and $v_i = ys$ with $xs \neq ys$. Then it's easy to see $[\![u_i]\!]_\rho \neq [\![v_i]\!]_\rho$ for some ρ.
2. $u_i = xs$ and $v_i = \mathsf{single}(\hat{v}_i)$. Then it suffices to take ρ such that $\rho(xs) = [\,]$.
3. $u_i = xs$ and $v_i = \mathsf{rev}(ys)$. If $xs \neq ys$ then it's easy to see $[\![u_i]\!]_\rho \neq [\![v_i]\!]_\rho$ for some ρ. If $xs = ys$ then it suffices to take ρ such that $\rho(xs) = [0, 1]$, as $[\![u_i]\!]_\rho = [0, 1] \neq [1, 0] = [\![v_i]\!]_\rho$.
4. $u_i = \mathsf{single}(\hat{u}_i)$ and $v_i = \mathsf{single}(\hat{v}_i)$. Then we have $\hat{u}_i \neq \hat{v}_i$ and hence $[\![\hat{u}_i]\!]_\rho \neq [\![\hat{v}_i]\!]_\rho$ for some ρ by the case (1). This implies $[\![u_i]\!]_\rho \neq [\![v_i]\!]_\rho$.
5. $u_i = \mathsf{single}(\hat{u}_i)$ and $v_i = \mathsf{rev}(xs)$. Then it suffices to take ρ such that $\rho(xs) = [0, 1]$.
6. $u_i = \mathsf{rev}(xs)$ and $v_i = \mathsf{rev}(ys)$ with $xs \neq ys$. Then it's easy to see $[\![u_i]\!]_\rho \neq [\![v_i]\!]_\rho$ for some ρ.

($\Leftarrow$) Suppose $k = l$ and for each $1 \leq i \leq k$, either (i), (ii) or (iii) holds. It suffices to claim $\mathbb{L} \models u_i \approx v_i$ for all $1 \leq i \leq k$. Cases (i) and (ii) are trivial. Case (iii) follows by (1). Hence $\mathbb{L} \models u_i \approx v_i$ for all i.

□

Proof: [of Theorem 4.7] Similar to the proof of Theorem 4.5, using Theorem 3.7 instead of Theorem 3.5. □

Proof: [of Lemma 5.3] Similar to Lemma 3.1. □

Proof: [of Lemma 5.4] Procedure `max-min-check(s,t)` can be implemented like this:

1. For a (max)-term u, let $\Phi(u)$ be given recursively like this: $\Phi(x) = \{\{x\}\}$, $\Phi(\mathsf{0}) = \{\{\mathsf{0}\}\}$, $\Phi(\mathsf{min}(u, v)) = \{X \cup Y \mid X \in \Phi(u), Y \in \Phi(v)\}$ and $\Phi(\mathsf{max}(u, v)) = \Phi(u) \cup \Phi(v)$. Then it is easy to see $\Phi(u) = [u\!\downarrow]$ for $u \in \{s, t\}$. Compute $\Phi(s)$ and $\Phi(t)$. Clearly, $\Phi(s)$ ($\Phi(t)$) can be computed in $\mathcal{O}(2^{|s|})$ (resp. $\mathcal{O}(2^{|t|})$), and since $\Phi(s)$ is a set of sets of variables in s, we have $|\Phi(s)| \leq 2^{|s|}$.
2. Compute $\mathcal{M}in(\Phi(s))$ and $\mathcal{M}in(\Phi(t))$. This can be done in $\mathcal{O}(|\Phi(s)|^2) + \mathcal{O}(|\Phi(t)|^2)$.
3. Finally check $\mathcal{M}in(\Phi(s)) = \mathcal{M}in(\Phi(t))$. This can be done in $\mathcal{O}(|\Phi(s)| \times |\Phi(t)|)$.

