An Efficient and Precise Finite-Tree Analysis for Constraint Logic-Based Languages[1]

Roberto Bagnara and Enea Zaffanella
Department of Mathematics
University of Parma, Italy
E-mail: bagnara@cs.unipr.it, zaffanella@cs.unipr.it

and

Roberta Gori
Department of Computer Science
University of Pisa, Italy
E-mail: gori@di.unipi.it

and

Patricia M. Hill
School of Computing
University of Leeds, U.K.
E-mail: hill@comp.leeds.ac.uk

Version: April 10, 2002

Logic languages based on the theory of rational, possibly infinite, trees have much appeal in that rational trees allow for faster unification (due to the safe omission of the occurs-check) and increased expressivity (cyclic terms can provide very efficient representations of grammars and other useful objects). Unfortunately, the use of infinite rational trees has problems. For instance, many of the built-in and library predicates are ill-defined for such trees and need to be supplemented by run-time checks whose cost may be significant. Moreover, some widely-used program analysis and manipulation techniques are correct only for those parts of programs working over finite trees. It is thus important to obtain, automatically, a knowledge of the program variables (the *finite variables*) that, at the program points of interest, will always be bound to finite terms. For these reasons, we propose here a new data-flow analysis that captures such information. We present a parametric domain where a simple component for recording finite variables is coupled, in the style of the *open product* construction of Cortesi et al., with a generic domain (the parameter of the construction) providing sharing information. The sharing domain is abstractly specified so as to guarantee the correctness of the combined domain and the generality of the approach. This finite-tree analysis domain is further enhanced by coupling it with a domain of Boolean functions, called *finite-tree dependencies*, that precisely captures how the finiteness of some variables influences the finiteness of other variables. We also summarize our experimental results showing how finite-tree analysis, enhanced with finite-tree dependencies, is a practical means of obtaining precise finiteness information.

[1]This work has been partly supported by MURST projects "Certificazione automatica di programmi mediante interpretazione astratta" and "Interpretazione astratta, sistemi di tipo e analisi control-flow". Some of this work was done during visits of the second author to Leeds, funded by EPSRC under grant M05645.

1. INTRODUCTION

The intended computation domain of most logic-based languages[2] includes the algebra (or structure) of *finite trees*. Other (constraint) logic-based languages, such as Prolog II and its successors [18, 20], SICStus Prolog [63], and Oz [59], refer to a computation domain of *rational trees*.[3] A rational tree is a possibly infinite tree with a finite number of distinct subtrees and where each node has a finite number of immediate descendants. These properties ensure that rational trees, even though infinite in the sense that they admit paths of infinite length, can be finitely represented. One possible representation makes use of connected, rooted, directed and possibly cyclic graphs where nodes are labeled with variable and function symbols as is the case of finite trees.

Applications of rational trees in logic programming include graphics [32], parser generation and grammar manipulation [18, 35], and computing with finite-state automata [18]. Other applications are described in [34] and [37]. Going from Prolog to CLP, [53] combines constraints on rational trees and record structures, while the logic-based language *Oz* allows constraints over rational and feature trees [59]. The expressive power of rational trees is put to use, for instance, in several areas of natural language processing. Rational trees are used in implementations of the HPSG formalism (Head-driven Phrase Structure Grammar) [55], in the ALE system (Attribute Logic Engine) [12], and in the ProFIT system (Prolog with Features, Inheritance and Templates) [33].

While rational trees allow for increased expressivity, they also come equipped with a surprising number of problems. As we will see, some of these problems are so serious that rational trees must be used in a very controlled way, disallowing them in any context where they are "dangerous". This, in turn, causes a secondary problem: in order to disallow rational trees in selected contexts one must first detect them, an operation that may be expensive.

The first thing to be aware of is that almost any semantics-based program manipulation technique developed in the field of logic programming —whether it be an analysis, a transformation, or an optimization— assumes a computation domain of *finite trees*. Some of these techniques might work with the rational trees but their correctness has only been proved in the case of finite trees. Others are clearly inapplicable. Let us consider a very simple Prolog program:

```
list([]).
list([_|T]) :- list(T).
```

Most automatic and semi-automatic tools for proving program termination[4] and for complexity analysis[5] agree on the fact that `list/1` will terminate when invoked with a ground argument. Consider now the query

```
?- X = [a|X], list(X).
```

and note that, after the execution of the first rational unification, the variable `X` will be bound to a rational term containing no variables, i.e., the predicate `list/1` will be invoked with `X` ground. However, if such a query is given to, say, SICStus

[2]That is, ordinary logic languages, (concurrent) constraint logic languages, functional logic languages and variations of the above.

[3]Support for rational trees is also provided as an option by the YAP Prolog system [56].

[4]Such as TerminWeb [16, 17], TermiLog [49], cTI [54], and LPTP [61, 62].

[5]Systems like GAIA [21], CASLOG [31], and the Ciao-Prolog preprocessor [38].

Prolog, then the only way to get the prompt back is by interrupting the program. The problem stems from the fact that the analysis techniques employed by these tools are only sound for finite trees: as soon as they are applied to a system where the creation of cyclic terms is possible, their results are inapplicable. The situation can be improved by combining these termination and/or complexity analyses with a finiteness analysis providing the precondition for the applicability of the other techniques.

The implementation of built-in predicates is another problematic issue. Indeed, it is widely acknowledged that, for the implementation of a system that provides real support for the rational trees, the biggest effort concerns proper handling of built-ins. Of course, the meaning of 'proper' depends on the actual built-in. Built-ins such as `copy_term/2` and `==/2` maintain a clear semantics when passing from finite to rational trees. For others, like `sort/2`, the extension can be questionable:[6] failing, raising an exception, answering `Y = [a]` (if duplicates are deleted) and answering `Y = [a|Y]` (if duplicates are kept) can all be argued to be "the right reaction" to the query

```
?- X = [a|X], sort(X, Y).
```

Other built-ins do not tolerate infinite trees in some argument positions. A good implementation should check for finiteness of the corresponding arguments and make sure "the right thing" —failing or raising an appropriate exception— always happens. However, such behavior appears to be uncommon. A small experiment we conducted on six Prolog implementations with queries like

```
?- X = 1+X, Y is X.
?- X = [97|X], name(Y, X).
?- X = [X|X], Y =..  [f|X].
```

resulted in infinite loops, memory exhaustion and/or system thrashing, segmentation faults or other fatal errors. One of the implementations tested, SICStus Prolog, is a professional one and implements run-time checks to avoid most cases where built-ins can have catastrophic effects.[7] The remaining systems are a bit more than research prototypes, but will clearly have to do the same if they evolve to the stage of production tools. Again, a data-flow analysis aimed at the detection of those variables that are definitely bound to finite terms could be used to avoid a (possibly significant) fraction of the useless run-time checks. Note that what has been said for built-in predicates applies to libraries as well. Even though it may be argued that it is enough for programmers to know that they should not use a particular library predicate with infinite terms, it is clear that the use of a "safe" library, including automatic checks ensuring that such a predicate is never called with an illegal argument, will result in a robuster system. With the appropriate data-flow analyses, safe libraries do not have to be inefficient libraries.

Another serious problem is the following: the standard term ordering dictated by ISO Prolog [43] cannot be extended to rational trees [M. Carlsson, Personal communication, October 2000]. Consider the rational trees defined by `A = f(B, a)` and `B = f(A, b)`. Clearly, `A == B` does not hold. Since the standard term ordering is total, we must have either `A @< B` or `B @< A`. Assume `A @< B`. Then

[6] Even though `sort/2` is not required to be a built-in by the ISO Prolog standard, it is offered as such by several implementations.

[7] SICStus 3.9.0 still loops on `?- X = [97|X], name(Y, X).`

`f(A, b) @< f(B, a)`, since the ordering of terms having the same principal functor is inherited by the ordering of subterms considered in a left-to-right fashion. Thus `B @< A` must hold, which is a contradiction. A dual contradiction is obtained by assuming `B @< A`. As a consequence, applying any Prolog term-ordering predicate to terms where one or both of them is infinite may cause inconsistent results, giving rise to bugs that are exceptionally difficult to diagnose. For this reason, any system that extends ISO Prolog with rational trees ought to detect such situations and make sure they are not ignored (e.g., by throwing an exception or aborting execution with a meaningful message). However, predicates such as the term-ordering ones are likely to be called a significant number of times, since they are often used to maintain structures implementing ordered collections of terms. This is another instance of the efficiency issue mentioned above.

Still on efficiency, it is worth noting that even for built-ins whose definition on rational trees is not problematic, there is often a performance penalty in catering for the possibility of infinite trees. Thus, for such predicates, a compile-time knowledge of term finiteness can also be beneficial. For instance, rational-tree implementations of the built-ins `ground/1`, `term_variables/2`, `copy_term/2`, `subsumes/2`, `variant/2` and `numbervars/3` need to use some sort of marking to ensure they do not enter an infinite loop. With finiteness information it is possible to avoid this overhead.

In this paper, we present a parametric abstract domain for finite-tree analysis, denoted by $H \times P$. This domain combines a simple component H (written with the initial of *Herbrand* and called the *finiteness* component) recording the set of definitely finite variables, with a generic domain P (the parameter of the construction) providing sharing information. The term "sharing information" is to be understood in its broader meaning, which includes variable aliasing, groundness, linearity, freeness and any other kind of information that can improve the precision on these components, such as explicit structural information. Several domain combinations and abstract operators, characterized by different precision/complexity trade-offs, have been proposed to capture these properties (see [6] for an account of some of them). By giving a generic specification for this parameter component, in the style of the *open product* construct proposed in [25], it is possible to define and establish the correctness of the abstract operators on the finite-tree domain independently from any particular domain for sharing analysis.

The information encoded by H is *attribute independent* [27], which means that each variable is considered in isolation. What this lacks is information about how finiteness of one variable affects the finiteness of other variables. This kind of information, usually called *relational information*, is not captured at all by H and is only partially captured by the composite domain $H \times P$. Moreover, $H \times P$ is designed to capture the "negative" aspect of term-finiteness, that is, the circumstances under which finiteness can be lost. However, term-finiteness has also a "positive" aspect: there are cases where a variable is granted to be bound to a finite term and this knowledge can be propagated to other variables. Guarantees of finiteness are provided by several built-ins like `unify_with_occurs_check/2`, `var/1`, `name/2`, all the arithmetic predicates, besides those explicitly provided to test for term-finiteness such as the `acyclic_term/1` predicate of SICStus Prolog. For these reasons $H \times P$ is coupled with a domain of Boolean functions that precisely captures how the finiteness of some variables influences the finiteness of other variables. This domain of *finite-tree dependencies* provides relational information that is important for the precision of the overall finite-tree analysis.

The domain $H \times P$ also has obvious similarities, interesting differences and somewhat unexpected connections with classical domains for *groundness dependencies*. Finite-tree and groundness dependencies are similar in that they both track *covering* information (a term s covers t if all the variables in t also occur in s) and share several abstract operations. However, they are different because covering does not tell the whole story. Suppose x and y are free variables before either the unification $x = f(y)$ or the unification $x = f(x, y)$ are executed. In both cases, x will be ground if and only if y will be so. However, when $x = f(y)$ is the performed unification, this equivalence will also carry over to finiteness. In contrast, when the unification is $x = f(x, y)$, x will never be finite and will be totally independent, as far as finiteness is concerned, from y. Among the unexpected connections is the fact that finite-tree dependencies can improve the groundness information obtained by the usual approaches to groundness analysis.

The paper is structured as follows. The required notations and preliminary concepts are given in Section 2. The concrete domain for the analysis is presented in Section 3. The finite-tree domain is then introduced in Section 4: Section 4.1 provides the specification of the parameter domain P; Section 4.2 defines some computable operators that extract, from substitutions in rational solved form, properties of the denoted rational trees; Section 4.3 defines the abstraction function for the finiteness component H; Section 4.4 defines the abstract unification operator for $H \times P$. Section 5 introduces the use of Boolean functions for tracking finite-tree dependencies, whereas Section 6 illustrates the interaction between groundness and finite-tree dependencies. Our experimental results are presented in Section 7. We conclude the main body of the paper in Section 8.

Appendix A specifies the sharing domain *SFL* defined in [41, 64] as a possible instance of the parameter P. All the results are then proved in Appendix B.

2. PRELIMINARIES

2.1. Infinite Terms and Substitutions

For a set S, $\wp(S)$ is the powerset of S, whereas $\wp_{\mathrm{f}}(S)$ is the set of all the *finite* subsets of S. Let *Sig* denote a possibly infinite set of function symbols, ranked over the set of natural numbers. It is assumed that *Sig* contains at least one function symbol having rank 0 and one having rank greater than 0. Let *Vars* denote a denumerable set of variables disjoint from *Sig* and *Terms* denote the free algebra of all (possibly infinite) terms in the signature *Sig* having variables in *Vars*. Thus a term can be seen as an ordered labeled tree, possibly having some infinite paths and possibly containing variables: every non-leaf node is labeled with a function symbol in *Sig* with a rank matching the number of the node's immediate descendants, whereas every leaf is labeled by either a variable in *Vars* or a function symbol in *Sig* having rank 0 (a constant).

If $t \in \mathit{Terms}$ then $\mathrm{vars}(t)$ and $\mathrm{mvars}(t)$ denote the set and the multiset of variables occurring in t, respectively. We will also write $\mathrm{vars}(o)$ to denote the set of variables occurring in an arbitrary syntactic object o.

Suppose $s, t \in \mathit{Terms}$: s and t are *independent* if $\mathrm{vars}(s) \cap \mathrm{vars}(t) = \varnothing$; t is said to be *ground* if $\mathrm{vars}(t) = \varnothing$; t is *free* if $t \in \mathit{Vars}$; if $y \in \mathrm{vars}(t)$ occurs exactly once in t, then we say that variable *y occurs linearly in t*, more briefly written using the predication $\mathrm{occ\_lin}(y, t)$; t is *linear* if we have $\mathrm{occ\_lin}(y, t)$ for all $y \in \mathrm{vars}(t)$; finally, t is a *finite term* (or *Herbrand term*) if it contains a finite number of occurrences of function symbols. The sets of all ground, linear and finite terms are denoted by *GTerms*, *LTerms* and *HTerms*, respectively. As we have specified that *Sig* contains function symbols of rank 0 and rank greater than 0, $\mathit{GTerms} \cap \mathit{HTerms} \neq \varnothing$ and $\mathit{GTerms} \setminus \mathit{HTerms} \neq \varnothing$.

A *substitution* is a total function $\sigma \colon \mathit{Vars} \to \mathit{HTerms}$ that is the identity almost everywhere; in other words, the *domain* of σ,

$$\mathrm{dom}(\sigma) \stackrel{\mathrm{def}}{=} \{\, x \in \mathit{Vars} \mid \sigma(x) \neq x \,\},$$

is finite. Given a substitution $\sigma \colon \mathit{Vars} \to \mathit{HTerms}$, we overload the symbol 'σ' so as to denote also the function $\sigma \colon \mathit{HTerms} \to \mathit{HTerms}$ defined as follows, for each term $t \in \mathit{HTerms}$:

$$\sigma(t) \stackrel{\mathrm{def}}{=} \begin{cases} t, & \text{if } t \text{ is a constant symbol;} \\ \sigma(t), & \text{if } t \in \mathit{Vars}; \\ f\bigl(\sigma(t_1), \ldots, \sigma(t_n)\bigr), & \text{if } t = f(t_1, \ldots, t_n). \end{cases}$$

If $t \in \mathit{HTerms}$, we write $t\sigma$ to denote $\sigma(t)$ and $t\sigma\tau$ to denote $(t\sigma)\tau$.

If $x \in \mathit{Vars}$ and $t \in \mathit{HTerms} \setminus \{x\}$, then $x \mapsto t$ is called a *binding*. The set of all bindings is denoted by *Bind*. Substitutions are denoted by the set of their bindings, thus a substitution σ is identified with the (finite) set

$$\{\, x \mapsto x\sigma \mid x \in \mathrm{dom}(\sigma) \,\}.$$

We denote by $\mathrm{vars}(\sigma)$ the set of variables occurring in the bindings of σ.

A substitution is said to be *circular* if, for $n > 1$, it has the form

$$\{x_1 \mapsto x_2, \ldots, x_{n-1} \mapsto x_n, x_n \mapsto x_1\},$$

where $x_1, \ldots, x_n$ are distinct variables. A substitution is in *rational solved form* if it has no circular subset. The set of all substitutions in rational solved form is denoted by *RSubst*.

The composition of substitutions is defined in the usual way. Thus $\tau \circ \sigma$ is the substitution such that, for all terms $t \in \mathit{HTerms}$,

$$(\tau \circ \sigma)(t) = \tau\bigl(\sigma(t)\bigr) = t\sigma\tau$$

and has the formulation

$$\tau \circ \sigma = \{\, x \mapsto x\sigma\tau \mid x \in \mathrm{dom}(\sigma) \cup \mathrm{dom}(\tau), x \neq x\sigma\tau \,\}.$$

As usual, σ^0 denotes the identity function (i.e., the empty substitution) and, when $i > 0$, σ^i denotes the substitution $(\sigma \circ \sigma^{i-1})$.

Consider an infinite sequence of terms $t_0, t_1, t_2, \ldots$ with $t_i \in \mathit{HTerms}$ for each $i \in \mathbb{N}$. Suppose there exists $t \in \mathit{Terms}$ such that, for each $n \in \mathbb{N}$, there exists $m_0 \in \mathbb{N}$ such that, for each $m \in \mathbb{N}$ with $m \geq m_0$, the trees corresponding to the terms t and t_m coincide up to the first n levels. Then we say that *the sequence* $t_0, t_1, t_2, \ldots$ *converges to* t and we write $t = \lim_{i \to \infty} t_i$ [8].

For each $\sigma \in \mathit{RSubst}$ and $t \in \mathit{HTerms}$, the sequence of finite terms

$$\sigma^0(t), \sigma^1(t), \sigma^2(t), \ldots$$

converges [8, 48]. Therefore, the function $\mathrm{rt} \colon \mathit{HTerms} \times \mathit{RSubst} \to \mathit{Terms}$ such that

$$\mathrm{rt}(t, \sigma) \stackrel{\mathrm{def}}{=} \lim_{i \to \infty} \sigma^i(t)$$

is well defined.

2.2. Equations

An *equation* is a statement of the form $s = t$ where $s, t \in \mathit{HTerms}$. *Eqs* denotes the set of all equations. A substitution σ may be regarded as a finite set of equations, that is, as the set $\{ x = t \mid x \mapsto t \in \sigma \}$. We say that a set of equations e is in *rational solved form* if $\bigl\{ s \mapsto t \bigm| (s = t) \in e \bigr\} \in \mathit{RSubst}$. In the rest of the paper, we will often write a substitution $\sigma \in \mathit{RSubst}$ to denote a set of equations in rational solved form (and vice versa).

Languages such as Prolog II, SICStus and Oz are based on $\mathcal{RT}$, the theory of rational trees [18, 19]. This is a syntactic equality theory (i.e., a theory where the function symbols are uninterpreted), augmented with a *uniqueness axiom* for each substitution in rational solved form. Informally speaking these axioms state that, after assigning a ground rational tree to each non-domain variable, the substitution uniquely defines a ground rational tree for each of its domain variables. Thus, any set of equations in rational solved form is, by definition, satisfiable in $\mathcal{RT}$. Equality theories and, in particular, $\mathcal{RT}$ are presented in more detail in Section B.1.1. Note that being in rational solved form is a very weak property. Indeed, unification algorithms returning a set of equations in rational solved form are allowed to be much more "lazy" than one would usually expect. For instance, $\{x = y, y = z\}$ and $\bigl\{x = f(y), y = f(x)\bigr\}$ are in rational solved form. We refer the interested reader to [46, 47, 50] for details on the subject.

