On the Word, Subsumption, and Complement Problem for Recurrent Term Schematizations

Miki Hermann, Gernot Salzer

On the Word, Subsumption, and Complement Problem for Recurrent Term Schematizations*

Miki Hermann[1] and Gernot Salzer[2]

[1] LORIA (CNRS), BP 239, 54506 Vandœuvre-lès-Nancy, France. hermann@loria.fr
[2] Technische Universität Wien, Karlsplatz 13, 1040 Wien, Austria. salzer@logic.at

Abstract. We investigate the word and the subsumption problem for recurrent term schematizations, which are a special type of constraints based on iteration. By means of unification, we reduce these problems to a fragment of Presburger arithmetic. Our approach is applicable to all recurrent term schematizations having a finitary unification algorithm. Furthermore, we study a particular form of the complement problem. Given a finite set of terms, we ask whether its complement can be finitely represented by schematizations, using only the equality predicate without negation. The answer is negative as there are ground terms too complex to be represented by schematizations with limited resources.

1 Introduction

Infinite sets of first-order terms with structural similarities appear frequently in several branches of automated deduction, like logic programming, model building, term rewriting, equational unification, or clausal theorem proving. They are usually produced by saturation-based procedures, like equational completion or hyper-resolution. A usual requirement for effective use of such sets is the possibility to handle them by finite means. There exist several approaches to cope with this phenomenon, like lazy evaluation, set constraints, or term schematizations. Lazy evaluation usually does not combine well with unification or other operations. Set constraints allow to describe regular sets of first-order terms, using the potential of regular tree grammars and tree automata, and having the good properties of regular tree languages. Schematizations exploit the recurring term structure in infinite sets, as produced by self-resolving clauses or by self-overlapping rewrite rules.

Several formalisms for recurrent term schematizations were introduced within the last years. They rely on the same principle, namely the iteration of first-order contexts, but differ in the expressive power. The main concern in this work is the decidability of unification and the construction of finite complete sets of unifiers. Formalisms satisfying these requirements are ρ-terms [CH95], I-terms [Com95], R-terms [Sal92], and primal grammars [HG97], all of them with a finitary unification algorithm. Set operations were studied in [AHL97].

* This work was done while the second author was visiting LORIA. His visit was funded by Univeristé Henri Poincaré, Nancy 1.

Applications of recurrent schematizations are quite rare and mostly theoretical, like in model building [Pel97] or cycle unification [Sal94]. One reason is that there are still some open problems to be solved prior to a successful implementation. A *sine qua non* of automated deduction is redundancy elimination. The elementary tools in this respect are testing for equality and subsumption. In other words, we need to solve the word problem and the subsumption problem for recurrent term schematizations. Moreover, only positive set operations were studied in [AHL97] without considering the complement. Complement building is interesting from the algebraic and logic point of view, e.g., during construction of counter-examples or for quantifier elimination.

In the first part of the paper, we investigate the word and the subsumption problem for primal grammars. By means of unification, we reduce them to a problem in Presburger arithmetic. Our approach is applicable to all recurrent term schematizations having a finitary unification algorithm. In the second part, we study a particular form of the complement problem. Given a finite set of terms, we ask whether its complement can be represented finitely by schematizations, using only the equality predicate without negation. The answer is negative as there are ground first-order terms too complex to be represented by primal grammars with limited resources.

2 Term schematizations

2.1 Syntax

The language of primal terms is based on four kinds of symbols: first-order variables $\mathcal{V}$, counter variables $\mathcal{C}$, function symbols $\mathcal{F}_p$ of arities $p \geq 0$, and defined symbols $\mathcal{D}_{q,p}$ of counter arities $q \geq 1$ and first-order arities $p \geq 0$. Nullary function symbols are called constants. The set of all function and defined symbols is denoted by $\mathcal{F}$ and $\mathcal{D}$, respectively.

Let $\mathbb{N}$ be the set of natural numbers. The set of *counter expressions* $\mathcal{L}$ is the set of linear expressions over $\mathcal{C}$ with coefficients in $\mathbb{N}$. It can be defined inductively as the smallest set satisfying the following conditions.

- $\mathbb{N} \subseteq \mathcal{L}$ and $\mathcal{C} \subseteq \mathcal{L}$
- $(cl) \in \mathcal{L}$ if $c \in \mathbb{N}$ and $l \in \mathcal{L}$
- $(l_1 + l_2) \in \mathcal{L}$ if $l_1, l_2 \in \mathcal{L}$

Two counter expressions are considered equal if they are equivalent with respect to the usual equalities of addition and multiplication. Furthermore, we drop parentheses where possible and do not distinguish between natural numbers and their symbolic representation.

The set of *primal terms* $\mathcal{P}$ is defined inductively as the smallest set satisfying the following conditions.

- $\mathcal{V} \subseteq \mathcal{P}$
- $f(\mathbf{t}) \in \mathcal{P}$ if $f \in \mathcal{F}_p$ and $\mathbf{t} \in \mathcal{P}^p$
- $\hat{f}(\mathbf{l}; \mathbf{t}) \in \mathcal{P}$ if $\hat{f} \in \mathcal{D}_{q,p}$, $\mathbf{l} \in \mathcal{L}^q$, and $\mathbf{t} \in \mathcal{P}^p$

The sets of counter variables and first-order variables of a primal term t are denoted by $\mathcal{CV}ar(t)$ and $\mathcal{V}ar(t)$, respectively.

Example 1. Let $x \in \mathcal{V}$, $a \in \mathcal{F}_0$, $h \in \mathcal{F}_2$, $m, n \in \mathcal{C}$, $\hat{f} \in \mathcal{D}_{1,1}$, and $\hat{g} \in \mathcal{D}_{2,0}$. Then $h(\hat{f}(3m+2; \hat{f}(5; h(a,x))), \hat{g}(m, m+n))$ is a primal term.

2.2 Semantics

In the sequel, we assume that the reader is familiar with the basic notions of term rewriting. With each defined symbol $\hat{f} \in \mathcal{D}_{q,p}$, we associate two rewrite rules $\hat{f}(0, \mathbf{n}; \mathbf{x}) \to r_1^{\hat{f}}$ and $\hat{f}(m+1, \mathbf{n}; \mathbf{x}) \to r_2^{\hat{f}}[\hat{f}(m, \mathbf{n}+\boldsymbol{\delta}; \mathbf{x})]_A$, where

- $m, \mathbf{n}$ and $\mathbf{x}$ are counter variables and first-order variables, respectively, i.e., $(m, \mathbf{n}) \in \mathcal{C}^q$ and $\mathbf{x} \in \mathcal{V}^p$
- $r_1^{\hat{f}}$ and $r_2^{\hat{f}}$ are primal terms, whose variables are among those of the left hand sides of the rules, i.e.,
  $r_1^{\hat{f}} \in \mathcal{P}$, $\mathcal{V}ar(r_1^{\hat{f}}) \subseteq \mathbf{x}$, $\mathcal{CV}ar(r_1^{\hat{f}}) \subseteq \mathbf{n}$
  $r_2^{\hat{f}} \in \mathcal{P}$, $\mathcal{V}ar(r_2^{\hat{f}}) \subseteq \mathbf{x}$, $\mathcal{CV}ar(r_2^{\hat{f}}) \subseteq \{m\} \cup \mathbf{n}$
- all defined symbols in $r_1^{\hat{f}}$ and $r_2^{\hat{f}}$ are smaller than $\hat{f}$ with respect to a given precedence relation on the defined symbols
- A is a set of independent first-order positions of $r_2^{\hat{f}}$ without the root position
- $\boldsymbol{\delta}$ is either the null vector or a k-dimensional unit vector, i.e., all components of $\boldsymbol{\delta}$ are zero except one which may be zero or one.