Thus the overall computation can be done in $\mathcal{O}(2^{(|s|+|t|)})$. □

Proof: [of Lemma 5.6] (1) This holds, since $\min(A \cup B) = \min\{\min(A), \min(B)\}$ holds for any non-empty $A, B \subseteq \mathbb{N}$. (2) For any non-empty $A, B \subseteq \mathbb{N}$, $A \subseteq B$ implies $\min(B) \leq \min(A)$: The case $A = B$ is trivial. Otherwise $B = A \cup C$ for some non-empty C, and so, $\min(A) = \min(B \cup C) = \min\{\min(B), \min(C)\} \leq \min(B)$. The claim follows immediately from this. □

Proof: [of Lemma 5.7] The case $A, B \in \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\}$ follows from Lemma 5.6 (2). If $A = \top$, then $A \subseteq^\circ B$ implies $B = \top$. Thus the claim follows trivially. If $B = \top$, then $\mathsf{Min}_\rho(B) = 0$, and thus $\mathsf{Min}_\rho(B) \leq \mathsf{Min}_\rho(A)$ holds for any A. □

Proof: [of Lemma 5.8] If v contains $\mathsf{0}$ then, clearly, $[\![v]\!]_\rho = 0$. Thus, $\mathsf{Min}_\rho([v]_{min}) = \mathsf{Min}_\rho(\top) = 0 = [\![v]\!]_\rho$. It remains to show the case that v does not contain $\mathsf{0}$. We prove $\mathsf{Min}_\rho([v]_{min}) = [\![v]\!]_\rho$ for any (min)-term v not containing $\mathsf{0}$ by induction on v. If $v = x \in \mathcal{V}$ then $\mathsf{Min}_\rho([x]_{min}) = \mathsf{Min}_\rho(\{x\}) = \min\{\rho(x)\} = \rho(x) = [\![x]\!]_\rho$. Otherwise $v = \mathsf{min}(v_1, v_2)$, for v_1, v_2 not containing $\mathsf{0}$. As v_1, v_2 does not contain $\mathsf{0}$, $[\mathsf{min}(v_1, v_2)]_{min} = [v_1]_{min} \cup [v_2]_{min}$. Hence, by Lemma 5.6 (1) and induction hypothesis, we have $\mathsf{Min}_\rho([\mathsf{min}(v_1, v_2)]_{min}) = \mathsf{Min}_\rho([v_1]_{min} \cup [v_2]_{min}) = \min(\mathsf{Min}_\rho([v_1]_{min}), \mathsf{Min}_\rho([v_2]_{min})) = \min([\![v_1]\!]_\rho, [\![v_2]\!]_\rho) = [\![\mathsf{min}(v_1, v_2)]\!]_\rho$. □

Proof: [of Lemma 5.10] By induction on w, we have the following cases:

- w is a (min)-term. Then, using Lemma 5.8, we have $\mathsf{Max}_\rho([w]_{max}) = \mathsf{Max}_\rho(\{[w]_{min}\}) = \max\{\mathsf{Min}_\rho([w]_{min})\} = \mathsf{Min}_\rho([w]_{min}) = [\![w]\!]_\rho$.
- $w = \mathsf{max}(w_1, w_2)$. Then, we have $\mathsf{Max}_\rho([w]_{max}) = \mathsf{Max}_\rho([w_1]_{max} \cup [w_2]_{max}) = \max\{\mathsf{Max}_\rho([w_1]_{max}), \mathsf{Max}_\rho([w_2]_{max})\} = \max\{[\![w_1]\!]_\rho, [\![w_2]\!]_\rho\} = [\![\mathsf{max}(w_1, w_2)]\!]_\rho = [\![w]\!]_\rho$.