Given a set of equations $e \in \wp_{\mathrm{f}}(\mathit{Eqs})$ that is satisfiable in $\mathcal{RT}$, a substitution $\sigma \in \mathit{RSubst}$ is called a *solution for e in $\mathcal{RT}$* if $\mathcal{RT} \vdash \forall(\sigma \rightarrow e)$, i.e., if theory $\mathcal{RT}$ entails the first order formula $\forall(\sigma \rightarrow e)$. If in addition $\mathrm{vars}(\sigma) \subseteq \mathrm{vars}(e)$, then σ is said to be a *relevant* solution for e. Finally, σ is a *most general solution for e in $\mathcal{RT}$* if $\mathcal{RT} \vdash \forall(\sigma \leftrightarrow e)$. In this paper, the set of all the relevant most general solution for e in $\mathcal{RT}$ will be denoted by $\mathrm{mgs}(e)$.

In the sequel, in order to model the constraint accumulation process of logic-based languages, we will need to characterize those sets of equations that are stronger than (that can be obtained by adding equations to) a given set of equations.

Definition 1. **($\downarrow(\cdot)$)** *The function $\downarrow(\cdot)\colon \mathit{RSubst} \rightarrow \wp(\mathit{RSubst})$ is defined, for each $\sigma \in \mathit{RSubst}$, by*

$$\downarrow \sigma \stackrel{\mathrm{def}}{=} \bigl\{ \tau \in \mathit{RSubst} \bigm| \exists \sigma' \in \mathit{RSubst} \mathrel{.} \tau \in \mathrm{mgs}(\sigma \cup \sigma') \bigr\}.$$

The next result shows that $\downarrow(\cdot)$ corresponds to the closure by entailment in $\mathcal{RT}$.

Proposition 2. *Let $\sigma \in \mathit{RSubst}$. Then*

$$\downarrow \sigma = \bigl\{ \tau \in \mathit{RSubst} \bigm| \mathcal{RT} \vdash \forall(\tau \rightarrow \sigma) \bigr\}.$$

2.3. Boolean Functions

Boolean functions have already been extensively used for data-flow analysis of logic-based languages. An important class of these functions used for tracking groundness dependencies is *Pos* [1]. This domain was introduced in [51] under the name *Prop* and further refined and studied in [23, 52].

Boolean functions are based on the notion of Boolean valuation.

Definition 3. **(Boolean valuation.)** *Let $\mathit{VI} \in \wp_{\mathrm{f}}(\mathit{Vars})$ and $\mathit{Bool} \stackrel{\mathrm{def}}{=} \{0, 1\}$. The set of* Boolean valuations over *VI is given by*

$$\mathit{Bval} \stackrel{\mathrm{def}}{=} \mathit{VI} \rightarrow \mathit{Bool}.$$

For each $a \in Bval$, each $x \in VI$, and each $c \in Bool$ the valuation $a[c/x] \in Bval$ is given, for each $y \in VI$, by

$$a[c/x](y) \stackrel{\text{def}}{=} \begin{cases} c, & \text{if } x = y; \\ a(y), & \text{otherwise.} \end{cases}$$

If $X = \{x_1, \ldots, x_k\} \subseteq VI$, then $a[c/X]$ denotes $a[c/x_1] \cdots [c/x_k]$.

The distinguished elements $\mathbf{0}, \mathbf{1} \in Bval$ are given by

$$\mathbf{0} \stackrel{\text{def}}{=} \lambda x \in VI \,.\, 0,$$
$$\mathbf{1} \stackrel{\text{def}}{=} \lambda x \in VI \,.\, 1.$$

Definition 4. **(Boolean function.)** *The set of* Boolean functions over *VI is*

$$Bfun \stackrel{\text{def}}{=} Bval \to Bool.$$

Bfun is partially ordered by the relation $\models$ where, for each $\phi, \psi \in Bfun$,

$$\phi \models \psi \quad \stackrel{\text{def}}{\iff} \quad \bigl(\forall a \in Bval : \phi(a) = 1 \implies \psi(a) = 1\bigr).$$

The distinguished elements $\bot, \top \in Bfun$ are the functions defined by

$$\bot \stackrel{\text{def}}{=} \lambda a \in Bval \,.\, 0,$$
$$\top \stackrel{\text{def}}{=} \lambda a \in Bval \,.\, 1.$$

For $\phi \in Bfun$, $x \in VI$, and $c \in Bool$, the Boolean function $\phi[c/x] \in Bfun$ is given, for each $a \in Bval$, by

$$\phi[c/x](a) \stackrel{\text{def}}{=} \phi\bigl(a[c/x]\bigr).$$

When $X \subseteq VI$, $\phi[c/X]$ is defined in the expected way. If $\phi \in Bfun$ and $x, y \in VI$ the function $\phi[y/x] \in Bfun$ is given, for each $a \in Bval$, by

$$\phi[y/x](a) \stackrel{\text{def}}{=} \phi\Bigl(a\bigl[a(y)/x\bigr]\Bigr).$$

Boolean functions are constructed from the elementary functions corresponding to variables and by means of the usual logical connectives. Thus, for each $x \in VI$, x also denotes the Boolean function ϕ such that, for each $a \in Bval$, $\phi(a) = 1$ if and only if $a(x) = 1$. For $\phi_1, \phi_2 \in Bfun$, we write $\phi_1 \wedge \phi_2$ to denote the function ϕ such that, for each $a \in Bval$, $\phi(a) = 1$ if and only if both $\phi_1(a) = 1$ and $\phi_2(a) = 1$. A variable is restricted away using Schröder's elimination principle [57]:

$$\exists x \,.\, \phi \stackrel{\text{def}}{=} \phi[1/x] \vee \phi[0/x].$$

Note that existential quantification is both monotonic and extensive on *Bfun*. The other Boolean connectives and quantifiers are handled similarly. For notational convenience, when $X \subseteq VI$, we inductively define

$$\bigwedge X \stackrel{\text{def}}{=} \begin{cases} \top, & \text{if } X = \varnothing; \\ x \wedge \bigwedge\bigl(X \setminus \{x\}\bigr) & \text{if } x \in X. \end{cases}$$

$Pos \subset Bfun$ consists precisely of those functions assuming the true value under the *everything-is-true* assignment, i.e.,

$$Pos \stackrel{\text{def}}{=} \bigl\{\, \phi \in Bfun \bigm| \phi(\mathbf{1}) = 1 \,\bigr\}.$$

For each $\phi \in Bfun$, the *positive part of* ϕ, denoted $\mathrm{pos}(\phi)$, is the strongest Pos formula that is entailed by ϕ. Formally,

$$\mathrm{pos}(\phi) \stackrel{\text{def}}{=} \phi \vee \bigwedge VI.$$

For each $\phi \in Bfun$, the set of *variables necessarily true for* ϕ and the set of *variables necessarily false for* ϕ are given, respectively, by

$$\mathrm{true}(\phi) \stackrel{\text{def}}{=} \bigl\{\, x \in VI \bigm| \forall a \in Bval : \phi(a) = 1 \implies a(x) = 1 \,\bigr\},$$
$$\mathrm{false}(\phi) \stackrel{\text{def}}{=} \bigl\{\, x \in VI \bigm| \forall a \in Bval : \phi(a) = 1 \implies a(x) = 0 \,\bigr\}.$$

3. THE CONCRETE DOMAIN

A knowledge of the basic concepts of abstract interpretation theory [26, 28] is assumed. In this paper, the concrete domain consists of pairs of the form (Σ, V), where V is a finite set of *variables of interest* and Σ is a (possibly infinite) set of substitutions in rational solved form.

Definition 5. **(The concrete domain.)** *Let* $\mathcal{D}^\flat \stackrel{\text{def}}{=} \wp(RSubst) \times \wp_\mathrm{f}(Vars)$. *If* $(\Sigma, V) \in \mathcal{D}^\flat$, *then* (Σ, V) *represents the (possibly infinite) set of first-order formulas* $\bigl\{\, \exists\Delta \,.\, \sigma \bigm| \sigma \in \Sigma, \Delta = \mathrm{vars}(\sigma) \setminus V \,\bigr\}$ *where* σ *is interpreted as the logical conjunction of the equations corresponding to its bindings.*

The operation of projecting $x \in Vars$ *away from* $(\Sigma, V) \in \mathcal{D}^\flat$ *is defined as follows:*

$$\exists\, x \,.\, (\Sigma, V) \stackrel{\text{def}}{=} \left\{\, \sigma' \in RSubst \;\middle|\; \begin{array}{l} \sigma \in \Sigma, \overline{V} = Vars \setminus V, \\ \mathcal{RT} \vdash \forall\bigl(\exists \overline{V} \,.\, (\sigma' \leftrightarrow \exists x \,.\, \sigma)\bigr) \end{array} \right\}.$$

Concrete domains for constraint languages would be similar. If the analyzed language allows the use of constraints on various domains to restrict the values of the variable leaves of rational trees, the corresponding concrete domain would have one or more extra components to account for the constraints (see [3] for an example).

The concrete element $\bigl(\bigl\{\{x \mapsto f(y)\}\bigr\}, \{x, y\}\bigr)$ expresses a dependency between x and y. In contrast, $\bigl(\bigl\{\{x \mapsto f(y)\}\bigr\}, \{x\}\bigr)$ only constrains x. The same concept can be expressed by saying that in the first case the variable name 'y' matters, but it does not in the second case. Thus, the set of variables of interest is crucial for defining the meaning of the concrete and abstract descriptions. Despite this, always specifying the set of variables of interest would significantly clutter the presentation. Moreover, most of the needed functions on concrete and abstract descriptions preserve the set of variables of interest. For these reasons, we assume the existence of a set $VI \in \wp_\mathrm{f}(Vars)$ that contains, at each stage of the analysis, the current variables of interest.[8] As a consequence, when the context makes it clear, we will write $\Sigma \in \mathcal{D}^\flat$ as a shorthand for $(\Sigma, VI) \in \mathcal{D}^\flat$.

[8] This parallels what happens in the efficient implementation of data-flow analyzers. In fact, almost all the abstract domains currently in use do not need to represent explicitly the set of variables of interest. In contrast, this set is maintained externally and in a unique copy, typically by the fixpoint computation engine.

4. AN ABSTRACT DOMAIN FOR FINITENESS ANALYSIS

Finite-tree analysis applies to logic-based languages computing over a domain of rational trees where cyclic structures are allowed. In contrast, analyses aimed at occurs-check reduction [29, 60] apply to programs that are meant to compute on a domain of finite trees only, but have to be executed over systems that are either designed for rational trees or intended just for the finite trees but omit the occurs-check for efficiency reasons. Despite their different objectives, finite-tree and occurs-check analyses have much in common: in both cases, it is important to detect all program points where cyclic structures can be generated.

Note however that, when performing occurs-check reduction, one can take advantage of the following invariant: all data structures generated so far are finite. This property is maintained by transforming the program so as to force finiteness whenever it is possible that a cyclic structure could have been built.[9] In contrast, a finite-tree analysis has to deal with the more general case when some of the data structures computed so far may be cyclic. It is therefore natural to consider an abstract domain made up of two components. The first one simply represents the set of variables that are guaranteed not to be bound to infinite terms. We will denote this *finiteness component* by H (from *Herbrand*).

Definition 6. **(The finiteness component.)** *The* finiteness component *is the set* $H \stackrel{\text{def}}{=} \wp(VI)$ *partially ordered by reverse subset inclusion.*

The second component of the finite-tree domain should maintain any kind of information that may be useful for computing finiteness information.

It is well-known that sharing information as a whole, therefore including possible variable aliasing, definite linearity, and definite freeness, has a crucial role in occurs-check reduction so that, as observed before, it can be exploited for finite-tree analysis too. Thus, a first choice for the second component of the finite-tree domain would be to consider one of the standard combinations of sharing, freeness and linearity as defined, e.g., in [6, 9, 36]. However, this would tie our specification to a particular sharing analysis domain, whereas the overall approach is inherently more general. For this reason, we will define a finite-tree analysis based on the abstract domain schema $H \times P$, where the generic *sharing component* P is a parameter of the abstract domain construction. This approach can be formalized as an application of the *open product* operator [25].

4.1. The parameter Component P

Elements of P can encode any kind of information. We only require that substitutions that are equivalent in the theory $\mathcal{RT}$ are identified in P.

Definition 7. **(The parameter component.)** *The parameter component* P *is an abstract domain related to the concrete domain* $\mathcal{D}^\flat$ *by means of the* concretization function $\gamma_P \colon P \to \wp(RSubst)$ *such that, for all* $p \in P$,

$$\Big(\sigma \in \gamma_P(p) \land \big(\mathcal{RT} \vdash \forall(\sigma \leftrightarrow \tau)\big)\Big) \implies \tau \in \gamma_P(p).$$

[9] Such a requirement is typically obtained by replacing the unification with a call to the standard predicate `unify_with_occurs_check/2`. As an alternative, in some systems based on rational trees it is possible to insert, after each problematic unification, a finiteness test for the generated term.

The interface between H and P is provided by a set of abstract operators that satisfy suitable correctness criteria. We only specify those that are useful for defining abstract unification and projection on the combined domain $H \times P$. Other operations needed for a full description of the analysis, such as renaming and upper bound, are very simple and, as usual, do not pose any problems.

DEFINITION 8. **(Abstract operators on P.)** *Let $s, t \in \mathit{HTerms}$ be finite terms. For each $p \in P$, we specify the following predicates:*
s and t are independent *in p if and only if* $\mathrm{ind}_p \colon \mathit{HTerms}^2 \to \mathit{Bool}$ *holds for (s, t), where*

$$\mathrm{ind}_p(s,t) \implies \forall \sigma \in \gamma_P(p) : \mathrm{vars}\bigl(\mathrm{rt}(s,\sigma)\bigr) \cap \mathrm{vars}\bigl(\mathrm{rt}(t,\sigma)\bigr) = \varnothing;$$

s and t share linearly *in p if and only if* $\mathrm{share\_lin}_p \colon \mathit{HTerms}^2 \to \mathit{Bool}$ *holds for (s, t), where*

$$\begin{aligned} \mathrm{share\_lin}_p(s,t) \implies \forall \sigma \in \gamma_P(p) : & \\ & \forall y \in \mathrm{vars}\bigl(\mathrm{rt}(s,\sigma)\bigr) \cap \mathrm{vars}\bigl(\mathrm{rt}(t,\sigma)\bigr) : \\ & \qquad \mathrm{occ\_lin}\bigl(y, \mathrm{rt}(s,\sigma)\bigr) \land \mathrm{occ\_lin}\bigl(y, \mathrm{rt}(t,\sigma)\bigr); \end{aligned}$$

t is ground *in p if and only if* $\mathrm{ground}_p \colon \mathit{HTerms} \to \mathit{Bool}$ *holds for t, where*

$$\mathrm{ground}_p(t) \implies \forall \sigma \in \gamma_P(p) : \mathrm{rt}(t,\sigma) \in \mathit{GTerms};$$

t is ground-or-free *in p if and only if* $\mathrm{gfree}_p \colon \mathit{HTerms} \to \mathit{Bool}$ *holds for t, where*

$$\mathrm{gfree}_p(t) \implies \forall \sigma \in \gamma_P(p) : \mathrm{rt}(t,\sigma) \in \mathit{GTerms} \lor \mathrm{rt}(t,\sigma) \in \mathit{Vars};$$

s is linear *in p if and only if* $\mathrm{lin}_p \colon \mathit{HTerms} \to \mathit{Bool}$ *holds for s, where*

$$\mathrm{lin}_p(s) \implies \forall \sigma \in \gamma_P(p) : \mathrm{rt}(s,\sigma) \in \mathit{LTerms};$$

s and t are or-linear *in p if and only if* $\mathrm{or\_lin}_p \colon \mathit{HTerms}^2 \to \mathit{Bool}$ *holds for (s, t), where*

$$\mathrm{or\_lin}_p(s,t) \implies \forall \sigma \in \gamma_P(p) : \mathrm{rt}(s,\sigma) \in \mathit{LTerms} \lor \mathrm{rt}(t,\sigma) \in \mathit{LTerms};$$

For each $p \in P$, the following functions compute subsets of the set of variables of interest:
the function $\mathrm{share\_same\_var}_p \colon \mathit{HTerms} \times \mathit{HTerms} \to \wp(\mathit{VI})$ *returns a set of variables that may share with the given terms via the same variable. For each pair of terms $s, t \in \mathit{HTerms}$,*

$$\mathrm{share\_same\_var}_p(s,t) \supseteq \left\{ y \in \mathit{VI} \;\middle|\; \begin{aligned} & \exists \sigma \in \gamma_P(p) \,. \\ & \quad \exists z \in \mathrm{vars}\bigl(\mathrm{rt}(y,\sigma)\bigr) \,. \\ & \qquad z \in \mathrm{vars}\bigl(\mathrm{rt}(s,\sigma)\bigr) \cap \mathrm{vars}\bigl(\mathrm{rt}(t,\sigma)\bigr) \end{aligned} \right\};$$

the function $\mathrm{share\_with}_p \colon HTerms \to \wp(VI)$ *yields a set of variables that may share with the given term. For each* $t \in HTerms$*,*

$$\mathrm{share\_with}_p(t) \stackrel{\mathrm{def}}{=} \bigl\{\, y \in VI \bigm| y \in \mathrm{share\_same\_var}_p(y, t) \,\bigr\}.$$

The function $\mathrm{amgu}_P \colon P \times Bind \to P$ *correctly captures the effects of a binding on an element of* P*. For each* $(x \mapsto t) \in Bind$ *and* $p \in P$*, let*

$$p' \stackrel{\mathrm{def}}{=} \mathrm{amgu}_P(p, x \mapsto t);$$

for all $\sigma \in \gamma_P(p)$*, if* $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$*, then* $\tau \in \gamma_P(p')$*.*

The function $\mathrm{proj}_P \colon P \times VI \to P$ *correctly captures the operation of projecting away a variable from an element of* P*. For each* $x \in VI$*,* $p \in P$ *and* $\sigma \in \gamma_P(p)$*, if* $\tau \in \exists x \,.\, \{\sigma\}$*, then* $\tau \in \gamma_P\bigl(\mathrm{proj}_P(p, x)\bigr)$*.*

As it will be shown in Section A, some of these generic operators can be directly mapped to the corresponding abstract operators defined for well-known sharing analysis domains. However, the specification given in Definition 8, besides being more general than a particular implementation, also allows for a modular approach when proving correctness results.

4.2. Operators on Substitutions in Rational Solved Form

There are cases when an analysis tries to capture properties of the particular substitutions computed by a specific (ordinary or rational) unification algorithm. This is the case, for example, when the analysis needs to track structure sharing for the purpose of compile-time garbage collection, or provide upper bounds on the amount of memory needed to perform a given computation. More often the interest is on properties of the (finite or rational) trees that are denoted by such substitutions.

When the concrete domain is based on the theory of finite trees, idempotent substitutions provide a finitely computable *strong normal form* for domain elements, meaning that different substitutions describe different sets of finite trees (as usual, this is modulo the possible renaming of variables). In contrast, when working on a concrete domain based on the theory of rational trees, substitutions in rational solved form, while being finitely computable, no longer satisfy this property: there can be an infinite set of substitutions in rational solved form all describing the same set of rational trees (i.e., the same element in the "intended" semantics). For instance, the substitutions

$$\sigma_n = \bigl\{x \mapsto \overbrace{f(\cdots f(}^{n} x)\cdots)\bigr\}$$

for $n = 1, 2, \ldots$, all map the variable x to the same rational tree (which is usually denoted by f^ω).