The first-order positions are those not below a defined symbol. Formally, the set of first-order positions is defined recursively by the following equations.

- $\mathcal{P}os(x) = \{\epsilon\}$ for $x \in \mathcal{V}$,
- $\mathcal{P}os(\hat{f}(\cdots)) = \{\epsilon\}$ for $\hat{f} \in \mathcal{D}$, and
- $\mathcal{P}os(f(t_1, \ldots, t_p)) = \{\epsilon\} \cup \bigcup_{i=1}^{p} \{i.a \mid a \in \mathcal{P}os(t_i)\}$ for $f \in \mathcal{F}_p$.

Two positions are independent if none is a prefix of the other.

Let $\mathcal{R}$ be the set of all rewrite rules associated with the defined symbols. The rewrite relation $\longrightarrow_{\mathcal{R}}$ generated by $\mathcal{R}$ is the smallest relation that contains $\mathcal{R}$, and is closed under congruence and substitution. By $t{\downarrow_{\mathcal{R}}}$ we denote the normal form of t with respect to $\mathcal{R}$. Note that $t{\downarrow_{\mathcal{R}}}$ is a first-order term if t contains no counter variables. The first-order terms represented by a primal term t are defined as $L(t) = \{t\xi{\downarrow_{\mathcal{R}}} \mid \xi{:}\mathcal{C} \longrightarrow \mathbb{N}\}$. Two primal terms s and t are *weakly equivalent*, if $L(s) = L(t)$. They are *(strongly) equivalent*, denoted by $s \doteq t$, if $s\xi{\downarrow_{\mathcal{R}}} = t\xi{\downarrow_{\mathcal{R}}}$ holds for all substitutions $\xi{:}\mathcal{C} \longrightarrow \mathbb{N}$. Obviously, equivalence implies weak equivalence.

Example 2. Let $x \in \mathcal{V}$, $a \in \mathcal{F}_0$, $f \in \mathcal{F}_1$, $m, n \in \mathcal{C}$, $\hat{f} \in \mathcal{D}_{1,0}$, and $\hat{g} \in \mathcal{D}_{1,1}$. Consider the primal terms $s = f(\hat{f}(n))$ and $t = \hat{g}(n{+}1; f(\hat{g}(n; a)))$, where

$$\begin{array}{ll} \hat{f}(0) \to f(a), & \hat{f}(n{+}1) \to f(f(\hat{f}(n))), \\ \hat{g}(0; x) \to x, & \hat{g}(n{+}1; x) \to f(\hat{g}(n; x)). \end{array}$$

The terms s and t are strongly equivalent. Moreover, the schematized sets $L(s)$ and $L(t)$ are equal: $L(s) = L(t) = \{f^n(a) \mid n \geq 2\}$. On the other hand, the terms $f(\hat{f}(m))$ and $f(\hat{f}(n))$ are weakly but not strongly equivalent.

2.3 Unification

A substitution is a mapping $\sigma\colon(\mathcal{V} \cup \mathcal{C}) \longrightarrow (\mathcal{P} \cup \mathcal{L})$, which is well-typed and whose domain is finite, i.e., $\sigma(x) \in \mathcal{P}$ for $x \in \mathcal{V}$, $\sigma(n) \in \mathcal{L}$ for $n \in \mathcal{C}$, and $\mathrm{dom}(\sigma) = \{v \in (\mathcal{V} \cup \mathcal{C}) \mid \sigma(v) \neq v\}$ is finite. As usual, we extend substitutions homomorphically to primal terms and counter expressions. The application of σ to a term t is written as $t\sigma$; the composition of two substitutions σ, τ is written as $\sigma\tau$ with the understanding that $t\sigma\tau = (t\sigma)\tau$ for all terms t. We denote σ by the set $\{v \mapsto v\sigma \mid v \in \mathrm{dom}(\sigma)\}$. Normalization is extended to substitutions in the natural way, i.e., $\sigma{\downarrow_{\mathcal{R}}} = \{v \mapsto v\sigma{\downarrow_{\mathcal{R}}} \mid v \in \mathrm{dom}(\sigma)\}$.

A substitution σ is a unifier of two primal terms s and t iff for all $\xi\colon\mathcal{C} \longrightarrow \mathbb{N}$ the first-order substitution $\sigma\xi{\downarrow_{\mathcal{R}}}$ unifies the first-order terms $s\xi{\downarrow_{\mathcal{R}}}$ and $t\xi{\downarrow_{\mathcal{R}}}$. A set of unifiers Σ is complete iff for every substitution ξ there exists $\sigma \in \Sigma$, such that $\sigma\xi{\downarrow_{\mathcal{R}}}$ is a unifier of $s\xi{\downarrow_{\mathcal{R}}}$ and $t\xi{\downarrow_{\mathcal{R}}}$. Note that σ is a unifier of s and t iff $s\sigma \doteq t\sigma$, i.e., our notion of unifiability corresponds to the standard one in the unification theory. This is not true for completeness: a unifier need not be an instance of any substitution in a given complete set of unifiers.

Unification of primal terms is decidable and finitary, i.e., for any pair of primal terms there exists a finite set of unifiers which is complete. Moreover, complete sets of unifiers can be effectively computed [HG97].

2.4 First-order formulas

In this paper, we use first-order formulas to define the word problem in a concise way and to compare different notions of subsumption. Quantified counter variables are interpreted over the domain of natural numbers, quantified first-order variables over the Herbrand universe with respect to the underlying set of function symbols. Free variables are treated as constants.

Additionally, we use vectors and notations from linear algebra as a compact representation of similar objects. For example, $\mathbf{x} \doteq \mathbf{s}(\mathbf{k})$ stands for a set of equations of the form $x \doteq s(\mathbf{k})$, where x is a variable from $\mathbf{x}$ and $s \in \mathbf{s}$ is a term containing variables $k_1, k_2, \ldots$ from $\mathbf{k}$. Furthermore, $\{\mathbf{n} \mapsto \mathbf{C}\mathbf{k} + \mathbf{c}\}$ represents the substitution replacing each variable in $\mathbf{n}$ by the corresponding row in the vector of linear expressions, which is obtained by multiplying the matrix $\mathbf{C}$ of natural numbers by the vector $\mathbf{k}$ of counter variables and adding the vector $\mathbf{c}$.