□

Proof: [of Lemma 5.11] Suppose $A, B \in S$ and $A \subseteq^\circ B \neq A$. Then by Lemma 5.7, $\mathsf{Min}_\rho(B) \leq \mathsf{Min}_\rho(A)$. Thus $\mathsf{Max}_\rho(S) = \mathsf{Max}_\rho(S \setminus \{B\})$. The claim readily follows from this. □

Proof: [of Lemma 5.12] ($\Rightarrow$) Obvious. ($\Leftarrow$) Let $X = \{x \in \mathcal{V} \mid \exists X.\ x \in X \in S \cup T\}$. Suppose $\forall \rho.\ \mathsf{Max}_\rho(S) = \mathsf{Max}_\rho(T)$. Suppose $\top \in S$. Then, by minimality of S, $S = \{\top\}$. If $\top \in T$ then, by minimality of T, $T = \{\top\} = S$. Otherwise, $T \subseteq \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\}$. Then, since T is non-empty, we have $\mathsf{Max}_\rho(T) = 1$ by taking $\rho = \{x \mapsto 1 \mid x \in X\}$. Since $\mathsf{Max}_\rho(S) = 0$, this is a contradiction. Thus, $T = \{\top\} = S$ if $\top \in S \cup T$. Therefore it remains to show the case $\top \notin S \cup T$, i.e. $S, T \subseteq \{X \subseteq \mathcal{V} \mid X \neq \emptyset, |X| < \infty\}$. Suppose $S \neq T$. Then w.l.o.g. one can assume that there exists $A \in S \setminus T$. We distinguish two cases.

1. There exists $B \in T$ such that $B \subseteq A \neq B$. Let $\rho = \{x \mapsto 1 \mid x \in B\} \cup \{x \mapsto 0 \mid x \in X \setminus B\}$. Clearly, $\mathsf{Min}_\rho(B) = 1$. Since $A \setminus B \neq \emptyset$, $\mathsf{Min}_\rho(A) = 0$. Let $A' \in S \setminus \{A\}$. Then we have $A' \setminus A \neq \emptyset$ by minimality, and hence $A' \setminus B \neq \emptyset$ by $B \subseteq A$. Hence $\mathsf{Min}_\rho(A') = 0$. Thus, since $\mathsf{Min}_\rho(A') = 0$ for all $A' \in S$, we have $\mathsf{Max}_\rho(S) = 0$. On the other hand, since $[\![B]\!]_\rho = 1$, we have $\mathsf{Max}_\rho(T) \geq 1$. This is a contradiction.
2. There exists no $B \in T$ such that $B \subseteq A \neq B$. Let $\rho = \{x \mapsto 1 \mid x \in A\} \cup \{x \mapsto 0 \mid x \in X\}$. Then we have $[\![A]\!]_\rho = 1$. On the other hand, for any $B \in T$, we have $B \setminus A \neq \emptyset$, and hence $[\![B]\!]_\rho = 0$. Thus $\mathsf{Max}_\rho(S) = 1$ and $\mathsf{Max}_\rho(T) = 0$. This is a contradiction.

□

Proof: [of Theorem 5.14] For the correctness of `max-min-check(s,t)`, by Lemmas 5.3 and 5.13, $\mathcal{R}_{(\mathsf{max},\mathsf{min})} \models_{ind}$

$s \approx t$ iff $\mathbb{N}_{(\mathsf{max},\mathsf{min},\mathsf{s},0)} \models s \approx t$ iff `max-min-check(`s`,`t`)` returns 'yes'. By Lemma 5.4, the procedure `max-min-check(`s`,`t`)` runs in exponential time. □

Proof: [of Lemma 5.17] Similar to Lemma 3.1. □

Proof: [of Lemma 5.18] Procedure `max-check` can be implemented more efficiently like this:

1. For each occurrence of $u \in \mathcal{V} \cup \{\mathsf{0}\}$ in s, count the number k of s from the root of the term to that occurrence, and collect all $\langle k, u\rangle$. This can be done in $\mathcal{O}(|s|)$. Let the collection be S. Clearly, $|S| \leq |s|$. Compute a set T by applying the same procedure to t.
2. Eliminate non-maximal elements w.r.t. $\prec$ in S (T). This can be done in $\mathcal{O}(|S|^2)$ (resp. $\mathcal{O}(|T|^2)$).
3. Check $S = T$ (as sets of (s)-terms). This can be done in $\mathcal{O}(|S| \times |T|)$.