Ideally, a strong normal form for the set of rational trees described by a substitution $\sigma \in RSubst$ can be obtained by computing the limit function

$$\sigma^\infty \stackrel{\mathrm{def}}{=} \lambda t \in HTerms \,.\, \mathrm{rt}(t, \sigma),$$

obtained by fixing the substitution parameter of 'rt'. The problem is that, in general, σ^∞ is not a substitution: while having a finite domain, its "bindings" $x \mapsto$

$\lim_{i \to \infty} \sigma^i(x)$ can map a domain variable x to an infinite rational term. This poses a non-trivial problem when trying to define a "good" abstraction function, since it would be really desirable for this function to map any two equivalent concrete elements to the same abstract element. Of course, it is important that the properties under investigation are exactly captured, so as to avoid any unnecessary precision loss. Pursuing this goal requires an ability to observe properties of (infinite) rational trees while just dealing with one of their finite representations. This is not always an easy task since even simple properties can be "hidden" when using non-idempotent substitutions. For instance, when σ^∞ maps variable x to an infinite and ground rational tree (i.e., when $\mathrm{rt}(x, \sigma) \in \mathit{GTerms} \setminus \mathit{HTerms}$), all of its finite representations in *RSubst* (i.e., all the $\tau \in \mathit{RSubst}$ such that $\mathcal{RT} \models \forall(\sigma \leftrightarrow \tau)$) will map the variable x into a finite term that is not ground. These are the motivations behind the introduction of the following computable operators on substitutions.

The groundness operator 'gvars' captures the set of variables that are mapped to ground rational trees by rt. We define it by means of the *occurrence operator* 'occ'. This was introduced in [40] as a replacement for the sharing-group operator 'sg' of [44]. In [40] the occ operator is used to define a new abstraction function for set-sharing analysis that, differently from the classical ones [22, 44], maps equivalent substitutions in rational solved form to the same abstract element.

Definition 9. **(Occurrence and groundness operators.)** *For each $n \in \mathbb{N}$, the* occurrence function $\mathrm{occ}_n \colon \mathit{RSubst} \times \mathit{Vars} \to \wp_\mathrm{f}(\mathit{Vars})$ *is defined, for each $\sigma \in \mathit{RSubst}$ and each $v \in \mathit{Vars}$, by*

$$\mathrm{occ}_n(\sigma, v) \stackrel{\mathrm{def}}{=} \begin{cases} \{v\} \setminus \mathrm{dom}(\sigma), & \text{if } n = 0; \\ \bigl\{\, y \in \mathit{Vars} \bigm| \mathrm{vars}(y\sigma) \cap \mathrm{occ}_{n-1}(\sigma, v) \neq \varnothing \,\bigr\}, & \text{if } n > 0. \end{cases}$$

The occurrence operator $\mathrm{occ} \colon \mathit{RSubst} \times \mathit{Vars} \to \wp_\mathrm{f}(\mathit{Vars})$ *is given, for each substitution $\sigma \in \mathit{RSubst}$ and $v \in \mathit{Vars}$, by* $\mathrm{occ}(\sigma, v) \stackrel{\mathrm{def}}{=} \mathrm{occ}_\ell(\sigma, v)$, *where $\ell = \# \sigma$.*

The groundness operator $\mathrm{gvars} \colon \mathit{RSubst} \to \wp_\mathrm{f}(\mathit{Vars})$ *is given, for each substitution $\sigma \in \mathit{RSubst}$, by*

$$\mathrm{gvars}(\sigma) \stackrel{\mathrm{def}}{=} \bigl\{\, y \in \mathrm{dom}(\sigma) \bigm| \forall v \in \mathrm{vars}(\sigma) : y \notin \mathrm{occ}(\sigma, v) \,\bigr\}.$$

Example 10. *Let*

$$\sigma = \bigl\{ x \mapsto f(y, z), y \mapsto g(z, x), z \mapsto f(a) \bigr\}.$$

Then $\mathrm{gvars}(\sigma) = \{x, y, z\}$, *although* $\mathrm{vars}(x\sigma^i) \neq \varnothing$ *and* $\mathrm{vars}(y\sigma^i) \neq \varnothing$, *for all* $0 \leq i < \infty$.

The *finiteness operator* is defined, like occ, by means of a fixpoint construction.

Definition 11. **(Finiteness functions.)** *For each $n \in \mathbb{N}$, the* finiteness function $\mathrm{hvars}_n \colon \mathit{RSubst} \to \wp(\mathit{Vars})$ *is defined, for each $\sigma \in \mathit{RSubst}$, by*

$$\mathrm{hvars}_0(\sigma) \stackrel{\mathrm{def}}{=} \mathit{Vars} \setminus \mathrm{dom}(\sigma)$$

and, for $n > 0$, by

$$\mathrm{hvars}_n(\sigma) \stackrel{\mathrm{def}}{=} \mathrm{hvars}_{n-1}(\sigma) \cup \bigl\{\, y \in \mathrm{dom}(\sigma) \bigm| \mathrm{vars}(y\sigma) \subseteq \mathrm{hvars}_{n-1}(\sigma) \,\bigr\}.$$

For each $\sigma \in \mathit{RSubst}$ and each $i \geq 0$, we have $\mathrm{hvars}_i(\sigma) \subseteq \mathrm{hvars}_{i+1}(\sigma)$ and also that $\mathit{Vars} \setminus \mathrm{hvars}_i(\sigma) \subseteq \mathrm{dom}(\sigma)$ is a finite set. By these two properties, the chain $\mathrm{hvars}_0(\sigma) \subseteq \mathrm{hvars}_1(\sigma) \subseteq \cdots$ is stationary and finitely computable. In particular, if $\ell = \# \sigma$, then, for all $n \geq \ell$, $\mathrm{hvars}_\ell(\sigma) = \mathrm{hvars}_n(\sigma)$.

DEFINITION 12. **(Finiteness operator.)** *For each $\sigma \in \mathit{RSubst}$, the* finiteness operator hvars: *$\mathit{RSubst} \to \wp(\mathit{Vars})$ is given by $\mathrm{hvars}(\sigma) \stackrel{\mathrm{def}}{=} \mathrm{hvars}_\ell(\sigma)$ where $\ell \stackrel{\mathrm{def}}{=} \ell(\sigma) \in \mathbb{N}$ is such that $\mathrm{hvars}_\ell(\sigma) = \mathrm{hvars}_n(\sigma)$ for all $n \geq \ell$.*

The following proposition shows that the hvars operator precisely captures the intended property.

PROPOSITION 13. *If $\sigma \in \mathit{RSubst}$ and $x \in \mathit{Vars}$ then*

$$x \in \mathrm{hvars}(\sigma) \iff \mathrm{rt}(x, \sigma) \in \mathit{HTerms}.$$

EXAMPLE 14. *Consider $\sigma \in \mathit{RSubst}$, where*

$$\sigma = \bigl\{ x_1 \mapsto f(x_2), x_2 \mapsto g(x_5), x_3 \mapsto f(x_4), x_4 \mapsto g(x_3) \bigr\}.$$

Then,

$$\begin{aligned} \mathrm{hvars}_0(\sigma) &= \mathit{Vars} \setminus \{x_1, x_2, x_3, x_4\}, \\ \mathrm{hvars}_1(\sigma) &= \mathit{Vars} \setminus \{x_1, x_3, x_4\}, \\ \mathrm{hvars}_2(\sigma) &= \mathit{Vars} \setminus \{x_3, x_4\} \\ &= \mathrm{hvars}(\sigma). \end{aligned}$$

Thus, $x_1 \in \mathrm{hvars}(\sigma)$, although $\mathrm{vars}(x_1\sigma) \subseteq \mathrm{dom}(\sigma)$.

The following proposition states how 'gvars' and 'hvars' behave with respect to the further instantiation of variables.

PROPOSITION 15. *Let $\sigma, \tau \in \mathit{RSubst}$, where $\tau \in \downarrow \sigma$. Then*

$$\mathrm{hvars}(\sigma) \supseteq \mathrm{hvars}(\tau), \tag{15a}$$

$$\mathrm{gvars}(\sigma) \cap \mathrm{hvars}(\sigma) \subseteq \mathrm{gvars}(\tau) \cap \mathrm{hvars}(\tau). \tag{15b}$$

4.3. The Abstraction Function for H

A Galois connection between $\wp(\mathit{RSubst})$ and H can now be defined naturally.

DEFINITION 16. **(The Galois connection between $\wp(\mathit{RSubst})$ and H.)** *The abstraction function $\alpha_H \colon \mathit{RSubst} \to H$ is defined, for each $\sigma \in \mathit{RSubst}$, by*

$$\alpha_H(\sigma) \stackrel{\mathrm{def}}{=} \mathit{VI} \cap \mathrm{hvars}(\sigma).$$

The concrete domain $\mathcal{D}^\flat$ is related to H by means of the abstraction function *$\alpha_H \colon \mathcal{D}^\flat \to H$ such that, for each $\Sigma \in \wp(\mathit{RSubst})$,*

$$\alpha_H(\Sigma) \stackrel{\mathrm{def}}{=} \bigcap \bigl\{ \alpha_H(\sigma) \bigm| \sigma \in \Sigma \bigr\}.$$

Since the abstraction function α_H is additive, the concretization function is given by its adjoint [26]*: whenever $h \in H$,*

$$\begin{aligned} \gamma_H(h) &\stackrel{\mathrm{def}}{=} \bigl\{ \sigma \in \mathit{RSubst} \bigm| \alpha_H(\sigma) \supseteq h \bigr\} \\ &\stackrel{\mathrm{def}}{=} \bigl\{ \sigma \in \mathit{RSubst} \bigm| \mathrm{hvars}(\sigma) \supseteq h \bigr\}. \end{aligned}$$

With these definitions, we have the desired result: equivalent substitutions in rational solved form have the same finiteness abstraction.

THEOREM 17. *If* $\sigma, \tau \in \mathit{RSubst}$ *and* $\mathcal{RT} \vdash \forall(\sigma \leftrightarrow \tau)$*, then* $\alpha_H(\sigma) = \alpha_H(\tau)$*.*

4.4. Abstract Unification and Projection on $H \times P$

The abstract unification for the combined domain $H \times P$ is defined by using the abstract predicates and functions as specified for P as well as a new finiteness predicate for the domain H.

DEFINITION 18. **(Abstract unification on $H \times P$.)** *A term* $t \in \mathit{HTerms}$ *is a* finite tree *in* $h \in H$ *if and only if the predicate* $\mathrm{hterm}_h \colon \mathit{HTerms} \to \mathit{Bool}$ *holds for* t*, where*

$$\mathrm{hterm}_h(t) \stackrel{\mathrm{def}}{=} \bigl(\mathrm{vars}(t) \subseteq h\bigr).$$

The function $\mathrm{amgu}_H \colon (H \times P) \times \mathit{Bind} \to H$ *captures the effects of a binding on an* H *element. Let* $\langle h, p\rangle \in H \times P$ *and* $(x \mapsto t) \in \mathit{Bind}$*. Then*

$$\mathrm{amgu}_H\bigl(\langle h, p\rangle, x \mapsto t\bigr) \stackrel{\mathrm{def}}{=} h',$$

where h' *is given by the first case that applies in*

$$h' \stackrel{\mathrm{def}}{=} \begin{cases} h \cup \mathrm{vars}(t), & \textit{if } \mathrm{hterm}_h(x) \land \mathrm{ground}_p(x); \\ h \cup \{x\}, & \textit{if } \mathrm{hterm}_h(t) \land \mathrm{ground}_p(t); \\ h, & \textit{if } \mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \\ & \quad \land \mathrm{ind}_p(x,t) \land \mathrm{or\_lin}_p(x,t); \\ h, & \textit{if } \mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \\ & \quad \land \mathrm{gfree}_p(x) \land \mathrm{gfree}_p(t); \\ h \setminus \mathrm{share\_same\_var}_p(x,t), & \textit{if } \mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \\ & \quad \land \mathrm{share\_lin}_p(x,t) \\ & \quad \land \mathrm{or\_lin}_p(x,t); \\ h \setminus \mathrm{share\_with}_p(x), & \textit{if } \mathrm{hterm}_h(x) \land \mathrm{lin}_p(x); \\ h \setminus \mathrm{share\_with}_p(t), & \textit{if } \mathrm{hterm}_h(t) \land \mathrm{lin}_p(t); \\ h \setminus \bigl(\mathrm{share\_with}_p(x) \cup \mathrm{share\_with}_p(t)\bigr), & \textit{otherwise.} \end{cases}$$

The abstract unification function $\mathrm{amgu} \colon (H \times P) \times \mathit{Bind} \to H \times P$*, for any* $\langle h, p\rangle \in H \times P$ *and* $(x \mapsto t) \in \mathit{Bind}$*, is given by*

$$\mathrm{amgu}\bigl(\langle h, p\rangle, x \mapsto t\bigr) \stackrel{\mathrm{def}}{=} \Bigl\langle \mathrm{amgu}_H\bigl(\langle h, p\rangle, x \mapsto t\bigr), \mathrm{amgu}_P(p, x \mapsto t)\Bigr\rangle.$$

In the computation of h' (the new finiteness component resulting from the abstract evaluation of a binding) there are eight cases based on properties holding for the concrete terms described by x and t.

1. In the first case, the concrete term described by x is both finite and ground. Thus, after a successful execution of the binding, any concrete term described by t will be finite. Note that t could have contained variables which may be possibly bound to cyclic terms just before the execution of the binding.

2. The second case is symmetric to the first one. Note that these are the only cases when a "positive" propagation of finiteness information is correct. In contrast, in all the remaining cases, the goal is to limit as much as possible the propagation of "negative" information, i.e., the possible cyclicity of terms.

3. The third case exploits the classical results proved in research work on occurs-check reduction [29, 60]. Accordingly, it is required that both x and t describe finite terms that do not share. The use of the implicitly disjunctive predicate $\mathrm{or\_lin}_p$ allows for the application of this case even when neither x nor t are known to be definitely linear. For instance, as observed in [29], this may happen when the component P embeds the domain *Pos* for groundness analysis.[10]

4. The fourth case exploits the observation that cyclic terms cannot be created when unifying two finite terms that are either ground or free. Ground-or-freeness [6] is a safe, more precise and inexpensive replacement for the classical freeness property when combining sharing analysis domains.

5. The fifth case applies when unifying a linear and finite term with another finite term possibly sharing with it, provided they can only share linearly (namely, all the shared variables occur linearly in the considered terms). In such a context, only the shared variables can introduce cycles.

6. In the sixth case, we drop the assumption about the finiteness of the term described by t. As a consequence, all variables sharing with x become possibly cyclic. However, provided x describes a finite and linear term, all finite variables independent from x preserve their finiteness.

7. The seventh case is symmetric to the sixth one.

8. The last case states that term finiteness is preserved for all variables that are independent from both x and t.

The following result, together with the assumption on amgu_P as specified in Definition 8, ensures that abstract unification on the combined domain $H \times P$ is correct.

THEOREM 19. *Let $\langle h, p \rangle \in H \times P$ and $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Let also $\sigma \in \gamma_H(h) \cap \gamma_P(p)$ and $h' = \mathrm{amgu}_H\bigl(\langle h, p \rangle, x \mapsto t\bigr)$. Then*

$$\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr) \implies \tau \in \gamma_H(h').$$

Abstract projection on the composite domain $H \times P$ is much simpler than abstract unification, because in this case there is no interaction between the two components of the abstract domain.

DEFINITION 20. **(Abstract projection on $H \times P$.)** *The function $\mathrm{proj}_H \colon H \times VI \to H$ captures the effects, on the H component, of projecting away a variable. For each $h \in H$ and $x \in VI$,*

$$\mathrm{proj}_H(h, x) \stackrel{\mathrm{def}}{=} h \cup \{x\}.$$

[10] Let t be y. Let also P be *Pos*. Then, given the *Pos* formula $\phi \stackrel{\mathrm{def}}{=} (x \vee y)$, both $\mathrm{ind}_\phi(x, y)$ and $\mathrm{or\_lin}_\phi(x, y)$ satisfy the conditions in Definition 4. Note that from ϕ we cannot infer that x is definitely linear and neither that y is definitely linear.

The abstract variable projection function proj: $(H \times P) \times VI \to H \times P$, *for any* $\langle h, p\rangle \in H \times P$ *and* $x \in VI$, *is given by*

$$\operatorname{proj}\bigl(\langle h, p\rangle, x\bigr) \stackrel{\text{def}}{=} \bigl\langle \operatorname{proj}_H(h, x), \operatorname{proj}_P(p, x)\bigr\rangle.$$

As a consequence, as far as the H component is concerned, the correctness of the projection function does not depend on the assumption on proj_P as specified in Definition 8.

THEOREM 21. *Let* $x \in VI$, $h \in H$ *and* $\sigma \in \gamma_H(h)$. *Then*

$$\tau \in \exists x \mathrel{.} \{\sigma\} \implies \tau \in \gamma_H\bigl(\operatorname{proj}_H(h, x)\bigr).$$

Several abstract domains for sharing analysis can be used to implement the parameter component P. As a basic implementation, one could consider the well-known set-sharing domain of Jacobs and Langen [44]. In such a case, most of the required correctness results have already been established in [40]. Note however that, since no freeness and linearity information is recorded in the plain set-sharing domain, some of the predicates of Definition 8 need to be grossly approximated. For instance, the predicate gfree_p will provide useful information only when applied to an argument that is known to be definitely ground. Another possibility would be to use the domain based on pair-sharing, definite groundness and definite linearity described in [48]. A more precise choice is constituted by the *SFL* domain (an acronym standing from Set-sharing plus Freeness plus Linearity) introduced in [42, 64]. Even in this case, all the non-trivial correctness results have already been proved. In particular, in [41, 64] it is shown that the abstraction function satisfies the requirement of Definition 7 and that the abstract unification operator is correct with respect to rational-tree unification. In order to better highlight the generality of our specification of the sharing component P, the instantiation of P to *SFL* is presented in Appendix A. Notice that the quest for more precision does not end with *SFL*: a number of possible precision improvements are presented and discussed in [6].

5. FINITE-TREE DEPENDENCIES

The precision of the finite-tree analysis based on $H \times P$ is highly dependent on the precision of the generic component P. As explained before, the information provided by P on groundness, freeness, linearity, and sharing of variables is exploited, in the combination $H \times P$, to circumscribe as much as possible the creation and propagation of cyclic terms. However, finite-tree analysis can also benefit from other kinds of relational information. In particular, we now show how *finite-tree dependencies* allow a positive propagation of finiteness information.

Let us consider the finite terms $t_1 = f(x)$, $t_2 = g(y)$, and $t_3 = h(x, y)$: it is clear that, for each assignment of rational terms to x and y, t_3 is finite if and only if t_1 and t_2 are so. We can capture this by the Boolean formula $t_3 \leftrightarrow (t_1 \wedge t_2)$.[11] The reasoning is based on the following facts:

1. t_1, t_2, and t_3 are finite terms, so that the finiteness of their instances depends only on the finiteness of the terms that take the place of x and y.

[11] The introduction of such Boolean formulas, called *dependency formulas*, is originally due to P. W. Dart [30].

2. $\mathrm{vars}(t_3) \supseteq \mathrm{vars}(t_1) \cup \mathrm{vars}(t_2)$, that is, t_3 *covers* both t_1 and t_2; this means that, if an assignment to the variables of t_3 produces a finite instance of t_3, that very assignment will necessarily result in finite instances of t_1 and t_2. Conversely, an assignment producing non-finite instances of t_1 or t_2 will forcibly result in a non-finite instance of t_3.