Let s and t be primal terms containing the variables $\mathbf{x} = \mathcal{V}ar(s)$, $\mathbf{y} = \mathcal{V}ar(t)$, $\mathbf{m} = \mathcal{C}\mathcal{V}ar(s)$ and $\mathbf{n} = \mathcal{C}\mathcal{V}ar(t)$. A complete set of unifiers for s and t can be considered as a solved form of the equation $s \doteq t$ in the following way. A unifier $\sigma = \{\mathbf{x} \mapsto s'(\mathbf{k}), \mathbf{y} \mapsto t'(\mathbf{k}), \mathbf{m} \mapsto \mathbf{C}\mathbf{k} + \mathbf{c}, \mathbf{n} \mapsto \mathbf{D}\mathbf{k} + \mathbf{d}\}$, where $\mathbf{k}$ are auxiliary counter variables introduced during unification, corresponds to the formula

$$\phi_\sigma(\mathbf{x}, \mathbf{y}, \mathbf{m}, \mathbf{n}) = \exists\mathbf{k}\big(\mathbf{x} \doteq s'(\mathbf{k}) \wedge \mathbf{y} \doteq t'(\mathbf{k}) \wedge \mathbf{m} = \mathbf{C}\mathbf{k} + \mathbf{c} \wedge \mathbf{n} = \mathbf{D}\mathbf{k} + \mathbf{d}\big).$$

Note that unification does not introduce auxiliary first-order variables. However, s' and t' may contain variables from $\mathbf{x}$ and $\mathbf{y}$; in this case these variables do not occur in the domain of the substitution. The formula associated with a complete set of unifiers Σ is the disjunction of the formulas corresponding to the single unifiers: $\phi_\Sigma(\mathbf{x},\mathbf{y},\mathbf{m},\mathbf{n}) = \bigvee_{\sigma\in\Sigma} \phi_\sigma(\mathbf{x},\mathbf{y},\mathbf{m},\mathbf{n})$. Therefore the formulas $s \doteq t$ and $\phi_\Sigma(\mathbf{x},\mathbf{y},\mathbf{m},\mathbf{n})$ are equivalent.

2.5 Miscellaneous notations

If t is a primal term and $A \subseteq \mathcal{P}os(t)$ is a set of independent first-order positions, then $t[\circ]_A$ is called a *context*. If s is a context and t is a context or primal term, then the concatenation of s and t, denoted by $s \cdot t$, is the context or primal term $s\{\circ \mapsto t\}$. Concatenation is associative, hence we drop parentheses where possible. The empty context $\circ$ serves as unit element with respect to concatenation. Exponentiation is defined by $s^0 = \circ$ and $s^{i+1} = s \cdot s^i$.

The depth of a primal term t, denoted by $\mathit{depth}(t)$, is recursively defined as $\mathit{depth}(t) = 0$ for $t \in (\mathcal{V} \cup \mathcal{F}_0)$, and $\mathit{depth}(f(\mathbf{t})) = \mathit{depth}(\hat{f}(\mathbf{l};\mathbf{t})) = 1 + \mathit{depth}(\mathbf{t})$ for $f \in \mathcal{F}_p$ $(p > 0)$ and $\hat{f} \in \mathcal{D}$. The depth of a set or vector of terms $\mathbf{t}$ is defined as $\mathit{depth}(\mathbf{t}) = \max\{\mathit{depth}(t) \mid t \in \mathbf{t}\}$. The depth of the set of rewrite rules $\mathcal{R}$ associated with $\mathcal{D}$ is the depth of the set of all right hand sides: $\mathit{depth}(\mathcal{R}) = \mathit{depth}(\{r_1^{\hat{f}}, r_2^{\hat{f}}[\hat{f}(m,\mathbf{n}+\boldsymbol{\delta};\mathbf{x})]_A \mid \hat{f} \in \mathcal{D}\})$.

3 Redundancy elimination

Recurrent term schematizations are of potential use in all areas concerned with first-order terms, mostly in automated deduction, like term rewriting with equational completion and proofs by consistency, or clausal theorem proving. An ubiquitous problem appearing there is the duplication of objects. Redundancy elimination plays therefore a vital role. In the simplest case, we need to maintain the set property, where no element (term, clause, literal) must occur twice. Another case of redundancy is the presence of two elements, where one is an instance of the other. In the first case we have to solve the *word problem*, i.e., to determine whether two terms s and t represent the same object in the underlying theory. The latter case is usually referred to as the *subsumption problem*.

Example 3. Consider the rewrite system $fgfx \to gfx$. Its completion produces the infinite set of rules $\{fg^nfx \to g^nfx \mid n \in \mathbb{N}\}$. This set can be presented by the primal term (as a rewrite rule) $f\hat{g}(n;fx) \to \hat{g}(n;fx)$, where $\mathcal{R} = \{\hat{g}(0;x) \to gx,\ \hat{g}(k+1;x) \to g(\hat{g}(k;x))\}$. The completion procedure continues to work with this new rewrite rule in the signature extended by the defined symbols and produces the rule $f\hat{g}(n;\hat{g}(n';fx)) \to \hat{g}(n;\hat{g}(n';fx))$. This rule is redundant, but we cannot determine it syntactically. To do so, we need to show that the following formula is valid:

$$\forall n \forall n'\ \exists k \exists x \quad (f\hat{g}(k;fy) \to \hat{g}(k;fy)) \doteq (f\hat{g}(n;\hat{g}(n';fx)) \to \hat{g}(n;\hat{g}(n';fx))).$$

This is just a subsumption test for the newly produced rewrite rule. One way to show the validity is to prove that the word problem

$$\forall n \forall n' (\hat{g}(n; \hat{g}(n'; x)) \doteq \hat{g}(n + n'; x))$$

holds in the equational theory of $\mathcal{R}$ and that $\forall n, n'\ \exists k(n + n' = k)$ holds.

Example 4. Another example for redundancy elimination is the check for instances of the identity axiom. Consider the rewrite system

$$\{\hat{f}(0) \to f(a),\ \hat{f}(n+1) \to f(f(\hat{f}(n))),\ \hat{g}(0; x) \to x,\ \hat{g}(n+1; x) \to f(\hat{g}(n; x))\}.$$

Suppose that we generate during a deduction process the equation $f(\hat{f}(n)) = \hat{g}(n + 1; f(\hat{g}(n; a)))$. To verify that it is an instance of the identity axiom, we need to solve the word problem $\forall n(f(\hat{f}(n)) \doteq \hat{g}(n + 1; f(\hat{g}(n; a))))$.

3.1 Word problem

Definition 5. The **word problem** for two primal terms s and t is the question whether the formula $\forall \mathbf{n}\ (s \doteq t)$ is valid in the equational theory generated by $\mathcal{R}$, where $\mathbf{n} = \mathcal{V}ar(s) \cup \mathcal{V}ar(t)$.