Thus the overall procedure is $\mathcal{O}((|s| + |t|)^2)$. Hence the claim follows. □

Proof: [of Lemma 5.19] In the following, let us abbreviate $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)}$ as $\mathbb{N}$, $u{\downarrow}$ as $u{\downarrow}$ for $u \in \{s, t\}$. Since $\mathbb{N} \models \mathsf{s}(\mathsf{max}(x, y)) \approx \mathsf{max}(\mathsf{s}(x), \mathsf{s}(y))$, we have $\mathbb{N} \models s \approx t$ iff $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$. Thus it remains to show that `max-check(`s`,`t`)` returns 'yes' iff $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$.

For any non-empty finite set $U = \{u_1, \ldots, u_n\}$ of (s)-terms, let $\mathsf{Max}(U) = \mathsf{max}(u_1, \mathsf{max}(u_2, \ldots, \mathsf{max}(u_{n-1}, u_n) \cdots))$. Then $\mathbb{N} \models u{\downarrow} \approx \mathsf{Max}([u{\downarrow}])$ for $u \in \{s, t\}$ by definition.

For any $u = \mathsf{s}^n(z)$ and $v = \mathsf{s}^m(z)$ with $n \leq m$ ($z \in \mathcal{V} \cup \{\mathsf{0}\}$), we have $\mathbb{N} \models \mathsf{max}(u, v) \approx v$. For $u = \mathsf{s}^n(\mathsf{0})$ and $v = \mathsf{s}^m(x)$ with $n \leq m$, we have $\mathbb{N} \models \mathsf{max}(u, v) \approx v$. Thus for any (s)-terms u, v such that $u \prec v$, we obtain $\mathbb{N} \models \mathsf{max}(u, v) \approx v$. Hence, we have $\mathbb{N} \models \mathsf{Max}(\mathcal{M}ax_{\prec}(U)) \approx \mathsf{Max}(U)$ for any non-empty finite set U of (s)-terms. Hence we have $\mathbb{N} \models u{\downarrow} \approx \mathsf{Max}([u{\downarrow}]) \approx \mathsf{Max}(\mathcal{M}ax_{\prec}([u{\downarrow}]))$ for $u \in \{s, t\}$ by definition. Let $S = \mathcal{M}ax_{\prec}([s{\downarrow}])$ and $T = \mathcal{M}ax_{\prec}([t{\downarrow}])$.

Suppose `max-check(`s`,`t`)` returns 'yes'. Then, by the definition of the procedure, we have $S = T$. Then, $\mathbb{N} \models s{\downarrow} \approx \mathsf{Max}(S) \approx \mathsf{Max}(T) \approx t{\downarrow}$, and thus $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$. Thus it remains to show the converse.

Suppose $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$. By $\mathbb{N} \models s{\downarrow} \approx \mathsf{Max}(S)$ and $\mathbb{N} \models t{\downarrow} \approx \mathsf{Max}(T)$, we have $\mathbb{N} \models \mathsf{Max}(S) = \mathsf{Max}(T)$. By the definition of the procedure, it suffices to show $S = T$.

Let $X = \{x \in \mathcal{V} \mid \mathsf{s}^n(x) \in S \cup T, \text{ for some } n \in \mathbb{N}\}$ and $Y = \{x \in \mathcal{V} \mid \mathsf{s}^n(x) \in T, \text{ for some } n \in \mathbb{N}\}$. Let $\rho = \{x \mapsto 0 \mid x \in X \cup Y\}$ and $k = \max\{[\![u]\!]_\rho \mid u \in S \cup T\}$.