3. Similarly, t_1 and t_2, taken together, cover t_3.

The important point to notice is that this dependency will keep holding for any further simultaneous instantiation of t_1, t_2, and t_3. In other words, such dependencies are preserved by forward computations (which proceed by consistently instantiating program variables).

Consider $x \mapsto t \in \mathit{Bind}$ where $t \in \mathit{HTerms}$ and $\mathrm{vars}(t) = \{y_1, \dots, y_n\}$. After this binding has been successfully applied, the destinies of x and t concerning term-finiteness are tied together: forever. This tie can be described by the dependency formula

$$x \leftrightarrow (y_1 \wedge \cdots \wedge y_n), \tag{2}$$

meaning that x will be bound to a finite term if and only if y_i is bound to a finite term, for each $i = 1, \dots, n$. While the dependency expressed by (2) is a correct description of any computation state following the application of the binding $x \mapsto t$, it is not as precise as it could be. Suppose that x and y_k are indeed the same variable. Then (2) is logically equivalent to

$$x \rightarrow (y_1 \wedge \cdots \wedge y_{k-1} \wedge y_{k+1} \wedge \cdots \wedge y_n). \tag{3}$$

Although this is correct —whenever x is bound to a finite term, all the other variables will be bound to finite terms— it misses the point that x has just been bound, irrevocably, to a non-finite term: no forward computation can change this. Thus, the implication (3) holds vacuously. A more precise and correct description for the state of affairs caused by the cyclic binding is, instead, the negated atom $\neg x$, whose intuitive reading is "x is not (and never will be) finite."

We are building an abstract domain for finite-tree dependencies where we are making the deliberate choice of including only information that cannot be withdrawn by forward computations. The reason for this choice is that we want the concrete constraint accumulation process to be paralleled, at the abstract level, by another constraint accumulation process: logical conjunction of Boolean formulas. For this reason, it is important to distinguish between *permanent* and *contingent* information. Permanent information, once established for a program point p, maintains its validity in all points that follow p in any forward computation. Contingent information, instead, does not carry its validity beyond the point where it is established. An example of contingent information is given by the h component of $H \times P$: having $x \in h$ in the description of some program point means that x is definitely bound to a finite term *at that point*; nothing is claimed about the finiteness of x at later program points and, in fact, unless x is ground, x can still be bound to a non-finite term. However, if at some program point x is finite and ground, then x will remain finite. In this case we will ensure our Boolean dependency formula entails the positive atom x.

At this stage, we already know something about the abstract domain we are designing. In particular, we have positive and negated atoms, the requirement of describing program predicates of any arity implies that arbitrary conjunctions of these atomic formulas must be allowed and, finally, it is not difficult to observe that the merge-over-all-paths operation [26] will be logical disjunction, so that the domain will have to be closed under this operation. This means that the carrier of our domain must be able to express any Boolean function: *Bfun* is the carrier.

DEFINITION 22. **(**$\gamma_F \colon \mathit{Bfun} \to \wp(\mathit{RSubst})$**.)** *The function* $\mathrm{hval} \colon \mathit{RSubst} \to \mathit{Bval}$ *is defined, for each* $\sigma \in \mathit{RSubst}$ *and each* $x \in \mathit{VI}$, *by*

$$\mathrm{hval}(\sigma)(x) = 1 \quad \overset{\mathrm{def}}{\iff} \quad x \in \mathrm{hvars}(\sigma).$$

The concretization function $\gamma_F \colon \mathit{Bfun} \to \wp(\mathit{RSubst})$ *is defined, for* $\phi \in \mathit{Bfun}$, *by*

$$\gamma_F(\phi) \overset{\mathrm{def}}{=} \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \forall \tau \in {\downarrow}\sigma : \phi\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\}.$$

The domain of positive Boolean functions *Pos* used, among other things, for groundness analysis is so popular that our use of the domain *Bfun* deserves some further comments. For the representation of finite-tree dependencies, the presence in the domain of negative functions such as $\neg x$, meaning that x is bound to an infinite term, is an important feature. One reason why it is so is that knowing about definite non-finiteness can improve the information on definite finiteness. The easiest example goes as follows: if we know that either x or y is finite (i.e., $x \vee y$) and we know that x is *not* finite (i.e., $\neg x$), then we can deduce that y must be finite (i.e., y). It is important to observe that this reasoning can be applied, verbatim, to groundness: a knowledge of non-groundness may improve groundness information. The big difference is that non-finiteness is information of the permanent kind while non-groundness is only contingent. As a consequence, a knowledge of finiteness and non-finiteness can be monotonically accumulated along computation paths by computing the logical conjunction of Boolean formulae. An approach where groundness and non-groundness information is represented by elements of *Bfun* would need to use a much more complex operation and significant extra information to correctly model the constraint accumulation process.

The other reason why the presence of negative functions in the domain is beneficial is efficiency. The most efficient implementations of *Pos* and *Bfun*, such as the ones described in [1, 5], are based on Reduced Ordered Binary Decision Diagrams (ROBDD) [10]. While an ROBDD representing the imprecise information given by the formula (3) has a worst case complexity that is exponential in n, the more precise formula $\neg x$ has constant complexity.

The following theorem shows how most of the operators needed to compute the concrete semantics of a logic program can be correctly approximated on the abstract domain *Bfun*. Notice how the addition of equations is modeled by logical conjunction and projection of a variable is modeled by existential quantification.

THEOREM 23. *Let* $\Sigma, \Sigma_1, \Sigma_2 \in \wp(\mathit{RSubst})$ *and* $\phi, \phi_1, \phi_2 \in \mathit{Bfun}$ *be such that* $\gamma_F(\phi) \supseteq \Sigma$, $\gamma_F(\phi_1) \supseteq \Sigma_1$, *and* $\gamma_F(\phi_2) \supseteq \Sigma_2$. *Let also* $(x \mapsto t) \in \mathit{Bind}$, *where* $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. *Then the following hold:*

$$\gamma_F\Bigl(x \leftrightarrow \bigwedge \mathrm{vars}(t)\Bigr) \supseteq \bigl\{\{x \mapsto t\}\bigr\}; \tag{23a}$$

$$\gamma_F(\neg x) \supseteq \bigl\{\{x \mapsto t\}\bigr\}, \ \text{if } x \in \mathrm{vars}(t); \tag{23b}$$

$$\gamma_F(x) \supseteq \bigl\{\, \sigma \in \mathit{RSubst} \bigm| x \in \mathrm{gvars}(\sigma) \cap \mathrm{hvars}(\sigma) \,\bigr\}; \tag{23c}$$

$$\gamma_F(\phi_1 \wedge \phi_2) \supseteq \bigl\{\, \mathrm{mgs}(\sigma_1 \cup \sigma_2) \bigm| \sigma_1 \in \Sigma_1, \sigma_2 \in \Sigma_2 \,\bigr\}; \tag{23d}$$

$$\gamma_F(\phi_1 \vee \phi_2) \supseteq \Sigma_1 \cup \Sigma_2; \tag{23e}$$

$$\gamma_F(\exists x \mathrel{.} \phi) \supseteq \exists\, x \mathrel{.} \Sigma. \tag{23f}$$

Cases (23a), (23b), and (23d) of Theorem 23 ensure that the following definition of amgu_F provides a correct approximation on *Bfun* of the concrete unification of rational trees.

DEFINITION 24. *The function* $\mathrm{amgu}_F \colon \mathit{Bfun} \times \mathit{Bind} \to \mathit{Bfun}$ *captures the effects of a binding on a finite-tree dependency formula. Let* $\phi \in \mathit{Bfun}$ *and* $(x \mapsto t) \in \mathit{Bind}$ *be such that* $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. *Then*

$$\mathrm{amgu}_F(\phi, x \mapsto t) \stackrel{\mathrm{def}}{=} \begin{cases} \phi \wedge \bigl(x \leftrightarrow \bigwedge \mathrm{vars}(t)\bigr), & \text{if } x \notin \mathrm{vars}(t); \\ \phi \wedge \neg x, & \text{otherwise.} \end{cases}$$

Other semantic operators, such as the consistent renaming of variables, are very simple and omitted for the sake of brevity.

The next result shows how finite-tree dependencies may improve the finiteness information encoded in the h component of the domain $H \times P$.

THEOREM 25. *Let* $h \in H$ *and* $\phi \in \mathit{Bfun}$. *Let also* $h' \stackrel{\mathrm{def}}{=} \mathrm{true}\Bigl(\phi \wedge \bigwedge h\Bigr)$. *Then*

$$\gamma_H(h) \cap \gamma_F(\phi) = \gamma_H(h') \cap \gamma_F(\phi).$$

EXAMPLE 26. *Consider the following program, where it is assumed that the only "external" query is '*`?- r(X, Y)`*':*

```
p(X, Y) :- X = f(Y, _).
q(X, Y) :- X = f(_, Y).
r(X, Y) :- p(X, Y), q(X, Y), acyclic_term(X).
```

Then the predicate `p/2` *in the clause defining* `r/2` *will called with* `X` *and* `Y` *both unbound. Computing on the abstract domain* $H \times P$ *gives us the finiteness description* $h_p = \{x, y\}$, *expressing the fact that both* `X` *and* `Y` *are bound to finite terms. Computing on the finite-tree dependencies domain Bfun, gives us the Boolean formula* $\phi_p = x \to y$ *(*`Y` *is finite if* `X` *is so).*

Considering now the call to the predicate `q/2`, *we note that, since variable* `X` *is already bound to a non-variable term sharing with* `Y`, *all the finiteness information encoded by* H *will be lost (i.e.,* $h_q = \varnothing$*). So, both* `X` *and* `Y` *are detected as possibly cyclic. However, the finite-tree dependency information is preserved, since we have* $\phi_q = (x \to y) \wedge (x \to y) = x \to y$.

Finally, consider the effect of the abstract evaluation of `acyclic_term(X)`. *On the* $H \times P$ *domain we can only infer that variable* `X` *cannot be bound to an infinite term, while* `Y` *will be still considered as possibly cyclic, so that* $h_r = \{x\}$. *On the domain Bfun we can just confirm that the finite-tree dependency computed so far still holds, so that* $\phi_r = x \to y$ *(no stronger finite-tree dependency can be inferred, since the finiteness of* `X` *is only contingent). Thus, by applying the result of* Theorem 25, *we can recover the finiteness of* `Y`*:*

$$h'_r = \mathrm{true}\Bigl(\phi_r \wedge \bigwedge h_r\Bigr) = \mathrm{true}\bigl((x \to y) \wedge x\bigr) = \mathrm{true}(x \wedge y) = \{x, y\}.$$

Information encoded in $H \times P$ and *Bfun* is not completely orthogonal and the following result provides a kind of consistency check.

THEOREM 27. *Let* $h \in H$ *and* $\phi \in \mathit{Bfun}$. *Then*

$$\gamma_H(h) \cap \gamma_F(\phi) \neq \varnothing \quad \Longrightarrow \quad h \cap \mathrm{false}(\phi) = \varnothing.$$

Note however that, provided the abstract operators are correct, the computed descriptions will always be mutually consistent, unless $\phi = \bot$.

6. GROUNDNESS DEPENDENCIES

Since information about the groundness of variables is crucial for many applications, it is natural to consider a static analysis domain including both a finite-tree and a groundness component. In fact, any reasonably precise implementation of the parameter component P of the abstract domain specified in Section 4 will include some kind of groundness information.[12] We highlight similarities, differences and connections relating the domain *Bfun* for finite-tree dependencies to the abstract domain *Pos* for groundness dependencies. Note that these results also hold when considering a combination of *Bfun* with the groundness domain *Def* [1].

We first define how elements of *Pos* represent sets of substitutions in rational solved form.

Definition 28. **($\gamma_G \colon \mathit{Pos} \to \wp(\mathit{RSubst})$.)** *The function* gval: $\mathit{RSubst} \to \mathit{Bval}$ *is defined as follows, for each $\sigma \in \mathit{RSubst}$ and each $x \in \mathit{VI}$:*

$$\mathrm{gval}(\sigma)(x) = 1 \quad \stackrel{\mathrm{def}}{\iff} \quad x \in \mathrm{gvars}(\sigma).$$

The concretization function $\gamma_G \colon \mathit{Pos} \to \wp(\mathit{RSubst})$ is defined, for each $\psi \in \mathit{Pos}$,

$$\gamma_G(\psi) \stackrel{\mathrm{def}}{=} \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \forall \tau \in {\downarrow}\sigma : \psi\bigl(\mathrm{gval}(\tau)\bigr) = 1 \,\bigr\}.$$

The following is a simple variant of the standard abstract unification operator for groundness analysis over finite-tree domains: the only difference concerns the case of cyclic bindings [2].

Definition 29. *The function* $\mathrm{amgu}_G \colon \mathit{Pos} \times \mathit{Bind} \to \mathit{Pos}$ *captures the effects of a binding on a groundness dependency formula. Let $\psi \in \mathit{Pos}$ and $(x \mapsto t) \in \mathit{Bind}$ be such that $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Then*

$$\mathrm{amgu}_G(\psi, x \mapsto t) \stackrel{\mathrm{def}}{=} \psi \wedge \Bigl(x \leftrightarrow \bigwedge\bigl(\mathrm{vars}(t) \setminus \{x\}\bigr)\Bigr).$$

The next result shows how, by exploiting the finiteness component H, the finite-tree dependencies (*Bfun*) component and the groundness dependencies (*Pos*) component can improve each other.

Theorem 30. *Let $h \in H$, $\phi \in \mathit{Bfun}$ and $\psi \in \mathit{Pos}$. Let also $\phi' \in \mathit{Bfun}$ and $\psi' \in \mathit{Pos}$ be defined as $\phi' = \exists \mathit{VI} \setminus h \,.\, \psi$ and $\psi' = \exists \mathit{VI} \setminus h \,.\, \mathrm{pos}(\phi)$. Then*

$$\gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi) = \gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi \wedge \psi'); \qquad (30a)$$

$$\gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi) = \gamma_H(h) \cap \gamma_F(\phi \wedge \phi') \cap \gamma_G(\psi). \qquad (30b)$$

Moreover, even without any knowledge of the H component, combining Theorem 25 and Eq. (30a), the groundness dependencies component can be improved.

Corollary 31. *Let $\phi \in \mathit{Bfun}$ and $\psi \in \mathit{Pos}$. Then*

$$\gamma_F(\phi) \cap \gamma_G(\psi) = \gamma_F(\phi) \cap \gamma_G\bigl(\psi \wedge \mathrm{true}(\phi)\bigr).$$

[12] One could define P so that it explicitly contains the abstract domain *Pos*. Even when this is not the case, it should be noted that, as soon as the parameter P includes the set-sharing domain of Jacobs and Langen [45], then it will subsume the groundness information captured by the domain *Def* [15, 24].

The following example shows that, when computing on rational trees, finite-tree dependencies may provide groundness information that is not captured by the usual approaches.

EXAMPLE 32. *Consider the program:*

```
p(a, Y).
p(X, a).
q(X, Y) :- p(X, Y), X = f(X, Z).
```

The abstract semantics of `p/2`*, for both finite-tree and groundness dependencies, is* $\phi_p = \psi_p = x \vee y$*. The finite-tree dependency for* `q/2` *is* $\phi_q = (x \vee y) \wedge \neg x = \neg x \wedge y$*. Using* Definition 29*, the groundness dependency for* `q/2` *is*

$$\psi_q = \exists z \,.\, \bigl((x \vee y) \wedge (x \leftrightarrow z)\bigr) = x \vee y.$$

This can be improved, using Corollary 31*, to*

$$\psi'_q = \psi_q \wedge \bigwedge \mathrm{true}(\phi_q) = y.$$

It is worth noticing that the groundness information can be improved regardless of whether, like *Pos*, the groundness domain captures disjunctive information: groundness information represented by the less expressive domain *Def* [1] can be improved as well. The next example illustrates this point.

EXAMPLE 33. *Consider the following program:*

```
p(a, a).
p(X, Y) :- X = f(X, _).
q(X, Y) :- p(X, Y), X = a.
```

Consider first the predicate `p/2`*. Concerning finite-tree dependencies, the abstract semantics of* `p/2` *is expressed by the Boolean formula* $\phi_p = x \rightarrow y$ *(*y *is finite if* x *is so). In contrast, the Pos-groundness abstract semantics of* `p/2` *is a plain "don't know": the Boolean formula* $\psi_p = \top$*. In fact, the groundness of* `X` *and* `Y` *can be completely decided by the call-pattern of* `p/2`*.*

Consider now the predicate `q/2`*. The finiteness semantics of* `q/2` *is given by* $\phi_q = (x \rightarrow y) \wedge x = x \wedge y$*, whereas the Pos formula expressing groundness dependencies is* $\psi_q = \top \wedge x = x$*. By applying the reduction process of* Theorem 80*, we obtain*

$$\psi'_q = \psi_q \wedge \bigwedge \mathrm{true}(\phi_q) = x \wedge y,$$

therefore recovering the groundness of variable y*.*

Since better groundness information, besides being useful in itself, may also improve the precision of many other analyses such as sharing [6, 15], the reduction steps given by Theorem 30 and Corollary 31 can trigger improvements to the precision of other components. Theorem 30 can also be exploited to recover precision after the application of a widening operator on either the groundness dependencies or the finite-tree dependencies component.

7. EXPERIMENTAL RESULTS

The work described here has been experimentally evaluated in the framework provided by the CHINA analyzer [2]. We implemented and compared the three domains Pattern(P), Pattern($H \times P$) and Pattern($\mathit{Bfun} \times H \times P$),[13] where the parameter component P has been instantiated to the domain $\mathit{Pos} \times \mathit{SFL}_2$ [6, 41, 64] for tracking groundness, freeness, linearity and (non-redundant) set-sharing information. The Pattern($\cdot$) operator [3] further upgrades the precision of its argument by adding explicit structural information.

Concerning the *Bfun* component, the implementation was straightforward, since all the techniques described in [5] (and almost all the code, including the widenings) was reused unchanged, obtaining comparable efficiency. As a consequence, most of the implementation effort was in the coding of the abstract operators on the H component and in the reduction processes between the different components. A key choice, in this sense, is 'when' the reduction steps given in Theorems 25 and 30 should be applied. When striving for maximum precision, a trivial strategy is to perform reductions immediately after any application of any abstract operator. This is how predicates like `acyclic_term/1` should be handled: after adding the variables of the argument to the H component, the reduction process is applied to propagate the new information to all domain components. However, such an approach turns out to be unnecessarily inefficient. In fact, the next result shows that Theorems 25 and 30 cannot lead to a precision improvement if applied just after the abstract evaluation of the merge-over-all-paths or the existential quantification operations (provided the initial descriptions are already reduced).