One possibility to solve the word problem is to reduce s and t to unique normal forms, followed by a check whether the latter are syntactically equal. This approach is described for R-strings in [Sal91]. In this paper, we choose a different approach: we transform the word problem to a unification problem and a subsequent problem in Presburger arithmetic. The first method is efficient but works only if we can define a unique normal form, like in the case of iterated terms. In general, there is no obvious way of defining the normal form of a primal term. Our approach does not depend on a specific syntactic representation for schematizations, but requires only the existence of a finitary and terminating unification algorithm. Therefore, our method is applicable to all known recurrent schematizations, i.e., to ρ-terms, I-terms, R-terms, and primal grammars.

We proceed in three steps.

1. *Elimination of first-order variables:* replace all first-order variables by new constants. Observe that the formula $\forall \mathbf{n}(s \doteq t)$ is valid if and only if the corresponding formula $\forall \mathbf{n}(s^* \doteq t^*)$ is valid, where the terms s^*, t^* are obtained from the terms s, t, respectively, by replacing each first-order variable x by a new constant c_x.
2. *Unification:* solve the equation $s^* \doteq t^*$. We solve the equation $s^* \doteq t^*$ by means of unification. Note that a finitary and terminating unification algorithm exists for all four known recurrent schematizations. This means that the output of the unification algorithm is a finite disjunction of formulas $\exists \mathbf{k}(\mathbf{n} = \mathbf{N}_i \mathbf{k} + \mathbf{d}_i)$, where $\mathbf{N}_i$ and $\mathbf{d}_i$ is a matrix and a vector of non-negative integers, respectively, and $\mathbf{k}$ are new counter variables introduced during unification. The resulting formula $\phi(\mathbf{n}) = \exists \mathbf{k} \bigvee_i (\mathbf{n} = \mathbf{N}_i \mathbf{k} + \mathbf{d}_i)$ contains only counter variables, since there are no first-order variables in s^* and t^*.

3. *Validity check:* check whether the formula $\forall \mathbf{n}\ \phi(\mathbf{n})$ is valid. The formula $\phi(\mathbf{n})$ represents a complete set of unifiers, one per disjunct, of the problem $s^* \doteq t^*$. To show that the universally quantified formula $\forall \mathbf{n}(s^* \doteq t^*)$ is valid, we need to prove that the unifiers from $\phi(\mathbf{n})$ cover the whole Cartesian product $\mathbb{N}^{|\mathbf{n}|}$. By correctness of the applied unification algorithm, the formulas $\forall \mathbf{n}(s^* \doteq t^*)$ and $\forall \mathbf{n}\ \phi(\mathbf{n})$ are equivalent. The latter expression is a Π_2-formula of Presburger arithmetic and can be solved by usual methods [Coo72]. For complexity issues see Section 3.3.

3.2 Subsumption problem

In the first-order case, a term s subsumes a term t if there exists a substitution σ, such that $s\sigma = t$. In the free algebra, this is equivalent to $\exists \mathbf{x}(s = t)$, where $\mathbf{x} = \mathcal{V}ar(s)$. An alternative definition is that the formula $\forall \mathbf{y} \exists \mathbf{x}(s = t)$ is valid, where $\mathbf{x} = \mathcal{V}ar(s)$ and $\mathbf{y} = \mathcal{V}ar(t)$. These two definitions are equivalent, except for singular signatures, since in the empty theory (without axioms) validity in the equational theory is equivalent to validity in the inductive theory.

For schematizations, there are several possibilities to define subsumption. Let s and t be two primal terms from a schematization G, where $\mathbf{m} = \mathcal{CV}ar(s)$, $\mathbf{n} = \mathcal{CV}ar(t)$, $\mathbf{x} = \mathcal{V}ar(s)$, and $\mathbf{y} = \mathcal{V}ar(t)$. Recall that we check the validity of formulas in the equational theory of $\mathcal{R}$, i.e., the free algebra generated by $\mathcal{R}$. The possibilities to define that s subsumes t are:

1. The formula $\exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ is valid.
2. The formula $\forall \mathbf{n} \forall \mathbf{y} \exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ is valid.
3. The formula $\forall \mathbf{n} \exists \mathbf{m}(s \doteq t)$ is valid.
4. The formula $\forall \mathbf{n} \exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ is valid.

The first two approaches are straightforward extensions of the first-order concept. The second approach does not meet a natural requirement for subsumption, namely independence of the underlying signature. Subsumption should be a local test on two terms independent of other elements. There exist two terms s, t, such that s subsumes t (according to the second definition) over a signature $\mathcal{F}$, but not over an extended signature $\mathcal{F}' \supset \mathcal{F}$ [AHL97, Example 14]. The same terms also show that the first two subsumption concepts are not equivalent, since there is no substitution σ, such that $s\sigma \doteq t$, as required by the first concept.

The problems with the second concept originate from quantification over first-order variables. One possibility to avoid them is to quantify only the counter variables, as in the third approach. This concept is not satisfactory either, since it does not capture usual first-order subsumption. When we extend the third concept with usual equational first-order subsumption, we get the fourth concept.

Hence, we have two suitable concepts for subsumption: the first and the last one. Intuitively, the first concept expresses that there is a uniform mapping σ, relating the term s and t in the equational theory of the schematization. In particular, for the counter variable vectors $\mathbf{m}$ and $\mathbf{n}$, this means that $\mathbf{m}$ is a linear expression of $\mathbf{n}$. In contrast, the fourth concept requires this uniformity only on the first-order level; the vectors $\mathbf{m}$ and $\mathbf{n}$ need not be related by a linear

function. Clearly, the first concept implies the fourth concept. The converse is not true, as the following example shows.

Example 6. Primal grammars can encode arbitrary linear expressions of the form $c_0 + c_1 k_1 + \cdots + c_n k_n$. A monomial ck can be represented by $\hat{g}_c(k; a)$, where the underlying rewrite system is

$$\hat{g}_c(0; x) \to x, \quad \hat{g}_c(k+1; x) \to \underbrace{f(\cdots f}_{c \text{ times}}(\hat{g}_c(k; x))).$$

Addition of monomials is encoded by nesting of defined symbols. Hence, $l_1 = 2m_1 + 3m_2$ is represented by $s = \hat{g}_2(m_1; \hat{g}_3(m_2; a))$ and $l_2 = n_1 + 2$ is encoded as $t = \hat{g}_1(n_1; f(f(a)))$.

We show that s subsumes t according to the last concept but not according to the first one. Both problems reduce to purely Diophantine problems upon l_1 and l_2, following the previously mentioned encoding.

According to the last concept, s subsumes t iff $\forall \mathbf{n} \exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$. This is equivalent to $\forall n_1 \exists m_1, m_2(2m_1 + 3m_2 = n_1 + 2)$, since the problem contains no first-order variables. This formula is valid since $n_1 + 2$ covers all natural numbers greater than 1, and each number except 1 can be written in the form $2m_1 + 3m_2$. Hence, s subsumes t.