Firstly, we claim $X = Y$. For this, we suppose $X \neq Y$ and show the contradiction. W.l.o.g. assume $\mathsf{s}^n(x) \in S$ and $x \notin Y$. Then by taking a valuation $\delta = \{x \mapsto k + 1\} \cup \{y \mapsto 0 \mid x \neq y, y \in X \cup Y\}$, we have $[\![\mathsf{Max}(S)]\!]_\delta \geq k + n + 1 > k = [\![\mathsf{Max}(T)]\!]_\delta$. This is a contradiction. Thus we have $X = Y$.

Next we show that if $\mathsf{s}^n(x) \in S$ and $\mathsf{s}^m(x) \in T$ then $n = m$. Suppose to the contrary that there exists $x \in \mathcal{V}$ such that $\mathsf{s}^n(x) \in S$ and $\mathsf{s}^m(x) \in T$ with $n \neq m$. Then by taking $\delta = \{x \mapsto k + 1\} \cup \{y \mapsto 0 \mid x \neq y, y \in X \cup Y\}$, we have $[\![\mathsf{Max}(S)]\!]_\delta = n + k + 1 \neq m + k + 1 = [\![\mathsf{Max}(T)]\!]_\delta$. This is a contradiction. Thus $\mathsf{s}^n(x) \in S$ and $\mathsf{s}^m(x) \in T$ imply $n = m$.

Let $U = \{\mathsf{s}^n(x) \mid \mathsf{s}^n(x) \in S, x \in \mathcal{V}\}$. We have shown that either $S = U$ or $S = U \cup \{\mathsf{s}^n(\mathsf{0})\}$ and either $T = U$ or $T = U \cup \{\mathsf{s}^m(\mathsf{0})\}$ for some n, m. If $S = U = T$, we are done. Suppose $S = U$ and $T = U \cup \{\mathsf{s}^m(\mathsf{0})\}$. Then, by definition of $\prec$, we have $m > n$ for any $\mathsf{s}^n(x) \in U$. Thus, by taking a valuation $\rho = \{x \mapsto 0 \mid x \in X\}$, $[\![\mathsf{Max}(S)]\!]_\rho = \max\{n \mid \mathsf{s}^n(x) \in U\} < m = [\![\mathsf{Max}(T)]\!]_\rho$. This is a contradiction. Similarly, it does not happen the case $S = U \cup \{\mathsf{s}^n(\mathsf{0})\}$ and $T = U$ for some n. It remains to show that if $S = U \cup \{\mathsf{s}^l(\mathsf{0})\}$ and $T = U \cup \{\mathsf{s}^m(\mathsf{0})\}$ then $l = m$. Suppose $l \neq m$. Suppose $S = U \cup \{\mathsf{s}^l(\mathsf{0})\}$ and $T = U \cup \{\mathsf{s}^m(\mathsf{0})\}$. Then by definition of $\prec$, we have $l, m > n$ for any $\mathsf{s}^n(x) \in U$. Thus, by taking a valuation $\rho = \{x \mapsto 0 \mid x \in X\}$, $[\![\mathsf{Max}(S)]\!]_\rho = l \neq m = [\![\mathsf{Max}(T)]\!]_\rho$. This is a contradiction. Thus, in all cases, we conclude $S = T$.

Therefore, $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$ implies $S = T$. Hence `max-check(`s`,`t`)` returns 'yes' iff $\mathbb{N} \models s{\downarrow} \approx t{\downarrow}$. □

Proof: [of Theorem 5.20] By Lemmas 5.17 and 5.19, $\mathcal{R}_{(\mathsf{max})} \models_{ind} s \approx t$ iff $\mathbb{N}_{(\mathsf{max},\mathsf{s},0)} \models s \approx t$ iff `max-check(`s`,`t`)` returns 'yes'. The procedure `max-check(`s`,`t`)` can be done in polynomial time by Lemma 5.18. □