THEOREM 34. *Let $x \in \mathit{VI}$, $h, h' \in H$ $\phi, \phi' \in \mathit{Bfun}$ and $\psi, \psi' \in \mathit{Pos}$. Let*

$$h_1 \stackrel{\mathrm{def}}{=} h \cap h', \qquad \phi_1 \stackrel{\mathrm{def}}{=} \phi \vee \phi', \qquad \psi_1 \stackrel{\mathrm{def}}{=} \psi \vee \psi',$$
$$h_2 \stackrel{\mathrm{def}}{=} \mathrm{proj}_H(h, x), \qquad \phi_2 \stackrel{\mathrm{def}}{=} \exists x \mathrel{.} \phi, \qquad \psi_2 \stackrel{\mathrm{def}}{=} \exists x \mathrel{.} \psi.$$

Let also

$$h \supseteq \mathrm{true}\bigl(\phi \wedge \bigwedge h\bigr), \qquad \phi \models (\exists \mathit{VI} \setminus h \mathrel{.} \psi), \qquad \psi \models \bigl(\exists \mathit{VI} \setminus h \mathrel{.} \mathrm{pos}(\phi)\bigr),$$
$$h' \supseteq \mathrm{true}\bigl(\phi' \wedge \bigwedge h'\bigr), \qquad \phi' \models (\exists \mathit{VI} \setminus h' \mathrel{.} \psi'), \qquad \psi' \models \bigl(\exists \mathit{VI} \setminus h' \mathrel{.} \mathrm{pos}(\phi')\bigr).$$

Then, for $i = 1, 2$,

$$h_i \supseteq \mathrm{true}\bigl(\phi_i \wedge \bigwedge h_i\bigr), \qquad \phi_i \models (\exists \mathit{VI} \setminus h_i \mathrel{.} \psi_i), \qquad \psi_i \models \bigl(\exists \mathit{VI} \setminus h_i \mathrel{.} \mathrm{pos}(\phi_i)\bigr).$$

A goal-dependent analysis was run for all the programs in our benchmark suite and the results (with respect to the precision) are summarized in Table 1. Here, the precision is measured as the percentage of the total number of variables that the analyser can show to be finite. Two alternative views are provided.

In the first view, each column is labeled by an analysis domain and each row is labeled by a precision interval. For instance, the value '31' at the intersection of column 'H' and row '$80 \leq p < 100$' is to be read as "*for 31 benchmarks, the percentage p of the total number of variables that the analyzer can show to be finite using the domain H is between 80% and 100%.*"

[13] For ease of notation, the domain names are shortened to P, H and Bfun, respectively.

Prec. class	P	H	Bfun
$p = 100$	2	84	86
$80 \leq p < 100$	1	31	36
$60 \leq p < 80$	7	26	23
$40 \leq p < 60$	6	41	40
$20 \leq p < 40$	47	47	46
$0 \leq p < 20$	185	19	17

Prec. improvement	P $\rightarrow$ H	H $\rightarrow$ Bfun
$i > 20$	185	4
$10 < i \leq 20$	31	3
$5 < i \leq 10$	11	6
$2 < i \leq 5$	4	10
$0 < i \leq 2$	2	24
no improvement	15	201

TABLE 1: The precision on finite variables when using P, H and Bfun.

The second view provides a better picture of the precision *improvements* obtained when moving from P to H (in the column 'P $\rightarrow$ H') and from H to Bfun (in the column 'H $\rightarrow$ Bfun'). For instance, the value '10' at the intersection of column 'H $\rightarrow$ Bfun' and row '$2 < i \leq 5$' is to be read as "*when moving from H to Bfun, for 10 benchmarks the improvement i in the percentage of the total number of variables shown to be finite was between 2% and 5%.*"

It can be seen from Table 1 that, even though the H domain is remarkably precise, the inclusion of the *Bfun* component allows for a further, and sometimes significant, precision improvement for a number of benchmarks. It is worth noting that the current implementation of CHINA does not yet fully exploit the finite-tree dependencies arising when evaluating many of the built-in predicates, therefore incurring an avoidable precision loss. We are working on this issue and we expect that the specialized implementation of the abstract evaluation of some built-ins will result in more and better precision improvements. The experimentation has also shown that, in practice, the Bfun domain does not improve the groundness information.

8. CONCLUSION

Several modern logic-based languages offer a computation domain based on rational trees. On the one hand, the use of such trees is encouraged by the possibility of using efficient and correct unification algorithms and by an increase in expressivity. On the other hand, these gains are countered by the extra problems rational trees bring with themselves and that can be summarized as follows: several built-ins, library predicates, program analysis and manipulation techniques are only well-defined for program fragments working with finite trees.

As a consequence, those applications that exploit rational trees tend to do so in a very controlled way, that is, most program variables can only be bound to finite terms. By detecting the program variables that may be bound to infinite terms with a good degree of accuracy, we can significantly reduce the disadvantages of using rational trees.

In this paper we have proposed an abstract-interpretation based solution to this problem, where the composite abstract domain $H \times P$ allows to track the creation and propagation of infinite terms. Even though this information is crucial to any finite-tree analysis, propagating the guarantees of finiteness that come from several built-ins (including those that are explicitly provided to test term-finiteness) is also important. Therefore, we have introduced a domain of Boolean functions *Bfun* for finite-tree dependencies which, when coupled to the domain $H \times P$, can enhance its expressive power. Since *Bfun* has many similarities with the domain *Pos* used for groundness analysis, we have investigated how these two domains relate to each other and, in particular, the synergy arising from their combination in the "global" domain of analysis.

REFERENCES

[1] T. Armstrong, K. Marriott, P. Schachte, and H. Søndergaard. Two classes of Boolean functions for dependency analysis. *Science of Computer Programming*, 31(1):3–45, 1998.

[2] R. Bagnara. *Data-Flow Analysis for Constraint Logic-Based Languages*. PhD thesis, Dipartimento di Informatica, Università di Pisa, Pisa, Italy, 1997. Printed as Report TD-1/97.

[3] R. Bagnara, P. M. Hill, and E. Zaffanella. Efficient structural information analysis for real CLP languages. In M. Parigot and A. Voronkov, editors, *Proceedings of the 7th International Conference on Logic for Programming and Automated Reasoning (LPAR 2000)*, volume 1955 of *Lecture Notes in Artificial Intelligence*, pages 189–206, Réunion Island, France, 2000. Springer-Verlag, Berlin.

[4] R. Bagnara, P. M. Hill, and E. Zaffanella. Set-sharing is redundant for pair-sharing. *Theoretical Computer Science*, 2002. To appear.

[5] R. Bagnara and P. Schachte. Factorizing equivalent variable pairs in ROBDD-based implementations of *Pos*. In A. M. Haeberer, editor, *Proceedings of the "Seventh International Conference on Algebraic Methodology and Software Technology (AMAST'98)"*, volume 1548 of *Lecture Notes in Computer Science*, pages 471–485, Amazonia, Brazil, 1999. Springer-Verlag, Berlin.

[6] R. Bagnara, E. Zaffanella, and P. M. Hill. Enhanced sharing analysis techniques: A comprehensive evaluation. In M. Gabbrielli and F. Pfenning, editors, *Proceedings of the 2nd International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming*, pages 103–114, Montreal, Canada, 2000. Association for Computing Machinery.

[7] R. Bagnara, E. Zaffanella, and P. M. Hill. Enhanced sharing analysis techniques: A comprehensive evaluation. Submitted for publication. Available at `http://www.cs.unipr.it/~bagnara/`, 2001.

[8] A. Berarducci and M. Venturini Zilli. Generalizations of unification. *Journal of Symbolic Computation*, 15:479–491, 1993.

[9] M. Bruynooghe, M. Codish, and A. Mulkers. Abstract unification for a composite domain deriving sharing and freeness properties of program variables. In F. S. de Boer and M. Gabbrielli, editors, *Verification and Analysis of Logic Languages, Proceedings of the W2 Post-Conference Workshop, International Conference on Logic Programming*, pages 213–230, Santa Margherita Ligure, Italy, 1994.

[10] R. E. Bryant. Symbolic boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.

[11] J. A. Campbell, editor. *Implementations of Prolog*. Ellis Horwood/Halsted Press/Wiley, 1984.

[12] B. Carpenter. *The Logic of Typed Feature Structures with Applications to Unification-based Grammars, Logic Programming and Constraint Resolution*, volume 32 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, New York, 1992.

[13] K. L. Clark. Negation as failure. In H. Gallaire and J. Minker, editors, *Logic and Databases*, pages 293–322, Toulouse, France, 1978. Plenum Press.

[14] M. Codish, D. Dams, and E. Yardeni. Derivation and safety of an abstract unification algorithm for groundness and aliasing analysis. In K. Furukawa, editor, *Logic Programming: Proceedings of the Eighth International Conference on Logic Programming*, MIT Press Series in Logic Programming, pages 79–93, Paris, France, 1991. The MIT Press.

[15] M. Codish, H. Søndergaard, and P. J. Stuckey. Sharing and groundness dependencies in logic programs. *ACM Transactions on Programming Languages and Systems*, 21(5):948–976, 1999.

[16] M. Codish and C. Taboch. A semantic basis for termination analysis of logic programs and its realization using symbolic norm constraints. In M. Hanus, J. Heering, and K. Meinke, editors, *Algebraic and Logic Programming, 6th International Joint Conference*, volume 1298 of *Lecture Notes in Computer Science*, pages 31–45, Southampton, U.K., 1997. Springer-Verlag, Berlin.

[17] M. Codish and C. Taboch. A semantic basis for the termination analysis of logic programs. *Journal of Logic Programming*, 41(1):103–123, 1999.

[18] A. Colmerauer. Prolog and infinite trees. In K. L. Clark and S. Å. Tärnlund, editors, *Logic Programming, APIC Studies in Data Processing*, volume 16, pages 231–251. Academic Press, New York, 1982.

[19] A. Colmerauer. Equations and inequations on finite and infinite trees. In *Proceedings of the International Conference on Fifth Generation Computer Systems (FGCS'84)*, pages 85–99, Tokyo, Japan, 1984. ICOT.

[20] A. Colmerauer. An introduction to Prolog-III. *Communications of the ACM*, 33(7):69–90, 1990.

[21] A. Cortesi, B. Le Charlier, and S. Rossi. Specification-based automatic verification of Prolog programs. In J. P. Gallagher, editor, *Logic Programming Synthesis and Transformation: Proceedings of the 6th International Workshop*,

volume 1207 of *Lecture Notes in Computer Science*, pages 38–57, Stockholm, Sweden, 1997. Springer-Verlag, Berlin.

[22] A. Cortesi and G. Filé. Sharing is optimal. *Journal of Logic Programming*, 38(3):371–386, 1999.

[23] A. Cortesi, G. Filé, and W. Winsborough. *Prop* revisited: Propositional formula as abstract domain for groundness analysis. In *Proceedings, Sixth Annual IEEE Symposium on Logic in Computer Science*, pages 322–327, Amsterdam, The Netherlands, 1991. IEEE Computer Society Press.

[24] A. Cortesi, G. Filé, and W. Winsborough. The quotient of an abstract interpretation for comparing static analyses. *Theoretical Computer Science*, 202(1&2):163–192, 1998.

[25] A. Cortesi, B. Le Charlier, and P. Van Hentenryck. Combinations of abstract domains for logic programming: Open product and generic pattern construction. *Science of Computer Programming*, 38(1–3):27–71, 2000.

[26] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of the Fourth Annual ACM Symposium on Principles of Programming Languages*, pages 238–252, 1977.

[27] P. Cousot and R. Cousot. Abstract interpretation and applications to logic programs. *Journal of Logic Programming*, 13(2&3):103–179, 1992.

[28] P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of Logic and Computation*, 2(4):511–547, 1992.

[29] L. Crnogorac, A. D. Kelly, and H. Søndergaard. A comparison of three occur-check analysers. In R. Cousot and D. A. Schmidt, editors, *Static Analysis: Proceedings of the 3rd International Symposium*, volume 1145 of *Lecture Notes in Computer Science*, pages 159–173, Aachen, Germany, 1996. Springer-Verlag, Berlin.

[30] P. W. Dart. On derived dependencies and connected databases. *Journal of Logic Programming*, 11(1&2):163–188, 1991.

[31] S. Debray and N.-W. Lin. Cost analysis of logic programs. *ACM Transactions on Programming Languages and Systems*, 15(5):826–875, 1993.

[32] P. R. Eggert and K. P. Chow. Logic programming, graphics and infinite terms. Technical Report UCSB DoCS TR 83-02, Department of Computer Science, University of California at Santa Barbara, 1983.

[33] G. Erbach. ProFIT: Prolog with Features, Inheritance and Templates. In *Proceedings of the 7th Conference of the European Chapter of the Association for Computational Linguistics*, pages 180–187, Dublin, Ireland, 1995.

[34] M. Filgueiras. A Prolog interpreter working with infinite terms. In Campbell [11], pages 250–258.

[35] F. Giannesini and J. Cohen. Parser generation and grammar manipulation using Prolog's infinite trees. *Journal of Logic Programming*, 3:253–265, 1984.

[36] W. Hans and S. Winkler. Aliasing and groundness analysis of logic programs through abstract interpretation and its safety. Technical Report 92–27, Technical University of Aachen (RWTH Aachen), 1992.

[37] S. Haridi and D. Sahlin. Efficient implementation of unification of cyclic structures. In Campbell [11], pages 234–249.

[38] M. Hermenegildo, F. Bueno, G. Puebla, and P. López. Program analysis, debugging, and optimization using the ciao system preprocessor. In D. De Schreye, editor, *Logic Programming: The 1999 International Conference*, MIT Press Series in Logic Programming, pages 52–66, Las Cruces, New Mexico, 1999. The MIT Press.

[39] P. M. Hill, R. Bagnara, and E. Zaffanella. The correctness of set-sharing. In G. Levi, editor, *Static Analysis: Proceedings of the 5th International Symposium*, volume 1503 of *Lecture Notes in Computer Science*, pages 99–114, Pisa, Italy, 1998. Springer-Verlag, Berlin.

[40] P. M. Hill, R. Bagnara, and E. Zaffanella. Soundness, idempotence and commutativity of set-sharing. *Theory and Practice of Logic Programming*, 2(2):155–201, 2002.

[41] P. M. Hill, E. Zaffanella, and R. Bagnara. A correct, precise and efficient integration of set-sharing, freeness and linearity for the analysis of finite and rational tree languages. Submitted for publication. Available at `http://www.cs.unipr.it/~bagnara/`.

[42] P. M. Hill, E. Zaffanella, and R. Bagnara. A correct, precise and efficient integration of set-sharing, freeness and linearity for the analysis of finite and rational tree languages. Quaderno 273, Dipartimento di Matematica, Università di Parma, 2001. Available at `http://www.cs.unipr.it/Publications/`. Also published as technical report No. 2001.22, School of Computing, University of Leeds, U.K.

[43] ISO/IEC. *ISO/IEC 13211-1: 1995 Information technology — Programming languages — Prolog — Part 1: General core*. International Standard Organization, 1995.

[44] D. Jacobs and A. Langen. Accurate and efficient approximation of variable aliasing in logic programs. In E. L. Lusk and R. A. Overbeek, editors, *Logic Programming: Proceedings of the North American Conference*, MIT Press Series in Logic Programming, pages 154–165, Cleveland, Ohio, USA, 1989. The MIT Press.

[45] D. Jacobs and A. Langen. Static analysis of logic programs for independent AND parallelism. *Journal of Logic Programming*, 13(2&3):291–314, 1992.

[46] J. Jaffar, J-L. Lassez, and M. J. Maher. Prolog-II as an instance of the logic programming scheme. In M. Wirsing, editor, *Formal Descriptions of Programming Concepts III*, pages 275–299. North-Holland, 1987.

[47] T. Keisu. *Tree Constraints*. PhD thesis, The Royal Institute of Technology, Stockholm, Sweden, May 1994. Also available in the SICS Dissertation Series: SICS/D–16–SE.

[48] A. King. Pair-sharing over rational trees. *Journal of Logic Programming*, 46(1–2):139–155, 2000.

[49] N. Lindenstrauss, Y. Sagiv, and A. Serebrenik. TermiLog: A system for checking termination of queries to logic programs. In O. Grumberg, editor, *Computer Aided Verification: Proceedings of the 9th International Conference*, volume 1250 of *Lecture Notes in Computer Science*, pages 444–447, Haifa, Israel, 1997. Springer-Verlag, Berlin.

[50] M. J. Maher. Complete axiomatizations of the algebras of finite, rational and infinite trees. In *Proceedings, Third Annual Symposium on Logic in Computer Science*, pages 348–357, Edinburgh, Scotland, 1988. IEEE Computer Society.

[51] K. Marriott and H. Søndergaard. Notes for a tutorial on abstract interpretation of logic programs. North American Conference on Logic Programming, Cleveland, Ohio, USA, 1989.

[52] K. Marriott and H. Søndergaard. Precise and efficient groundness analysis for logic programs. *ACM Letters on Programming Languages and Systems*, 2(1–4):181–196, 1993.

[53] K. Mukai. *Constraint Logic Programming and the Unification of Information.* PhD thesis, Department of Computer Science, Faculty of Engineering, Tokio Institute of Technology, 1991.

[54] U. Neumerkel and F. Mesnard. Localizing and explaining reasons for non-terminating logic programs with failure-slices. In G. Nadathur, editor, *Principles and Practice of Declarative Programming*, volume 1702 of *Lecture Notes in Computer Science*, pages 328–341, Paris, France, 1999. Springer-Verlag, Berlin.

[55] C. Pollard and I. A. Sag. *Head-Driven Phrase Structure Grammar.* University of Chicago Press, Chicago, 1994.

[56] V. Santos Costa, L. Damas, R. Reis, and R. Azevedo. *YAP User's Manual.* Universidade do Porto, version 4.3.20 edition, 2001.

[57] E. Schröder. *Der Operationskreis des Logikkalkuls.* B. G. Teubner, Leibzig, 1877.

[58] F. Scozzari. Abstract domains for sharing analysis by optimal semantics. In J. Palsberg, editor, *Static Analysis: 7th International Symposium, SAS 2000*, volume 1824 of *Lecture Notes in Computer Science*, pages 397–412, Santa Barbara, CA, USA, 2000. Springer-Verlag, Berlin.

[59] Gert Smolka and Ralf Treinen. Records for logic programming. *Journal of Logic Programming*, 18(3):229–258, 1994.

[60] H. Søndergaard. An application of abstract interpretation of logic programs: Occur check reduction. In B. Robinet and R. Wilhelm, editors, *Proceedings of the 1986 European Symposium on Programming*, volume 213 of *Lecture Notes in Computer Science*, pages 327–338. Springer-Verlag, Berlin, 1986.

[61] R. F. Stärk. Total correctness of pure Prolog programs: A formal approach. In R. Dyckhoff, H. Herre, and P. Schroeder-Heister, editors, *Extensions of Logic Programming: Proceedings of the 5th International Workshop*, volume 1050 of *Lecture Notes in Computer Science*, pages 237–254, Leipzig, Germany, 1996. Springer-Verlag, Berlin.

[62] R. F. Stärk. The theoretical foundations of LPTP (a Logic Program Theorem Prover). *Journal of Logic Programming*, 36(3):241–269, 1998.

[63] Swedish Institute of Computer Science, Intelligent Systems Laboratory. *SICStus Prolog User's Manual*, release 3.9 edition, 2002.

[64] E. Zaffanella. *Correctness, Precision and Efficiency in the Sharing Analysis of Real Logic Languages*. PhD thesis, School of Computing, University of Leeds, Leeds, U.K., 2001. Available at `http://www.cs.unipr.it/~zaffanella/`.

[65] E. Zaffanella, P. M. Hill, and R. Bagnara. Decomposing non-redundant sharing by complementation. *Theory and Practice of Logic Programming*, 2(2):233–261, 2002.

APPENDIX A: AN INSTANCE OF THE PARAMETER DOMAIN P

As discussed in Section 4, several abstract domains for sharing analysis can be used to implement the parameter component P. We here consider the abstract domain *SFL* [41, 64], integrating the set-sharing domain of Jacobs and Langen with definite freeness and linearity information.