According to the first concept, s subsumes t iff $\exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ holds. This is equivalent to $\exists m_1 \exists m_2(2m_1 + 3m_2 = n_1 + 2)$. Now suppose that there is a substitution $\sigma = \{m_1 \mapsto q_1 n_1 + d_1,\ m_2 \mapsto q_2 n_1 + d_2\}$, where q_1 and q_2 are non-negative coefficients. By applying the substitution and regrouping, we obtain the equations $2q_1 + 3q_2 = 1$ and $2d_1 + 3d_2 = 2$. The first equation has no solution in non-negative integers. Hence, there is no such substitution σ and the formula $\exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ is not valid.[1]

The last subsumption concept encompasses the first one. Moreover, the last concept corresponds to the natural view that schematizations are just a finite representation of infinite sets of first-order terms: s subsumes t if every term represented by t is subsumed by a term represented by s. Therefore we adopt the last concept of subsumption.

Definition 7. Let s and t be primal terms, where $\mathbf{m} = \mathcal{CV}ar(s)$, $\mathbf{n} = \mathcal{CV}ar(t)$, and $\mathbf{x} = \mathcal{V}ar(s)$. The term s **subsumes** t if the formula $\forall \mathbf{n} \exists \mathbf{m} \exists \mathbf{x}(s \doteq t)$ is valid. A set S subsumes a set T if for each term $t' \in T$ there exists a term $s' \in S$, such that s' subsumes t'.

Lemma 8. *A primal term s subsumes a primal term t if and only if the set $L(s)$ subsumes the set $L(t)$.*

Similar to the word problem, we want to reduce subsumption to unification. In this way, the algorithm becomes independent of the chosen schematization

[1] We thank Eric Domenjoud for providing this example.

formalism. We proceed in four steps: we replace certain first-order variables by new constants, apply the unification algorithm, simplify the resulting formula, and check its validity in Presburger arithmetic.

1. *Elimination of first-order variables in t:* replace all first-order variables in t by new constants, producing the term t^*. The formula $\forall\mathbf{n}\exists\mathbf{m}\exists\mathbf{x}(s \doteq t)$ is valid iff $\forall\mathbf{n}\exists\mathbf{m}\exists\mathbf{x}(s \doteq t^*)$ holds by the way how we interpret free variables.
2. *Unification:* solve the equation $s = t^*$ by means of a unification algorithm. Its output can be written as the finite formula

$$\phi(\mathbf{m},\mathbf{n},\mathbf{x}) = \exists\mathbf{k}\bigvee_i(\mathbf{x} = \mathbf{u}_i(\mathbf{k}) \wedge \mathbf{m} = \mathbf{M}_i\mathbf{k} + \mathbf{c}_i \wedge \mathbf{n} = \mathbf{N}_i\mathbf{k} + \mathbf{d}_i),$$

   where $\mathbf{k}$ are the new counter variables introduced during unification, $\mathbf{M}_i$, $\mathbf{N}_i$ are matrices of non-negative integers, and $\mathbf{c}_i$, $\mathbf{d}_i$ are vectors of non-negative integers, for each i.
3. *Simplification:* remove the equations $\mathbf{x} = \mathbf{u}_i(\mathbf{k})$ and $\mathbf{m} = \mathbf{M}_i\mathbf{k} + \mathbf{c}_i$ from the formula $\phi(\mathbf{m},\mathbf{n},\mathbf{x})$, producing $\phi'(\mathbf{n})$. Note that $\exists\mathbf{m}\exists\mathbf{x}\ \phi(\mathbf{m},\mathbf{n},\mathbf{x})$ is equivalent to $\phi'(\mathbf{n})$, since the variables $\mathbf{m}$ and $\mathbf{x}$ are existentially quantified and appear only once and separated on the left-hand side of equations.
4. *Validity check:* check if $\forall\mathbf{n}\ \phi'(\mathbf{n})$ is valid. The result $\forall\mathbf{n}\exists\mathbf{k}\bigvee_i(\mathbf{n} = \mathbf{N}_i\mathbf{k} + \mathbf{d}_i)$ belongs to the Π_2-fragment of Presburger arithmetic.

3.3 Complexity issues

Both the word problem and the subsumption problem reduce in the last step to a Π_2-formula in Presburger arithmetic. While the complexity of full Presburger arithmetic is at least doubly exponential and Cooper presents in [Coo72] an algorithm of triple exponential complexity, the Π_2-fragment is only coNP-complete, as it was proved by Grädel [Grä88] and Schöning [Sch97]. Our formulas are quite simple and do not cover the whole Π_2-fragment: they are of the form $\forall\mathbf{n}\exists\mathbf{k}\bigvee_i(\mathbf{n} = \mathbf{N}_i\mathbf{k} + \mathbf{d}_i)$, i.e., the formula is in disjunctive normal form and the variables $\mathbf{n}$ appear only once separated on the left-hand side. Therefore we can ask whether our special problems are still coNP-complete. The lower bound reductions used by Grädel and Schöning require more complex formulas. However, following an idea in [Sch97], due to Grädel, we can prove the coNP-hardness of our problems by a reduction from SIMULTANEOUS INCONGRUENCES [GJ79]. This NP-complete problem is defined as follows.

SIMULTANEOUS INCONGRUENCES
Instance: Collection $\{(a_1,b_1),\ldots,(a_p,b_p)\}$ of ordered pairs of positive integers, with $a_i \leq b_i$, for $1 \leq i \leq p$.
Question: Is there an integer n such that, for $1 \leq i \leq p$, $n \not\equiv a_i \pmod{b_i}$?

We use the dual problem to show coNP-hardness. Encoding $n \equiv a_i \pmod{b_i}$ as $\exists k(n = b_ik + a_i)$, we obtain the disjunction $\exists k\bigvee_{i=1}^{p}(n = b_ik + a_i)$. The final formula is $\forall n\exists k\bigvee_i(n = b_ik + a_i)$.

Note that in both cases only the problem solved in the last step is coNP-complete. The overall complexity of our algorithms is determined by the complexity of unification. In particular, the cardinality of a minimal complete set of

unifiers can be at least exponential [Sal91]; and we have to compute all solutions to obtain the formula. Hence, the formula in the last step can be exponentially longer than the input of the original problem.

4 Complement problem

If t is a first-order term, its Herbrand universe is $\mathcal{H}(t) = \{t\sigma \mid \sigma\colon \mathcal{X} \longrightarrow \mathcal{T}(\mathcal{F})\}$, the set of the ground instances of t with respect to the underlying signature $\mathcal{F}$. Similarly, if T is a set of first-order terms, its Herbrand universe $\mathcal{H}(T)$ is the union of the Herbrand universes $\mathcal{H}(t)$ for each $t \in T$. For a primal term t, its Herbrand universe is the set $\mathcal{H}(L(t))$, i.e., the Herbrand universe of the schematized set. Finally, the Herbrand universe of a set of primal terms T is obtained as the union of the Herbrand universes $\mathcal{H}(t)$ for each $t \in T$.

Given a set of first-order or primal terms T, its *complement* is the set $T^c = \mathcal{T}(\mathcal{F}) \setminus \mathcal{H}(T)$. A class $\mathbb{C}$ is a collection of sets of terms satisfying a common property. For a given class $\mathbb{C}$, the *complement problem* is the question whether for each finite set of terms $T \in \mathbb{C}$ there exists a finite set of terms $T' \in \mathbb{C}$, such that $\mathcal{H}(T') = T^c$ holds. The set T' is called a finite complement representation.

For first-order terms, Lassez and Marriott proved that finite sets of linear terms always have a finite complement representation [LM87]. On the other hand, they showed that this is not true for arbitrary finite sets of first-order terms. Since schematizations were introduced to increase the expressive power of first-order terms, we might expect to be able to represent the complements of non-linear terms by a finite set of primal terms. However, as we show in the sequel, already the very simple non-linear term $f(x, x)$ has no finite complement representation by primal terms.

The potential of primal terms resides in the possibility to generate arbitrarily deep terms by iterating contexts. The expressive power of iteration is limited by the fact that the number of contexts must be finite. The maximal number of consecutive iterations during a reduction of a primal term is measured by the iteration depth. Each iteration terminates with the application of the base rule $\hat{f}(0, \ldots) \to r_1^{\hat{f}}$ for some defined symbol $\hat{f}$. Therefore we can determine the iteration depth by counting the occasions when a variable gets decremented to 0. The iteration depth of a primal term is then the maximum over all reductions. Inspection of the rewrite system $\mathcal{R}$ reveals that there is a correspondence between the application of base rules and the number of counter positions present in the primal term: each iteration consumes a counter position.

Definition 9. The **iteration depth** of a primal term is the function τ defined recursively as follows:

- $\tau(x) = \tau(a) = 0$ for a first-order variable x and a constant a,
- $\tau(f(t_1, \ldots, t_n)) = \max\{\tau(t_i) \mid i = 1, \ldots, n\}$ for an n-ary function symbol f,
- $\tau(\hat{f}(\mathbf{c}; t_1, \ldots, t_n)) = |\mathbf{c}| + \max\{\tau(t_i) \mid i = 1, \ldots, n\}$ for a defined symbol $\hat{f}$.

The iteration depth naturally extends to a set of primal terms T, defined by $\tau(T) = \max\{\tau(t) \mid t \in T\}$.

This definition emphasizes the static aspect by looking at the primal term only. The operational aspect, namely counting the occasions when a variable is decremented to 0, is expressed by the equalities $\tau(\hat{f}(0,\ldots)\theta) = 1 + \tau(r_1^{\hat{f}}\theta)$ and $\tau(\hat{f}(n+1,\ldots)\theta) = \tau(r_2^{\hat{f}}\theta)$ for each defined symbol $\hat{f}$ and substitution θ. Note that $\tau(t) \leq |\mathcal{D}| \times \mathit{depth}(t)$.

Iteration of contexts consumes resources of the primal term. On one hand, a single iteration can produce an arbitrarily deep term. On the other hand, there are ground first-order terms that require a certain iteration depth. We use two different contexts, $f(\circ, a)$ and $f(a, \circ)$, to force a consumption of resources. Consider the ground term $s = f(\circ, a)^m \cdot a$. If the value of m is sufficiently large, then a primal term t representing s must contain a defined symbol through which we iterate the context $f(\circ, a)$, and the iteration depth of t must be at least 1. If we simply concatenate two blocks of the same context, like in $f(\circ, a)^m \cdot f(\circ, a)^m \cdot a$, we do not necessarily need to increase the iteration depth of the primal term. However, if we insert the context $f(a, \circ)$ between the two blocks, producing the term $s = f(\circ, a)^m \cdot f(a, \circ) \cdot f(\circ, a)^m \cdot a$, we force a primal term t representing s to have an iteration depth of at least 2. Repeating the step, this idea leads to an upper bound on the number of context blocks $f(\circ, a)^m \cdot f(a, \circ)$ that can be represented by a given primal term t.

Lemma 10. *Let t be a primal term without first-order variables and let $s = w \cdot (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$ be a ground first-order term, where w is a proper subcontext of $f(\circ, a)^m \cdot f(a, \circ)$. If $s \in L(t)$ and $m > \tau(t) \times \mathit{depth}(\mathcal{R}) + \mathit{depth}(t)$ then $n \leq \tau(t)$.*

Proof. Let $B(t) = \tau(t) \times \mathit{depth}(\mathcal{R}) + \mathit{depth}(t)$ be the lower bound on the value of m. Note that the context w is either $f(\circ, a)^i \cdot f(a, \circ)$ for some $i < m$ or the empty context. We perform the proof by induction on the tuple $(s, \tau(t))$, where the first component is ordered by subterm ordering and the second by the usual ordering on natural numbers. Note that $\tau(t) = 0$ for all first-order terms t.

The base case is presented by $s = a$ and $n = 0$. The inequality $0 \leq \tau(t)$ holds for each term t. For the induction step, we perform a case analysis on the structure of t. The primal term t can begin with different prefixes of the term s.

Case 1: $t = f(\circ, a)^i \cdot f(a, t')$ for a term t'. Then the term t' must represent $s' = (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$, where $s = w \cdot s'$, i.e., s' is a proper subterm of s. By induction hypothesis, we have that $n \leq \tau(t')$. Since the iteration depths of t and t' are equal ($f(\circ, a)^i$ is a first-order context), we obtain $n \leq \tau(t)$.

Case 2: $t = f(\circ, a)^j \cdot \hat{f}(c, \ldots)$ for some $j \leq i$ and a defined symbol $\hat{f}$. To represent the term s, the counter expression c must be instantiated. Let ξ be a counter variable substitution, such that $t\xi{\downarrow_{\mathcal{R}}} = s$. There are two subcases to analyze, one for $c\xi = 0$, the other for positive values of $c\xi$.

Case 2.1: $c\xi = 0$. Then there is a reduction $t\xi \longrightarrow_{\mathcal{R}} t'$, where $t' = f(\circ, a)^i \cdot r_1^{\hat{f}}\theta$ for a substitution θ. Both terms t and t' represent the term s, but the inequality $\tau(t') \leq \tau(t) + 1$ holds. Compared to t, the term t' grew at least by the term $r_1^{\hat{f}}$,

but the condition $m > B(t')$ still holds, since $depth(t') \leq depth(\mathcal{R}) + depth(t)$ follows from the rewrite step. We have that $B(t') \leq B(t) < m$, therefore we can apply the induction hypothesis since the iteration depth decreases: $\tau(t) > \tau(t')$. From the induction hypothesis follows that $n \leq \tau(t')$. Hence, $n \leq \tau(t)$ holds.

Case 2.2: $c\xi > 0$. We must perform a case analysis whether the context $f(a, \circ)$ is present in $r_2^{\hat{f}}$ or not.