Definition 35. **(The set-sharing domain SH.)** *The set SH is defined by $SH \stackrel{\mathrm{def}}{=} \wp(SG)$, where $SG \stackrel{\mathrm{def}}{=} \wp(VI) \setminus \{\varnothing\}$ is the set of* sharing groups*. SH is ordered by subset inclusion.*

The information about definite freeness and linearity is encoded by two sets of variables, one for each property.

Definition 36. **(The domain *SFL*.)** *Let $F \stackrel{\mathrm{def}}{=} \wp(VI)$ and $L \stackrel{\mathrm{def}}{=} \wp(VI)$ be partially ordered by reverse subset inclusion. The domain SFL is defined by the Cartesian product $SFL \stackrel{\mathrm{def}}{=} SH \times F \times L$ ordered by '$\leq_S$', the component-wise extension of the orderings defined on the sub-domains; the bottom element is $\bot_S \stackrel{\mathrm{def}}{=} \langle \varnothing, VI, VI \rangle$.*

In the next definition we introduce a few well-known operations on the set-sharing domain SH. These will be used to define the operations on the domain *SFL*.

Definition 37. **(Abstract operators on SH.)** *For each $sh \in SH$ and each $V \subseteq VI$, the extraction of the* relevant component *of sh* with respect to V *is given by the function* $\mathrm{rel}\colon \wp(VI) \times SH \to SH$ *defined as*

$$\mathrm{rel}(V, sh) \stackrel{\mathrm{def}}{=} \{\, S \in sh \mid S \cap V \neq \varnothing \,\}.$$

For each $sh \in SH$ and each $V \subseteq VI$, the function $\overline{\mathrm{rel}}\colon \wp(VI) \times SH \to SH$ gives the irrelevant component *of sh* with respect to V*. It is defined as*

$$\overline{\mathrm{rel}}(V, sh) \stackrel{\mathrm{def}}{=} sh \setminus \mathrm{rel}(V, sh).$$

The function $(\cdot)^\star \colon SH \to SH$*, called* star-union*, is given, for each* $sh \in SH$*, by*

$$sh^\star \stackrel{\text{def}}{=} \left\{ S \in SG \;\middle|\; \exists n \geq 1 \mathrel{.} \exists T_1, \ldots, T_n \in sh \mathrel{.} S = \bigcup_{i=1}^{n} T_i \right\}.$$

For each $sh_1, sh_2 \in SH$*, the function* $\mathrm{bin} \colon SH \times SH \to SH$*, called* binary union*, is given by*

$$\mathrm{bin}(sh_1, sh_2) \stackrel{\text{def}}{=} \{\, S_1 \cup S_2 \mid S_1 \in sh_1, S_2 \in sh_2 \,\}.$$

For each $sh \in SH$ *and each* $(x \mapsto t) \in \mathit{Bind}$*, the function* $\mathrm{cyclic}_x^t \colon SH \to SH$ *strengthens the sharing set sh by forcing the coupling of x with t:*

$$\mathrm{cyclic}_x^t(sh) \stackrel{\text{def}}{=} \overline{\mathrm{rel}}\bigl(\{x\} \cup \mathrm{vars}(t), sh\bigr) \cup \mathrm{rel}\bigl(\mathrm{vars}(t) \setminus \{x\}, sh\bigr).$$

For each $sh \in SH$ *and each* $x \in \mathit{VI}$*, the function* $\mathrm{proj}_{SH} \colon SH \times \mathit{VI} \to SH$ *projects away variable x from sh:*

$$\mathrm{proj}_{SH}(sh, x) \stackrel{\text{def}}{=} \bigl\{\{x\}\bigr\} \cup \bigl\{\, S \setminus \{x\} \bigm| S \in sh, S \neq \{x\} \,\bigr\}.$$

It is now possible to define the implementation, on the domain *SFL*, of all the predicates and functions specified in Definition 8.

DEFINITION 38. **(Abstract operators on *SFL*.)** *For each* $d \in \mathit{SFL}$ *and* $s, t \in \mathit{HTerms}$*, where* $d = \langle sh, f, l \rangle$ *and* $\mathrm{vars}(s) \cup \mathrm{vars}(t) \subseteq \mathit{VI}$*, let* $sh_s = \mathrm{rel}\bigl(\mathrm{vars}(s), sh\bigr)$ *and* $sh_t = \mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr)$*. Then*

$$
\begin{aligned}
\mathrm{ind}_d(s,t) &\stackrel{\text{def}}{=} \bigl(sh_s \cap sh_t = \varnothing\bigr);\\
\mathrm{ground}_d(t) &\stackrel{\text{def}}{=} \bigl(\mathrm{vars}(t) \subseteq \mathit{VI} \setminus \mathrm{vars}(sh)\bigr);\\
\mathrm{occ\_lin}_d(y,t) &\stackrel{\text{def}}{=} \mathrm{ground}_d(y) \lor \Bigl(\mathrm{occ\_lin}(y,t) \land (y \in l)\\
&\qquad\qquad \land \forall z \in \mathrm{vars}(t) : \bigl(y \neq z \implies \mathrm{ind}_d(y,z)\bigr)\Bigr);\\
\mathrm{share\_lin}_d(s,t) &\stackrel{\text{def}}{=} \forall y \in \mathrm{vars}(sh_s \cap sh_t) :\\
&\qquad y \in \mathrm{vars}(s) \implies \mathrm{occ\_lin}_d(y,s)\\
&\qquad \land y \in \mathrm{vars}(t) \implies \mathrm{occ\_lin}_d(y,t);\\
\mathrm{free}_d(t) &\stackrel{\text{def}}{=} \exists y \in \mathit{VI} \mathrel{.} (y = t) \land (y \in f);\\
\mathrm{gfree}_d(t) &\stackrel{\text{def}}{=} \mathrm{ground}_d(t) \lor \mathrm{free}_d(t);\\
\mathrm{lin}_d(t) &\stackrel{\text{def}}{=} \forall y \in \mathrm{vars}(t) : \mathrm{occ\_lin}_d(y,t);\\
\mathrm{or\_lin}_d(s,t) &\stackrel{\text{def}}{=} \mathrm{lin}_d(s) \lor \mathrm{lin}_d(t);\\
\mathrm{share\_same\_var}_d(s,t) &\stackrel{\text{def}}{=} \mathrm{vars}(sh_s \cap sh_t);\\
\mathrm{share\_with}_d(t) &\stackrel{\text{def}}{=} \mathrm{vars}(sh_t).
\end{aligned}
$$

The function $\mathrm{amgu}_S \colon \mathit{SFL} \times \mathit{Bind} \to \mathit{SFL}$ *captures the effects of a binding on an element of SFL. Let* $d = \langle sh, f, l \rangle \in \mathit{SFL}$ *and* $(x \mapsto t) \in \mathit{Bind}$*, where* $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$*. Let also*

$$sh' \stackrel{\text{def}}{=} \mathrm{cyclic}_x^t(sh_- \cup sh''),$$

where

$$sh_x \stackrel{\text{def}}{=} \mathrm{rel}\bigl(\{x\}, sh\bigr), \qquad sh_t \stackrel{\text{def}}{=} \mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr),$$
$$sh_{xt} \stackrel{\text{def}}{=} sh_x \cap sh_t, \qquad sh_{-} \stackrel{\text{def}}{=} \overline{\mathrm{rel}}\bigl(\{x\} \cup \mathrm{vars}(t), sh\bigr),$$

$$sh'' \stackrel{\text{def}}{=} \begin{cases} \mathrm{bin}(sh_x, sh_t), & \text{if } \mathrm{free}_d(x) \vee \mathrm{free}_d(t); \\ \mathrm{bin}\bigl(sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^\star), \\ \qquad\qquad sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^\star)\bigr), & \text{if } \mathrm{lin}_d(x) \wedge \mathrm{lin}_d(t); \\ \mathrm{bin}(sh_x^\star, sh_t), & \text{if } \mathrm{lin}_d(x); \\ \mathrm{bin}(sh_x, sh_t^\star), & \text{if } \mathrm{lin}_d(t); \\ \mathrm{bin}(sh_x^\star, sh_t^\star), & \text{otherwise.} \end{cases}$$

Letting $S_x \stackrel{\text{def}}{=} \mathrm{share\_with}_d(x)$ *and* $S_t \stackrel{\text{def}}{=} \mathrm{share\_with}_d(t)$*, we also define*

$$f' \stackrel{\text{def}}{=} \begin{cases} f, & \text{if } \mathrm{free}_d(x) \wedge \mathrm{free}_d(t); \\ f \setminus S_x, & \text{if } \mathrm{free}_d(x); \\ f \setminus S_t, & \text{if } \mathrm{free}_d(t); \\ f \setminus (S_x \cup S_t), & \text{otherwise;} \end{cases}$$
$$l' \stackrel{\text{def}}{=} \bigl(VI \setminus \mathrm{vars}(sh')\bigr) \cup f' \cup l'',$$

where

$$l'' \stackrel{\text{def}}{=} \begin{cases} l \setminus (S_x \cap S_t), & \text{if } \mathrm{lin}_d(x) \wedge \mathrm{lin}_d(t); \\ l \setminus S_x, & \text{if } \mathrm{lin}_d(x); \\ l \setminus S_t, & \text{if } \mathrm{lin}_d(t); \\ l \setminus (S_x \cup S_t), & \text{otherwise.} \end{cases}$$

Then

$$\mathrm{amgu}_S\bigl(d, x \mapsto t\bigr) \stackrel{\text{def}}{=} \langle sh', f', l' \rangle.$$

The function $\mathrm{proj}_S \colon SFL \times VI \to SFL$ *correctly captures the operation of projecting away a variable from an element of SFL. For each* $d \in SFL$ *and* $x \in VI$*,*

$$\mathrm{proj}_S(d, x) \stackrel{\text{def}}{=} \begin{cases} \bot_S, & \text{if } d = \bot_S; \\ \bigl\langle \mathrm{proj}_{SH}(sh, x), f \cup \{x\}, l \cup \{x\} \bigr\rangle, & \text{if } d = \langle sh, f, l \rangle \neq \bot_S. \end{cases}$$

Observe that a set-sharing domain such as *SFL* is strictly more precise for term finiteness information than a pair-sharing domain such as SFL_2 [41, 64] (where the set-sharing component *SH* in *SFL* is replaced by the domain *PSD* as defined in [4, 65]). To see this, consider the abstract evaluation of the binding $x \mapsto y$ and the description $\langle h, d \rangle \in H \times SFL$, where $h = \{x, y, z\}$ and $d = \langle sh, f, l \rangle$ is such that $sh = \bigl\{\{x, y\}, \{x, z\}, \{y, z\}\bigr\}$, $f = \varnothing$ and $l = \{x, y, z\}$. Then $z \notin \mathrm{share\_same\_var}_d(x, y)$ so that we have $h' = \{z\}$. In contrast, when using a pair sharing domain such as SFL_2 the element d is equivalent to $d' = \langle sh', f, l \rangle$, where $sh' = sh \cup \bigl\{\{x, y, z\}\bigr\}$. Hence we have $z \in \mathrm{share\_same\_var}_{d'}(x, y)$ and $h' = \varnothing$. Thus, in *sh* the information provided by the sharing group $\{x, y, z\}$ is redundant for the pair-sharing and groundness properties, but not redundant for term finiteness. Note that the above observation holds regardless of the pair-sharing variant considered, so that similar examples can be obtained for ASub [14, 60] and $\mathsf{Sh}^{\mathsf{PSh}}$ [58].

Although the domain *SFL* described here is very precise and used to implement the parameter component P for computing our experimental results, it is not intended as the target of the generic specification given in Definition 8; more powerful sharing domains can also satisfy this schema, including all the enhanced combinations considered in [6, 7]. For instance, as the predicate gfree_d defined on *SFL* does not fully exploit the disjunctive nature of its generic specification gfree_p, the precision of the analysis may be improved by adding a domain component explicitly tracking ground-or-freeness, as proposed in [6, 7]. The same argument applies to the predicate $\mathrm{or\_lin}_d$, with respect to $\mathrm{or\_lin}_p$, when considering the combination with the groundness domain *Pos*.

APPENDIX B: PROOFS OF THE STATED RESULTS

This appendix provides the proofs of the results stated in the paper. Section B.1 introduces the notations and preliminary concepts that are subsequently used in the proofs. In Section B.2 we recall few general results holding for (syntactic) equality theories and provide the proof of Proposition 2. The definition of (strongly) variable idempotent substitutions is given in Section B.3, together with some properties holding for them; these are then used in Section B.4 to prove some general results on operators on substitutions in *RSubst*, Propositions 13 and 15. Section B.4 is propaedeutic to Section B.5, where we prove Theorem 17 and to Section B.6, where we provide the proofs of Theorems 19 and 21. Results in Section B.4 are then used in Section B.7 to prove Theorems 23, 25 and 27, and in Section B.8 to prove Theorems 30 and 34.

B.1. Notations and Preliminaries for the Proofs

To simplify the expressions in the paper, any variable in a formula that is not in the scope of an explicit quantifier is assumed to be universally quantified.

A path $p \in \bigl(\mathbb{N} \setminus \{0\}\bigr)^\star$ is any finite sequence of non-zero natural numbers. The empty path is denoted by ϵ, whereas $i.p$ denotes the path obtained by concatenating the sequence formed by the natural number $i \neq 0$ with the sequence of the path p. Given a path p and a (possibly infinite) term $t \in \mathit{Terms}$, we denote by $t[p]$ the subterm of t found by following path p. Formally,

$$t[p] = \begin{cases} t & \text{if } p = \epsilon; \\ t_i[q] & \text{if } p = i \,.\, q \wedge (1 \leq i \leq n) \wedge t = f(t_1, \ldots, t_n). \end{cases}$$

Note that $t[p]$ is only defined for those paths p actually corresponding to subterms of t.

The function $\mathrm{size}\colon \mathit{HTerms} \to \mathbb{N}$ is defined, for each $t \in \mathit{HTerms}$, by

$$\mathrm{size}(t) \stackrel{\mathrm{def}}{=} \begin{cases} 1, & \text{if } t \in \mathit{Vars}; \\ 1 + \sum_{i=1}^{n} \mathrm{size}(t_i), & \text{if } t = f(t_1, \ldots, t_n), \text{ where } n \geq 0. \end{cases}$$

A substitution σ is *idempotent* if, for all $t \in \mathit{HTerms}$, we have $t\sigma\sigma = t\sigma$. The set of all idempotent substitutions is denoted by *ISubst* and $\mathit{ISubst} \subset \mathit{RSubst}$.

If $t \in \mathit{HTerms}$, we denote the set of variables that occur more than once in t by:

$$\operatorname{nlvars}(t) \stackrel{\mathrm{def}}{=} \bigl\{\, y \in \operatorname{vars}(t) \bigm| \neg\operatorname{occ\_lin}(y, t) \,\bigr\}.$$

If $\bar{s} = (s_1, \ldots, s_n) \in \mathit{HTerms}^n$ and $\bar{t} = (t_1, \ldots, t_n) \in \mathit{HTerms}^n$ are two tuples of finite terms, then we let $\bar{s} = \bar{t}$ denote the set of equations between corresponding components of $\bar{s}$ and $\bar{t}$. Namely,

$$(\bar{s} = \bar{t}) \stackrel{\mathrm{def}}{=} \{\, s_i = t_i \mid 1 \leq i \leq n \,\}.$$

Moreover, we overload the functions mvars, occ_lin and nlvars to work on tuples of terms; thus, we will say that $\bar{s}$ is linear if and only if $\operatorname{nlvars}(\bar{s}) = \varnothing$.

B.1.1. Equality Theories

Let $\{s, t, s_1, \ldots, s_n, t_1, \ldots, t_m\} \subseteq \mathit{HTerms}$. We assume that any equality theory T over *Terms* includes the *congruence axioms* denoted by the following schemata:

$$s = s, \tag{6}$$

$$s = t \leftrightarrow t = s, \tag{7}$$

$$r = s \land s = t \rightarrow r = t, \tag{8}$$

$$s_1 = t_1 \land \cdots \land s_n = t_n \rightarrow f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n). \tag{9}$$

In logic programming and most implementations of Prolog it is usual to assume an equality theory based on syntactic identity. This consists of the congruence axioms together with the *identity axioms* denoted by the following schemata, where f and g are distinct function symbols or $n \neq m$:

$$f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \rightarrow s_1 = t_1 \land \cdots \land s_n = t_n, \tag{10}$$

$$\neg\bigl(f(s_1, \ldots, s_n) = g(t_1, \ldots, t_m)\bigr). \tag{11}$$

The axioms characterized by schemata (10) and (11) ensure the equality theory depends only on the syntax. The equality theory for a non-syntactic domain replaces these axioms by ones that depend instead on the semantics of the domain and, in particular, on the interpretation given to functor symbols.

The equality theory of Clark [13] on which pure logic programming is based, usually called the *Herbrand* equality theory and denoted $\mathcal{FT}$, is given by the congruence axioms, the identity axioms, and the axiom schema

$$\forall z \in \mathit{Vars} : \forall t \in (\mathit{HTerms} \setminus \mathit{Vars}) : z \in \operatorname{vars}(t) \rightarrow \neg(z = t). \tag{12}$$

Axioms characterized by the schema (12) are called the *occurs-check axioms* and are an essential part of the standard unification procedure in SLD-resolution.

An alternative approach used in some implementations of Prolog, does not require the occurs-check axioms. This approach is based on the theory of rational trees $\mathcal{RT}$ [18, 19]. It assumes the congruence axioms and the identity axioms together with a *uniqueness axiom* for each substitution in rational solved form. Informally speaking these state that, after assigning a ground rational tree to each parameter variable, the substitution uniquely defines a ground rational tree for each of its domain variables.

In the sequel we will use the expression "equality theory" to denote any consistent, decidable theory T satisfying the congruence axioms. We will also use the expression "syntactic equality theory" to denote any equality theory T also satisfying the identity axioms.[14] Note that both $\mathcal{FT}$ and $\mathcal{RT}$ are syntactic equality theories. When the equality theory T is clear from the context, it is convenient to adopt the notations $\sigma \implies \tau$ and $\sigma \iff \tau$, where σ, τ are sets of equations, to denote $T \vdash \forall(\sigma \to \tau)$ and $T \vdash \forall(\sigma \leftrightarrow \tau)$, respectively.

Given an equality theory T, and a set of equations in rational solved form σ, we say that σ is *satisfiable* in T if $T \vdash \forall \mathit{Vars} \setminus \mathrm{dom}(\sigma) : \exists \, \mathrm{dom}(\sigma) \, . \, \sigma$.

Given a satisfiable set of equations $e \in \wp_{\mathrm{f}}(\mathit{Eqs})$ in an equality theory T, then a substitution $\sigma \in \mathit{RSubst}$ is called a *solution for e in T* if σ is satisfiable in T and $T \vdash \forall(\sigma \to e)$. If $\mathrm{vars}(\sigma) \subseteq \mathrm{vars}(e)$, then σ is said to be a *relevant* solution for e. In addition, σ is a *most general solution for e in T* if $T \vdash \forall(\sigma \leftrightarrow e)$. In this paper, the set of all the relevant most general solution for e will be denoted by $\mathrm{mgs}(e)$.

Observe that, given an arbitrary equality theory T, a set of equations in rational solved form may not be satisfiable in T. For example, $\exists x \, . \, \bigl\{x = f(x)\bigr\}$ is false in the Clark equality theory. However, by the uniqueness axioms, any set of equations in rational solved form is satisfiable in $\mathcal{RT}$.