Case 2.2.1: The context $f(a, \circ)$ is absent from $r_2^{\hat{f}}$. Hence, the context $r_2^{\hat{f}}$ must be of the form $f(\circ, a)^k$ for some k and $t\xi \xrightarrow{+}_{\mathcal{R}} f(\circ, a)^{j+k(c\xi)} \cdot t'$, where t' is an instance of the term $r_1^{\hat{f}}$. The primal term t' represents either the first-order term

$$s' = f(\circ, a)^{i-j-k(c\xi)} \cdot f(a, \circ) \cdot (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$$

or the first-order term

$$s' = f(\circ, a)^{m-j-k(c\xi)} \cdot f(a, \circ) \cdot (f(\circ, a)^m \cdot f(a, \circ))^{n-1} \cdot a.$$

In both cases, the term s' is a subterm of s and $B(t') \leq B(t) < m$ holds. Hence, by induction hypothesis, $n - 1 \leq \tau(t')$ holds. Moreover, the iteration depth decreases ($\tau(t) > \tau(t')$ holds), therefore we have that $n \leq \tau(t)$.

Case 2.2.2: The context $f(a, \circ)$ is present in $r_2^{\hat{f}}$. Hence, the context $r_2^{\hat{f}}$ must be of the form $f(\circ, a)^k \cdot f(a, \circ) \cdot f(\circ, a)^l$ for some k and l, where the inequalities $k + l < depth(\mathcal{R}) < B(t) < m$ hold. Therefore $c\xi$ must be equal to 1, since m is too large, and there exists the reduction $t\xi \xrightarrow{+}_{\mathcal{R}} f(\circ, a)^{j+k} \cdot f(a, \circ) \cdot f(\circ, a)^l \cdot t'$. The primal term t' represents the first-order term

$$s' = f(\circ, a)^{m-l} \cdot f(a, \circ) \cdot (f(\circ, a)^m \cdot f(a, \circ))^{n-1} \cdot a.$$

Note that $j + k = i < m$ holds. The term s' is a subterm of s and the inequalities $B(t') \leq B(t) < m$ hold. Hence, by induction hypothesis, $n - 1 \leq \tau(t')$ holds. The iteration depth decreases ($\tau(t) > \tau(t')$ holds), therefore $n \leq \tau(t)$ holds. □

The lemma indicates that if we choose the value of n in the term $s = (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$ larger than the iteration depth $\tau(t)$ of the primal term t, then we cannot represent s by t using iteration only. Therefore, the term t must contain variables.

Corollary 11. *If $s = (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$ is an instance of a primal term t with $\tau(t) < n$ and $m > \tau(t) \times depth(\mathcal{R}) + depth(t)$, then t must end with a variable. More precisely, for each counter substitution ξ, such that s is an instance of $t\xi{\downarrow_{\mathcal{R}}}$, the term $t\xi{\downarrow_{\mathcal{R}}}$ is of the form $(f(\circ, *)^m \cdot f(*, \circ))^i \cdot f(\circ, *)^j \cdot x$, where the signs $*$ are either variables different from x or the constant a.*

Proof. If t ends with a variable x and represents s, then there exist a counter substitution $\xi : \mathcal{C} \longrightarrow \mathbb{N}$ and a first-order substitution σ, such that $t\xi{\downarrow_{\mathcal{R}}}\sigma = s$.

The substitution σ is of the form $\{x \mapsto s'\} \cup \{\mathbf{y} \mapsto a\}$, where $\mathcal{V}ar(t) = \{x\} \cup \mathbf{y}$. Note that $t\xi{\downarrow_{\mathcal{R}}}\sigma = t\sigma\xi{\downarrow_{\mathcal{R}}}$ holds.

Now suppose that t does not end with a variable. Then $t\sigma$ is a primal term without first-order variables and is of the same size as t, i.e., $\tau(t\sigma) = \tau(t)$ and $depth(t\sigma) = depth(t)$. The instance $t\sigma$ represents s, therefore by Lemma 10 we have $n \leq \tau(t\sigma)$. This is a contradiction with the condition $\tau(t\sigma) = \tau(t) < n$. □

The Herbrand universes of a set of terms T and of a representation T' of its complement must be disjoint. This leads to the following result.

Lemma 12. *Let T be a set of first-order terms and T' a representation of its complement. Then for all $t \in T$ and $t' \in T'$, the terms t and t' are not unifiable.*

Proof. Suppose that t and t' are unifiable with the unifier σ. Hence, there exists a ground term t^* and a ground substitution ρ, such that $t\sigma\rho = t^* = t'\sigma\rho$ holds. The ground term t^* belongs to both Herbrand universes $\mathcal{H}(t)$ and $\mathcal{H}(t')$, therefore the term t' cannot be in the complement representation T'. Contradiction. □

We have now assembled the necessary tools to show that primal terms cannot finitely represent the complement of first-order terms. The proof is done by contradiction. We try to find a finite representation for the complement of the first-order term $f(x, x)$. The underlying idea is to choose a ground term $s = f(s_1, s_2)$ from the complement, such that both s_1 and s_2 are too complex to be produced by iteration alone, and s_2 is twice as deep as s_1. Therefore a term representing s must be of the form $f(u, v)$, where both u and v end with variables y and z, respectively. If $y \neq z$ then the terms $f(u, v)$ and $f(x, x)$ are unifiable, what contradicts Lemma 12. If $y = z$, then there is no substitution σ, such that $u\sigma{\downarrow_{\mathcal{R}}} = s_1$ and $v\sigma{\downarrow_{\mathcal{R}}} = s_2$ hold.

Theorem 13. *The complement of a finite set of first-order terms cannot be represented in general by a finite set of primal terms.*

Proof. We show that the term $f(x, x)$ has no finite complement representation even if we use schematizations. Assume that the finite set of primal terms T represents the complement of $f(x, x)$. The set T must contain a primal term t representing the ground term

$$s = f((f(\circ, a)^m \cdot f(a, \circ))^n \cdot a, (f(\circ, a)^m \cdot f(a, \circ))^{2n} \cdot a)$$

where m and n are parameters depending on the set T and the the used schematization. Let $n > \tau(T)$ and $m > \tau(T) \times depth(\mathcal{R}) + depth(T)$. There must be a substitution σ, such that $t\sigma{\downarrow_{\mathcal{R}}} = s$ holds. We analyze the possibilities for t.

Without loss of generality, we assume that t is a variable, or a constant, or begins with a functional constructor symbol. If t begins with a defined symbol, i.e., $t = \hat{f}(n, \ldots)$ for a defined symbol $\hat{f}$, then either $n = 0$ or $n = n' + 1$. Hence, after one reduction step by $\mathcal{R}$ we get $t \longrightarrow_{\mathcal{R}} t'$ where $t' = r_1^{\hat{f}}\theta$ or $t' = r_2^{\hat{f}}\theta$ for a substitution θ. The context $r_2^{\hat{f}}$ must start with a functional constructor symbol.

The rewrite step does not increase the iteration depth. For $t' = r_1^{\hat{f}}\theta$, we have that $\tau(t) > \tau(t')$, therefore we can apply the induction hypothesis.