B.2. Properties of Equality Theories

LEMMA 39. *Let $\sigma \in \mathit{RSubst}$ and $\{x \mapsto t\} \in \mathit{RSubst}$ be both satisfiable in the equality theory T, where $x \notin \mathrm{dom}(\sigma)$ and $\mathrm{vars}(t) \cap \mathrm{dom}(\sigma) = \varnothing$. Define also $\sigma' \stackrel{\mathrm{def}}{=} \sigma \cup \{x \mapsto t\}$. Then $\sigma' \in \mathit{RSubst}$ and σ' is satisfiable in T.*

Proof. Note that σ' is a substitution, since $\sigma \in \mathit{RSubst}$ and $x \notin \mathrm{dom}(\sigma)$. Moreover, as $\mathrm{vars}(t) \cap \mathrm{dom}(\sigma) = \varnothing$, σ' cannot contain circular subsets. Hence, $\sigma' \in \mathit{RSubst}$.

Since both σ and $\{x \mapsto t\}$ are satisfiable in T, we have

$$T \vdash \forall \mathit{Vars} \setminus \mathrm{dom}(\sigma) : \exists \, \mathrm{dom}(\sigma) \, . \, \sigma,$$
$$T \vdash \forall \mathit{Vars} \setminus \{x\} : \exists x \, . \, \{x = t\}.$$

Letting $V = \mathit{Vars} \setminus \bigl(\mathrm{dom}(\sigma) \cup \{x\}\bigr)$, we can rewrite these as

$$T \vdash \forall V : \forall x : \exists \, \mathrm{dom}(\sigma) \, . \, \sigma, \tag{13}$$
$$T \vdash \forall V : \forall \, \mathrm{dom}(\sigma) : \exists x \, . \, \{x = t\}. \tag{14}$$

Then, as $\mathrm{vars}(x = t) \cap \mathrm{dom}(\sigma) = \varnothing$, it follows from (14) that

$$T \vdash \forall V : \exists x \, . \, \{x = t\}.$$

Combining this with (13) gives

$$T \vdash \forall V : \Bigl(\bigl(\forall x : \exists \, \mathrm{dom}(\sigma) \, . \, \sigma\bigr) \wedge \bigl(\exists x \, . \, \{x = t\}\bigr)\Bigr).$$

[14]Note that, as a consequence of axiom (11) and the assumption that there are at least two distinct function symbols in the language, one of which is a constant, there exist two terms $a_1, a_2 \in \mathit{GTerms} \cap \mathit{HTerms}$ such that, for any syntactic equality theory T, we have $T \vdash a_1 \neq a_2$.

Thus we have

$$T \vdash \forall V : \exists x \,.\, \bigl(\exists \operatorname{dom}(\sigma) \,.\, \sigma \wedge \{x = t\}\bigr),$$

and hence, as $\operatorname{vars}(x = t) \cap \operatorname{dom}(\sigma) = \varnothing$,

$$T \vdash \forall V : \exists x \,.\, \exists \operatorname{dom}(\sigma) \,.\, \bigl(\sigma \wedge \{x = t\}\bigr).$$

Therefore,

$$T \vdash \forall V : \exists\bigl(\operatorname{dom}(\sigma) \cup \{x\}\bigr) \,.\, \sigma \cup \{x = t\}.$$

Thus σ' is satisfiable in T. ∎

Corollary 40. *Suppose T is an equality theory, $\sigma \in \mathit{RSubst}$ is satisfiable in T, $x \in \mathit{Vars} \setminus \operatorname{dom}(\sigma)$, and $t \in \mathit{HTerms} \cap \mathit{GTerms}$. Then, $\tau \stackrel{\mathrm{def}}{=} \sigma \cup \{x \mapsto t\} \in \mathit{RSubst}$ and τ is satisfiable in T.*

Lemma 41. *Assume T is an equality theory and $\sigma \in \mathit{RSubst}$. Then, for each $t \in \mathit{HTerms}$,*

$$T \vdash \forall\bigl(\sigma \to (t = t\sigma)\bigr).$$

Proof. Proved in [40, Lemma 2]. ∎

Lemma 42. *Assume T is an equality theory and $\sigma \in \mathit{RSubst}$. Then, for each $s, t \in \mathit{HTerms}$,*

$$T \vdash \forall\bigl(\sigma \cup \{s = t\} \leftrightarrow \sigma \cup \{s = t\sigma\}\bigr).$$

Proof. First, note, using the congruence axioms (7) and (8), that, for any terms $p, q, r \in \mathit{HTerms}$,

$$T \vdash \forall(p = q \wedge q = r) \leftrightarrow \forall(p = r \wedge q = r). \tag{15}$$

Secondly note that, using Lemma 41, for any substitution $\tau \in \mathit{RSubst}$ and term $r \in \mathit{HTerms}$, $T \vdash \forall\bigl(\tau \to (r = r\tau)\bigr)$. Thus

$$T \vdash \forall\bigl(\tau \leftrightarrow \tau \cup \{r = r\tau\}\bigr). \tag{16}$$

Using these results, we obtain

$$\begin{aligned}
&T \vdash \forall\bigl(\sigma \cup \{s = t\} \leftrightarrow \sigma \cup \{s = t, t = t\sigma\}\bigr), && \text{[by (16)]}\\
&T \vdash \forall\bigl(\sigma \cup \{s = t\} \leftrightarrow \sigma \cup \{s = t\sigma, t = t\sigma\}\bigr), && \text{[by (15)]}\\
&T \vdash \forall\bigl(\sigma \cup \{s = t\} \leftrightarrow \sigma \cup \{s = t\sigma\}\bigr). && \text{[by (16)]}
\end{aligned}$$

∎

Lemma 43. *Let $\sigma \in \mathit{RSubst}$ and $s, t \in \mathit{HTerms}$, where $\mathcal{RT} \vdash \forall\bigl(\sigma \to (s = t)\bigr)$. Then $\operatorname{rt}(s, \sigma) = \operatorname{rt}(t, \sigma)$.*

Proof. We suppose, towards a contradiction, that $\operatorname{rt}(s, \sigma) \neq \operatorname{rt}(t, \sigma)$. Then, there must exist a finite path p such that:

a. $x = \operatorname{rt}(s, \sigma)[p] \in \mathit{Vars} \setminus \operatorname{dom}(\sigma)$, $y = \operatorname{rt}(t, \sigma)[p] \in \mathit{Vars} \setminus \operatorname{dom}(\sigma)$ and $x \neq y$; or

b. $x = \mathrm{rt}(s, \sigma)[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$ and $r = \mathrm{rt}(t, \sigma)[p] \notin \mathit{Vars}$ or, symmetrically, $r = \mathrm{rt}(s, \sigma)[p] \notin \mathit{Vars}$ and $x = \mathrm{rt}(t, \sigma)[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$; or

c. $r_1 = \mathrm{rt}(s, \sigma)[p] \notin \mathit{Vars}$, $r_2 = \mathrm{rt}(t, \sigma)[p] \notin \mathit{Vars}$ and r_1 and r_2 have different principal functors.

Then, by definition of 'rt', there must exists an index $i \in \mathbb{N}$ such that one of these holds:

1. $x = s\sigma^i[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$, $y = t\sigma^i[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$ and $x \neq y$; or
2. $x = s\sigma^i[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$ and $r = t\sigma^i[p] \notin \mathit{Vars}$ or, in a symmetrical way, $r = s\sigma^i[p] \notin \mathit{Vars}$ and $x = t\sigma^i[p] \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$; or
3. $r_1 = s\sigma^i[p] \notin \mathit{Vars}$ and $r_2 = t\sigma^i[p] \notin \mathit{Vars}$ have different principal functors.

By Lemma 41, we have $\mathcal{RT} \vdash \forall\bigl(\sigma \to (s\sigma^i = t\sigma^i)\bigr)$; from this, since $\mathcal{RT}$ is a syntactic equality theory, we obtain that

$$\mathcal{RT} \vdash \forall\bigl(\sigma \to (s\sigma^i[p] = t\sigma^i[p])\bigr). \tag{17}$$

We now prove that each case leads to a contradiction.

Consider case 1. Let $r_1, r_2 \in \mathit{GTerms} \cap \mathit{HTerms}$ be two terms having different principal functors, so that $\mathcal{RT} \vdash \forall(r_1 \neq r_2)$. Then, by Lemma 39, we have that $\sigma' = \sigma \cup \{x \mapsto r_1, y \mapsto r_2\} \in \mathit{RSubst}$ is satisfiable and also $\mathcal{RT} \vdash \forall(\sigma' \to \sigma)$, $\mathcal{RT} \vdash \forall\bigl(\sigma' \to (x = r_1)\bigr)$, $\mathcal{RT} \vdash \forall\bigl(\sigma' \to (y = r_2)\bigr)$. This is a contradiction, since, by (17), we have $\mathcal{RT} \vdash \forall\bigl(\sigma \to (x = y)\bigr)$.

Consider case 2. Without loss of generality, consider the first subcase, where $x = s\sigma^i$ and $r = t\sigma^i[p] \notin \mathit{Vars}$. Let $r' \in \mathit{GTerms} \cap \mathit{HTerms}$ be such that r and r' have different principal functors, so that $\mathcal{RT} \vdash \forall(r \neq r')$. By Lemma 39, $\sigma' = \sigma \cup \{x \mapsto r'\} \in \mathit{RSubst}$ is satisfiable; we also have that $\mathcal{RT} \vdash \forall(\sigma' \to \sigma)$ and $\mathcal{RT} \vdash \forall\bigl(\sigma' \to (x = r')\bigr)$. This is a contradiction as, by (17), $\mathcal{RT} \vdash \forall\bigl(\sigma \to (x = r)\bigr)$.

Finally, consider case 3. In this case $\mathcal{RT} \vdash \forall(r_1 \neq r_2)$. This immediately leads to a contradiction, since, by (17), $\mathcal{RT} \vdash \forall\bigl(\sigma \to (r_1 = r_2)\bigr)$. ∎

Lemma 44. *Let T be a syntactic equality theory. Let $s \in \mathit{HTerms} \cap \mathit{GTerms}$ and $t \in \mathit{HTerms}$ be such that $\mathrm{size}(t) > \mathrm{size}(s)$. Then $T \vdash \forall(s \neq t)$.*

Proof. By induction on $m = \mathrm{size}(s)$. For the base case, when $m = 1$, we have that s is a term functor of arity 0. Since $\mathrm{size}(t) > 1$, then $t = f(t_1, \ldots, t_n)$, where $n > 0$. Then, by the identity axioms, we have $T \vdash \forall(s \neq t)$.

For the inductive case, when $m > 1$, assume that the result holds for all $m' < m$ and let $s = f(s_1, \ldots, s_n)$, where $n > 0$. Since $\mathrm{size}(t) > m$, we have $t = f'(t_1, \ldots, t_{n'})$, where $n' > 0$. If $f \neq f'$ or $n \neq n'$ then, by the identity axioms, we have $T \vdash \forall(s \neq t)$. Otherwise, let $f = f'$ and $n = n'$. Note that, for all $i \in \{1, \ldots, n\}$, we have $\mathrm{size}(s_i) < m$. Also, there exists an index $j \in \{1, \ldots, n\}$ such that $\mathrm{size}(t_j) > \mathrm{size}(s_j)$. By the inductive hypothesis, $T \vdash \forall(s_j \neq t_j)$ so that, by the identity axioms, $T \vdash \forall(s \neq t)$. ∎

Proof of Proposition 2 on page 7. We have the following chain of double implications

$$
\begin{aligned}
\tau \in \downarrow \sigma &\iff \exists \sigma' \in \mathit{RSubst} \mathrel{.} \tau \in \mathrm{mgs}(\sigma \cup \sigma') \\
&\iff \exists \sigma' \in \mathit{RSubst} \mathrel{.} \mathcal{RT} \vdash \forall\bigl(\tau \leftrightarrow (\sigma \cup \sigma')\bigr) \\
&\iff \exists \sigma' \in \mathit{RSubst} \mathrel{.} \\
&\qquad\quad \mathcal{RT} \vdash \Bigl(\forall(\tau \rightarrow \sigma) \land \forall(\tau \rightarrow \sigma') \\
&\qquad\qquad\qquad \land \forall\bigl((\sigma \cup \sigma') \rightarrow \tau\bigr)\Bigr) \\
&\iff \mathcal{RT} \vdash \forall(\tau \rightarrow \sigma).
\end{aligned}
$$

Note that the left implication in the last step is obtained by taking $\sigma' = \tau$. ∎

B.3. Variable-Idempotence

In [40], (weak) variable-idempotent substitutions were introduced as a subclass of substitutions in rational solved form in order to allow a more convenient reasoning about the sharing of variables for possibly non-idempotent substitutions. In [39] a stronger definition was used, taking into consideration also the variables in the domain of the substitution. *Strong* variable-idempotence is a useful concept when dealing with the finiteness of a rational term and the multiplicity of variables occurring in it (e.g., when linearity is a property of interest). In the following we consider this stronger definition, also adopted in [41, 64].

Definition 45. **(Variable-idempotence.)** *A substitution $\sigma \in \mathit{RSubst}$ is said to be (strongly)* variable-idempotent *if and only if for all $t \in \mathit{HTerms}$ we have*

$$\mathrm{vars}(t\sigma\sigma) = \mathrm{vars}(t\sigma).$$

The set of variable-idempotent substitutions is denoted VSubst.

Note that we have $\mathit{ISubst} \subset \mathit{VSubst} \subset \mathit{RSubst}$.

Definition 46. **($\mathcal{S}$-transformation.)** *The relation $\overset{\mathcal{S}}{\longmapsto} \subseteq \mathit{RSubst} \times \mathit{RSubst}$, called* $\mathcal{S}$-step*, is defined by*

$$\frac{(x \mapsto t) \in \sigma \qquad (y \mapsto s) \in \sigma \qquad x \neq y}{\sigma \overset{\mathcal{S}}{\longmapsto} \bigl(\sigma \setminus \{y \mapsto s\}\bigr) \cup \bigl\{y \mapsto s\{x \mapsto t\}\bigr\}}.$$

If we have a finite sequence of $\mathcal{S}$-steps $\sigma_1 \overset{\mathcal{S}}{\longmapsto} \cdots \overset{\mathcal{S}}{\longmapsto} \sigma_n$ mapping σ_1 to σ_n, then we write $\sigma_1 \overset{\mathcal{S}}{\longmapsto}{}^* \sigma_n$ and say that σ_1 can be rewritten, by $\mathcal{S}$-transformation, to σ_n.

The following theorems show that considering substitutions in *VSubst* is not a restrictive hypothesis.

Theorem 47. *Suppose $\sigma \in \mathit{RSubst}$ and $\sigma \overset{\mathcal{S}}{\longmapsto}{}^* \sigma'$. Then we have $\sigma' \in \mathit{RSubst}$, $\mathrm{dom}(\sigma) = \mathrm{dom}(\sigma')$, and $\mathrm{vars}(\sigma) = \mathrm{vars}(\sigma')$. Moreover, if T is any equality theory, we have $T \vdash \forall(\sigma \leftrightarrow \sigma')$.*

Proof. Proved in [40, Theorem 1]. ∎

Theorem 48. *Suppose $\sigma \in \mathit{RSubst}$. Then there exists $\sigma' \in \mathit{VSubst}$ such that $\sigma \overset{\mathcal{S}}{\longmapsto}{}^* \sigma'$ and, for all $\tau \subseteq \sigma'$, $\tau \in \mathit{VSubst}$.*

Proof. The proof is the same given for [40, Theorem 2], where a weaker result, using *weak* variable-idempotence, was stated. ∎

THEOREM 49. *Let T be an equality theory and $\sigma \in RSubst$. Then there exists $\sigma' \in VSubst$ such that* $\mathrm{dom}(\sigma) = \mathrm{dom}(\sigma')$, $\mathrm{vars}(\sigma) = \mathrm{vars}(\sigma')$, $T \vdash \forall(\sigma \leftrightarrow \sigma')$ *and for all $\tau \subseteq \sigma'$, $\tau \in VSubst$.*

Proof. The result easily follows from Theorems 47 and 48. ∎

B.4. Some Results on Operators on Substitutions in *RSubst*

When computing $\mathrm{hvars}(\sigma)$ by means of the fixpoint computation given in Definition 11 on page 13, the fixpoint is reached after a single iteration if $\sigma \in VSubst$.

LEMMA 50. *For each $\sigma \in VSubst$ we have* $\mathrm{hvars}(\sigma) = \mathrm{hvars}_1(\sigma)$.

Proof. We show that $\mathrm{hvars}_2(\sigma) \subseteq \mathrm{hvars}_1(\sigma)$. Let $y \in \mathrm{hvars}_2(\sigma)$. By Definition 11, we have two cases:

1. if $y \in \mathrm{hvars}_1(\sigma)$ then there is nothing to prove;
2. assume now $y \in \mathrm{dom}(\sigma)$ and $\mathrm{vars}(y\sigma) \subseteq \mathrm{hvars}_1(\sigma)$. By Definition 11, we have two subcases:
   (a) $\mathrm{vars}(y\sigma) \subseteq Vars \setminus \mathrm{dom}(\sigma)$.
   Then $\mathrm{vars}(y\sigma) \subseteq \mathrm{hvars}_0(\sigma)$, so that $y \in \mathrm{hvars}_1(\sigma)$;
   (b) $V = \mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) \neq \varnothing$ and, for all $z \in V$, $\mathrm{vars}(z\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$.
   Let $z \in V$ so that $z \in \mathrm{vars}(y\sigma)$. By hypothesis, we have $\sigma \in VSubst$ so that $z \in \mathrm{vars}(y\sigma\sigma)$. As $z \in \mathrm{dom}(\sigma)$ and $\mathrm{vars}(z\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$, $z \notin \mathrm{vars}(z\sigma)$. This means that $z \notin \mathrm{vars}(y\sigma\sigma)$, which is a contradiction since $\sigma \in VSubst$.

∎

PROPOSITION 51. *For each $\sigma \in VSubst$, we have*

$$\mathrm{hvars}(\sigma) = \bigl\{\, y \in Vars \bigm| \mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing \,\bigr\}.$$

Proof. The result is obtained by applying Lemma 50 and then unfolding Definition 11. ∎

PROPOSITION 52. *Let $\sigma \in VSubst$ and $r \in HTerms$, where* $\mathrm{vars}(r) \subseteq \mathrm{hvars}(\sigma)$. *Then*

$$\mathrm{rt}(r, \sigma) = r\sigma,$$
$$\mathrm{vars}(r\sigma) \cap \mathrm{dom}(\sigma) = \varnothing.$$

Proof. Suppose $y \in \mathrm{vars}(r)$. Then, by Proposition 51, $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. Thus, for any $i > 0$, we have $y\sigma^i = y\sigma \in HTerms$. Thus $\mathrm{rt}(y, \sigma) = y\sigma$. As this holds for all $y \in \mathrm{vars}(r)$, it follows that $\mathrm{rt}(r, \sigma) = r\sigma$ and $\mathrm{vars}(r\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. ∎

PROPOSITION 53. *Let $\sigma \in RSubst$ and $t \in HTerms$. Then*

$$\mathrm{vars}\bigl(\mathrm{rt}(t, \sigma)\bigr) \cap \mathrm{dom}(\sigma) = \varnothing, \tag{53a}$$
$$\mathrm{rt}(t, \sigma) \in HTerms \iff \exists i \in \mathbb{N} \,.\, \mathrm{rt}(t, \sigma) = t\sigma^i. \tag{53b}$$

Proof.