We perform a case analysis for t. The term t starts with a constant, or a variable, or a functional symbol.

Case 1: $t = a$ for a constant a. The constant a clearly cannot represent the term s, since the root symbol of s is the functional symbol f.

Case 2: $t = y$ for a variable y. Then t is unifiable with $f(x, x)$, hence it cannot be a term from a complement representation T following Lemma 12. Contradiction.

Case 3: $t = f(u, v)$ for some terms u and v. Clearly, from $n > \tau(T)$ follows that $n > \tau(u)$ and $n > \tau(v)$. By Corollary 11, both terms u and v must end with a first-order variable.

There must be a counter substitution ξ and a first-order substitution σ, such that $t\xi{\downarrow_{\mathcal{R}}}\sigma = s$. Let $\bar{u} = n\xi{\downarrow_{\mathcal{R}}}$ and $\bar{v} = v\xi{\downarrow_{\mathcal{R}}}$. From the structure of the term s and the properties of the first-order substitutions follows that

$$\bar{u} = (f(\circ, *)^m \cdot f(*, \circ))^{n'} \cdot f(\circ, *)^{m'} \cdot y, \quad \bar{v} = (f(\circ, *)^m \cdot f(*, \circ))^{n''} \cdot f(*, \circ)^{m''} \cdot z$$

where $*$ stands for either a variable (different from y and z) or for the constant a. Both terms $\bar{u}$ and $\bar{v}$ must end by a variable since both iteration depths $\tau(u)$ and $\tau(v)$ a smaller that n. We perform a case analysis on the variables y and z.

Case 3.1: the variables are different: $y \neq z$. Then we can unify $f(\bar{u}, \bar{v})$ with $f(x, x)$ and therefore t cannot be in T following Lemma 12. Contradiction.

Case 3.2: the variables are equal: $y = z$. Then there must be a first-order substitution σ, such that $\bar{u}\sigma = (f(\circ, a)^m \cdot f(a, \circ))^n \cdot a$ holds. From the structure of the term $\bar{u}$ follows that the variable y must be instantiated by σ to the ground term $(f(\circ, a)^{m-m'} \cdot f(a, \circ)) \cdot (f(\circ, a)^m \cdot f(a, \circ))^{n-n'-1} \cdot a$. Now, the instance $\bar{v}\sigma$ is equal to the ground term

$$(f(\circ, a)^m \cdot f(a, \circ))^{n''} \cdot f(\circ, a)^{m''} \cdot f(\circ, a)^{m-m'} \cdot f(a, \circ) \cdot (f(\circ, a)^m f(a, \circ))^{n-n'-1} \cdot a.$$

The context $f(\circ, a)^{m''} \cdot f(\circ, a)^{m-m'}$ must be equal to the context $f(\circ, a)^m$, therefore we get $m' = m''$. Hence, the instance $\bar{v}\sigma$ must be equal to the term $(f(\circ, a)^m \cdot f(a, \circ))^{n''+n-n'} \cdot a$. Now it is clear that $\bar{v}\sigma$ cannot be equal to the required term $(f(\circ, a)^m \cdot f(a, \circ))^{2n}$, since $n'' - n' \neq n$ holds because of the inequalities $n > \tau(u)$, $n > \tau(v)$, $n' \leq \tau(u)$, and $n'' \leq \tau(v)$. Contradiction. □

5 Conclusion

We presented general algorithms for solving the word and the subsumption problem for primal terms that also work for ρ-terms, I-terms, and R-terms. The algorithms require a finitary unification algorithm for the schematization formalisms, as well as a solver for the Π_2-fragment of Presburger arithmetic. Still, there are some problems left, especially concerning efficiency. For the word problem, it would be interesting to have an algorithm that computes first a suitable normal

form of primal terms, followed by a syntactic comparison. Algebraically, this amounts to axiomatizing the theory of primal terms.

We also showed that equations and primal terms are not sufficient for describing in general the complement of first-order terms. This result trivially extends to recurrent term schematizations, since first-order terms are just a special case. On the other hand, the complement problem is easily solvable if we extend the language by negation and quantification. Then the complement can be expressed by a formula in the first-order theory of term schematizations. In this context, we are interested in deciding the validity of formulas and in obtaining solved forms, e.g., by quantifier elimination. Peltier showed in [Pel97] that the first-order theory of R-terms is decidable by quantifier elimination. The decidability of the first-order theory of primal terms is still an open problem.

References

[AHL97] A. Amaniss, M. Hermann, and D. Lugiez. Set operations for recurrent term schematizations. In M. Bidoit and M. Dauchet, editors, *Proc. 7th Int. Joint Conf. on Theory and Practice of Software Development (TAPSOFT'97), Lille (France)*, LNCS 1214, pages 333–344. Springer, 1997.

[CH95] H. Chen and J. Hsiang. Recurrence domains: Their unification and application to logic programming. *Information and Computation*, 122:45–69, 1995.

[Com95] H. Comon. On unification of terms with integer exponents. *Mathematical Systems Theory*, 28(1):67–88, 1995.

[Coo72] D.C. Cooper. Theorem proving in arithmetic without multiplication. In B. Meltzer and D. Mitchie, editors, *Machine Intelligence*, volume 7, pages 91–99. Edinburgh University Press, Edinburgh, UK, 1972.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness.* W.H. Freeman and Co, 1979.

[Grä88] E. Grädel. Subclasses of Preburger arithmetic and the polynomial-time hierarchy. *Theoretical Computer Science*, 56(3):289–301, 1988.

[HG97] M. Hermann and R. Galbavý. Unification of infinite sets of terms schematized by primal grammars. *Theoretical Computer Science*, 176(1-2):111–158, 1997.

[LM87] J.-L. Lassez and K. Marriott. Explicit representation of terms defined by counter examples. *J. Automated Reasoning*, 3(3):301–317, 1987.

[Pel97] N. Peltier. Increasing model building capabilities by constraint solving on terms with integer exponents. *J. Symbolic Computation*, 24(1):59–101, 1997.

[Sal91] G. Salzer. Deductive generalization and meta-reasoning, or how to formalize Genesis. In *Österreichische Tagung für Künstliche Intelligenz, Informatik-Fachberichte* 287, pages 103–115. Springer, 1991.

[Sal92] G. Salzer. The unification of infinite sets of terms and its applications. In A. Voronkov, editor, *Proc. 3rd Int. Conf. on Logic Programming and Automated Reasoning (LPAR'92), St. Petersburg (Russia)*, LNCS (LNAI) 624, pages 409–420. Springer, 1992.

[Sal94] G. Salzer. Primal grammars and unification modulo a binary clause. In A. Bundy, editor, *Proc. 12th Int. Conf. on Automated Deduction (CADE'94), Nancy (France)*, LNCS (LNAI) 814, pages 282–295. Springer, 1994.

[Sch97] U. Schöning. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theory of Computing Systems*, 30(4):423–428, 1997.