(53a) Let $x \in \mathrm{dom}(\sigma)$ and, towards a contradiction, suppose $x \in \mathrm{vars}\bigl(\mathrm{rt}(t,\sigma)\bigr)$. Thus, there exists a finite path p such that $x = \mathrm{rt}(t,\sigma)[p]$. Thus, by definition of 'rt', there exists an index $i \in \mathbb{N}$ such that $x = \sigma^i(t)[p]$. Since $x \in \mathrm{dom}(\sigma)$, then $x \neq x\sigma$, so that $x \neq \sigma^{i+1}(t)[p]$. Also note that, being $\sigma \in \mathit{RSubst}$, σ contains no circular subsets, so that we have $x \neq \sigma^j(t)[p]$, for each index $j > i$. This implies $x \neq \mathrm{rt}(t,\sigma)[p]$, which is a contradiction. Since no such finite path p can exist, we can conclude $x \notin \mathrm{vars}\bigl(\mathrm{rt}(t,\sigma)\bigr)$.

(53b) Since substitutions map finite terms into finite terms, a finite number of applications cannot produce an infinite term, so that the left implication holds. Proving the right implication by contraposition, suppose that $\mathrm{rt}(t,\sigma) \neq t\sigma^i$, for all $i \in \mathbb{N}$. Then, by definition of 'rt', we have $t\sigma^i \neq t\sigma^{i+1}$, for all $i \in \mathbb{N}$. Letting $n \in \mathbb{N}$ be the number of bindings in $\sigma \in \mathit{RSubst}$, for all $i \in \mathbb{N}$ we have that $\mathrm{size}(t\sigma^i) < \mathrm{size}(t\sigma^{i+n})$, because σ has no circular subsets. Thus $\mathrm{rt}(t,\sigma) \notin \mathit{HTerms}$, because there is no finite upper bound to the number of function symbols occurring in $\mathrm{rt}(t,\sigma)$. ∎

The following proposition shows that, for a substitution $\sigma \in \mathit{VSubst}$, the finiteness operator precisely captures the intended property.

Proposition 54. *Let $\sigma \in \mathit{VSubst}$ and $y \in \mathit{Vars}$. Then*

$$\mathrm{rt}(y,\sigma) \in \mathit{HTerms} \quad\iff\quad y \in \mathrm{hvars}(\sigma).$$

Proof. Since $\sigma \in \mathit{VSubst}$, by Proposition 51 we have $y \in \mathrm{hvars}(\sigma)$ if and only if $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$.

Let $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. Then, for any $i > 0$, we have $y\sigma^i = y\sigma \in \mathit{HTerms}$. Hence $\mathrm{rt}(y,\sigma) = y\sigma \in \mathit{HTerms}$.

In order to prove the other inclusion, let now $\mathrm{rt}(y,\sigma) \in \mathit{HTerms}$. By Proposition 53, there exists an $i \in \mathbb{N}$ such that $\mathrm{rt}(y,\sigma) = y\sigma^i$ and $\mathrm{vars}(y\sigma^i) \cap \mathrm{dom}(\sigma) = \varnothing$. Since $\sigma \in VSubst$, we have $\mathrm{vars}(y\sigma^i) = \mathrm{vars}(y\sigma)$, so that $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. ∎

The following proposition is proved in [40], and shows that the function 'gvars' precisely captures the intended property.

Proposition 55. *Let $\sigma \in \mathit{RSubst}$ and $x \in \mathit{Vars}$. Then*

$$y \in \mathrm{gvars}(\sigma) \iff \mathrm{rt}(y,\sigma) \in \mathit{GTerms}.$$

The following results is a consequence of Proposition 54 and Proposition 55.

Corollary 56. *Let $\sigma \in \mathit{RSubst}$ and $t \in \mathit{HTerms}$. Then*

$$\mathrm{vars}(t) \subseteq \mathrm{gvars}(\sigma) \iff \mathrm{rt}(t,\sigma) \in \mathit{GTerms}, \tag{56a}$$

$$\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma) \iff \mathrm{rt}(t,\sigma) \in \mathit{HTerms}. \tag{56b}$$

Proof of Proposition 15 on page 14. We prove the two statements (15a) and (15b), one at a time.

(15a). Suppose $x \in \mathrm{hvars}(\tau) \setminus \mathrm{hvars}(\sigma)$. Then, by Proposition 54, we have that $\mathrm{rt}(x,\tau) \in \mathit{HTerms}$. By Proposition 53, there exists $i \in \mathbb{N}$ such that $\mathrm{rt}(x,\tau) = x\tau^i$ and also $\mathrm{vars}(x\tau^i) \cap \mathrm{dom}(\tau) = \varnothing$. Let $t \in \mathit{GTerms} \cap \mathit{HTerms}$ and

$$\upsilon \stackrel{\mathrm{def}}{=} \bigl\{\, y \mapsto t \bigm| y \in \mathrm{vars}(x\tau^i) \,\bigr\}.$$

Then, by Lemma 39, $\tau' \stackrel{\text{def}}{=} \tau \cup \upsilon \in RSubst$ is satisfiable. Moreover, we have that $x\tau^i\tau' \in GTerms \cap HTerms$. Define now $n \stackrel{\text{def}}{=} \mathrm{size}(x\tau^i\tau')$. Note that, since $x \notin \mathrm{hvars}(\sigma)$, $\mathrm{rt}(x, \sigma) \notin HTerms$, then there exists $j \in \mathbb{N}$ such that $\mathrm{size}(x\sigma^j) > n$. Therefore, by Lemma 44,

$$\mathcal{RT} \vdash \forall(x\tau^i\tau' \neq x\sigma^j). \tag{20}$$

Also, by Lemma 41, $\mathcal{RT} \vdash \forall\bigl(\sigma \to (x = x\sigma^j)\bigr)$ and $\mathcal{RT} \vdash \forall\bigl(\tau \to (x = x\tau^i)\bigr)$. By definition, $\tau' \in {\downarrow}\,\tau$ and, by hypothesis, $\tau \in {\downarrow}\,\sigma$, so that $\tau' \in {\downarrow}\,\sigma$. Thus, by Proposition 2 and transitivity, we have $\mathcal{RT} \vdash \forall\bigl(\tau' \to (x\tau^i = x\sigma^j)\bigr)$. Applying Lemma 41, we obtain $\mathcal{RT} \vdash \forall\bigl(\tau' \to (x\tau^i\tau' = x\sigma^j)\bigr)$, which contradicts (20).

(15b). Suppose $x \in \mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\sigma)$. Then, by Propositions 54 and 55, $\mathrm{rt}(x, \sigma) \in GTerms \cap HTerms$. Thus, by case (53b) of Proposition 53, there exists $i \in \mathbb{N}$ such that $\mathrm{rt}(x, \sigma) = x\sigma^i$ and also $\mathrm{vars}(x\sigma^i) = \varnothing$. Thus $\mathrm{rt}(x\sigma^i, \tau) = x\sigma^i$. Since by hypothesis we have $\tau \in {\downarrow}\,\sigma$, by Lemma 41 and transitivity we obtain that $\mathcal{RT} \vdash \forall\bigl(\tau \to (x = x\sigma^i)\bigr)$. Thus, by Lemma 43, $\mathrm{rt}(x, \tau) = \mathrm{rt}(x\sigma^i, \tau) = x\sigma^i$. Therefore, by Propositions 54 and 55, $x \in \mathrm{gvars}(\tau) \cap \mathrm{hvars}(\tau)$. ∎

In order to prove Proposition 13, i.e., to show that the finiteness operator precisely captures the intended property even for arbitrary substitutions in *RSubst*, we now prove that this operator is invariant under the application of *S*-steps.

LEMMA 57. *For each $m > 0$, we have* $\mathrm{hvars}_{m-1}(\sigma) \subseteq \mathrm{hvars}_m(\sigma)$.

Proof. Straightforward by Definition 11. ∎

LEMMA 58. *Let $\sigma, \sigma' \in RSubst$ where $\sigma \overset{\mathcal{S}}{\longmapsto} \sigma'$. Then* $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma')$.

Proof. Let $(x \mapsto t), (y \mapsto s) \in \sigma$, where $x \neq y$, such that

$$\sigma' = \bigl(\sigma \setminus \{y \mapsto s\}\bigr) \cup \bigl\{y \mapsto s\{x \mapsto t\}\bigr\}.$$

If $x \notin \mathrm{vars}(s)$ then we have $\sigma = \sigma'$ and the result trivially holds. Thus, we assume $x \in \mathrm{vars}(s)$. We prove the two inclusions separately.

In order to prove $\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\sigma')$ we show, by induction on $m \geq 0$, that we have

$$\mathrm{hvars}_m(\sigma) \subseteq \mathrm{hvars}_m(\sigma').$$

For the base case, when $m = 0$, by Theorem 47 we have $\mathrm{dom}(\sigma) = \mathrm{dom}(\sigma')$ so that

$$\begin{aligned} \mathrm{hvars}_0(\sigma) &= Vars \setminus \mathrm{dom}(\sigma) \\ &= Vars \setminus \mathrm{dom}(\sigma') \\ &= \mathrm{hvars}_0(\sigma'). \end{aligned}$$

For the inductive step, when $m > 0$, assume $\mathrm{hvars}_{m-1}(\sigma) \subseteq \mathrm{hvars}_{m-1}(\sigma')$ and let $z \in \mathrm{hvars}_m(\sigma)$. By Definition 11, we have two cases: if $z \in \mathrm{hvars}_{m-1}(\sigma)$ then the result follows by a straight application of the inductive hypothesis; otherwise, we have

$$z \in \mathrm{dom}(\sigma) \wedge \mathrm{vars}(z\sigma) \subseteq \mathrm{hvars}_{m-1}(\sigma).$$

Now, if $z \neq y$ we have $z\sigma = z\sigma'$, so that, by Theorem 47 and the inductive hypothesis we have

$$z \in \mathrm{dom}(\sigma') \wedge \mathrm{vars}(z\sigma') \subseteq \mathrm{hvars}_{m-1}(\sigma'),$$

so that, by Definition 11, $z \in \mathrm{hvars}_m(\sigma')$. Otherwise, if $z = y$, then

$$\begin{aligned}\mathrm{vars}(z\sigma) &= \mathrm{vars}(s) \\ &\subseteq \mathrm{hvars}_{m-1}(\sigma).\end{aligned}$$

Since, by hypothesis, $x \in \mathrm{vars}(s)$,

$$\begin{aligned}\mathrm{vars}(z\sigma') &= \mathrm{vars}\bigl(s\{x \mapsto t\}\bigr) \\ &= \bigl(\mathrm{vars}(s) \setminus \{x\}\bigr) \cup \mathrm{vars}(t),\end{aligned}$$

and we need to show $\mathrm{vars}(z\sigma') \subseteq \mathrm{hvars}_{m-1}(\sigma')$. By the inductive hypothesis we have

$$\mathrm{vars}(s) \subseteq \mathrm{hvars}_{m-1}(\sigma');$$

Note that, since $x \in \mathrm{vars}(s)$, it follows $x \in \mathrm{hvars}_{m-1}(\sigma')$ so that, by Definition 11 and Lemma 57,

$$\begin{aligned}\mathrm{vars}(t) &\subseteq \mathrm{hvars}_{m-2}(\sigma') \\ &\subseteq \mathrm{hvars}_{m-1}(\sigma').\end{aligned}$$

In order to prove $\mathrm{hvars}(\sigma) \supseteq \mathrm{hvars}(\sigma')$ we show, by induction on $m \geq 0$, that we have

$$\mathrm{hvars}_{m+1}(\sigma) \supseteq \mathrm{hvars}_m(\sigma').$$

For the base case, when $m = 0$, by Lemma 57 and Theorem 47 we have

$$\begin{aligned}\mathrm{hvars}_1(\sigma) &\supseteq \mathrm{hvars}_0(\sigma) \\ &= \mathit{Vars} \setminus \mathrm{dom}(\sigma) \\ &= \mathit{Vars} \setminus \mathrm{dom}(\sigma') \\ &= \mathrm{hvars}_0(\sigma').\end{aligned}$$

For the inductive step, when $m > 0$, assume $\mathrm{hvars}_m(\sigma) \supseteq \mathrm{hvars}_{m-1}(\sigma')$ and let $z \in \mathrm{hvars}_m(\sigma')$. By Definition 11, we have two cases: if $z \in \mathrm{hvars}_{m-1}(\sigma')$ then the result follows by the inductive hypothesis and Lemma 57; otherwise, we have

$$z \in \mathrm{dom}(\sigma') \wedge \mathrm{vars}(z\sigma') \subseteq \mathrm{hvars}_{m-1}(\sigma').$$

Now, if $z \neq y$ we have $z\sigma = z\sigma'$, so that, by Theorem 47 and the inductive hypothesis we have

$$z \in \mathrm{dom}(\sigma) \wedge \mathrm{vars}(z\sigma) \subseteq \mathrm{hvars}_m(\sigma),$$

so that, by Definition 11, $z \in \mathrm{hvars}_{m+1}(\sigma)$. Otherwise, if $z = y$, by definition of σ', the inductive hypothesis and Lemma 57, we have

$$\begin{aligned}
\mathrm{vars}(z\sigma') &= \mathrm{vars}\bigl(s\{x \mapsto t\}\bigr) \\
&= \bigl(\mathrm{vars}(s) \setminus \{x\}\bigr) \cup \mathrm{vars}(t) \\
&\subseteq \mathrm{hvars}_{m-1}(\sigma') \\
&\subseteq \mathrm{hvars}_{m}(\sigma) \\
&\subseteq \mathrm{hvars}_{m+1}(\sigma).
\end{aligned}$$

Also note that we have

$$\begin{aligned}
\mathrm{vars}(x\sigma) &= \mathrm{vars}(t) \\
&\subseteq \mathrm{hvars}_{m}(\sigma)
\end{aligned}$$

so that, by Definition 11 we have

$$x \in \mathrm{hvars}_{m+1}(\sigma).$$

The result follows by observing that

$$\mathrm{vars}(z\sigma) = \mathrm{vars}(s) = \bigl(\mathrm{vars}(s) \setminus \{x\}\bigr) \cup \{x\}.$$

∎

LEMMA 59. *Let $\sigma, \sigma' \in RSubst$, where $\sigma \overset{\mathcal{S}}{\longmapsto}{}^{*} \sigma'$. Then* $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma')$.

Proof. By induction on the length $n \geq 0$ of the derivation. For the base case, when $n = 0$, there is nothing to prove. Suppose now that

$$\sigma = \sigma_0 \overset{\mathcal{S}}{\longmapsto} \cdots \overset{\mathcal{S}}{\longmapsto} \sigma_{n-1} \overset{\mathcal{S}}{\longmapsto} \sigma_n = \sigma',$$

where $n > 1$. By the inductive hypothesis, since the derivation $\sigma \overset{\mathcal{S}}{\longmapsto}{}^{*} \sigma_{n-1}$ has length $n-1$, we have $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma_{n-1})$. Then the thesis follows by Lemma 58. ∎

Proof of Proposition 13 on page 14. By Theorem 49, there exists $\sigma' \in VSubst$ such that $\sigma \overset{\mathcal{S}}{\longmapsto}{}^{*} \sigma'$ and, for all equality theories T, $T \vdash \forall(\sigma \leftrightarrow \sigma')$. Thus, by Lemma 59, we have $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma')$. The thesis then follows by applying Proposition 54. ∎

LEMMA 60. *Let $\sigma, \tau \in VSubst$ be satisfiable in a syntactic equality theory T and suppose that $T \vdash \forall(\sigma \leftrightarrow \tau)$. Then* $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\tau)$.

Proof. We assume that the congruence and identity axioms hold. We will prove the inclusion $\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\tau)$, while the other inclusion will follow by symmetry.

Let $y \in \mathrm{hvars}(\sigma)$. Then, by Proposition 51, $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. We will show that $\mathrm{rt}(y, \tau) \in HTerms$ so that, by Proposition 54, $y \in \mathrm{hvars}(\tau)$.

Take $t \in HTerms \cap GTerms$ and let

$$\sigma' \stackrel{\mathrm{def}}{=} \sigma \cup \bigl\{\, z \mapsto t \bigm| z \in \mathrm{vars}(y\sigma) \,\bigr\}.$$

Note that $y\sigma\sigma' \in \mathit{HTerms} \cap \mathit{GTerms}$, so that $\mathrm{size}(y\sigma\sigma') = n \in \mathbb{N}$. Also, by Lemma 40, we have $\sigma' \in \mathit{RSubst}$ is satisfiable in T.

By contraposition, suppose that $\mathrm{rt}(y, \tau) \notin \mathit{HTerms}$. Then, there exists an index $i \in \mathbb{N}$ such that $\mathrm{size}(y\tau^i) > n$. By Lemma 41, we have $\sigma' \implies \{y = y\sigma\sigma'\}$ and

$$\sigma' \implies \sigma \implies \tau \implies \{y = y\tau^i\},$$

so that, by the congruence axioms, $\sigma' \implies \{y\sigma\sigma' = y\tau^i\}$. However, by Lemma 44, $T \vdash \forall(y\sigma\sigma' \neq y\tau^i)$, therefore obtaining a contradiction. Thus $\mathrm{rt}(y, \tau) \in \mathit{HTerms}$. ∎

PROPOSITION 61. *Let $\sigma, \tau \in \mathit{RSubst}$. Let also $W \subseteq \mathit{Vars}$, where*

$$\mathcal{RT} \vdash \forall(\exists W \,.\, \sigma \leftrightarrow \exists W \,.\, \tau).$$

Then $\mathrm{hvars}(\sigma) \setminus W = \mathrm{hvars}(\tau) \setminus W$.

Proof. Consider a variable $z \in \mathrm{hvars}(\sigma) \setminus W$. We assume that $z \notin \mathrm{hvars}(\tau)$ to obtain a contradiction.

By Proposition 54, $\mathrm{rt}(z, \sigma) \in \mathit{HTerms}$. By Proposition 53, there exists $i \in \mathbb{N}$ such that $\mathrm{rt}(z, \sigma) = z\sigma^i$ and $\mathrm{vars}(z\sigma^i) \cap \mathrm{dom}(\sigma) = \varnothing$.

Take $t \in \mathit{GTerms} \cap \mathit{HTerms}$ and let

$$\upsilon \stackrel{\mathrm{def}}{=} \bigl\{\, y \mapsto t \bigm| y \in \mathrm{vars}(z\sigma^i) \,\bigr\}.$$

By Lemma 39, $\sigma' \stackrel{\mathrm{def}}{=} \sigma \cup \upsilon \in {\downarrow}\,\sigma$ is satisfiable. Thus, by Proposition 2, we have

$$\mathcal{RT} \vdash \forall(\sigma' \to \sigma). \tag{21}$$

By the definition of σ', $z\sigma^i\sigma' \in \mathit{GTerms} \cap \mathit{HTerms}$. As $z \notin \mathrm{hvars}(\tau)$, there exists $j \in \mathbb{N}$ such that $\mathrm{size}(z\tau^j) > \mathrm{size}(z\sigma^i\sigma')$. Thus, by Lemma 44,

$$\mathcal{RT} \vdash \forall(z\sigma^i\sigma' \neq z\tau^j). \tag{22}$$

From the application of Lemma 41, we obtain that $\mathcal{RT} \vdash \forall\bigl(\sigma \to (z = z\sigma^i)\bigr)$ and $\mathcal{RT} \vdash \forall\bigl(\sigma' \to (z\sigma^i = z\sigma^i\sigma')\bigr)$. Thus, by (21),

$$\mathcal{RT} \vdash \forall\bigl(\sigma' \to (z = z\sigma^i\sigma')\bigr). \tag{23}$$

Using (21), the hypothesis and the logically true statement $\forall(\sigma \to \exists W \,.\, \sigma)$, we obtain $\mathcal{RT} \vdash \forall(\sigma' \to \exists W \,.\, \tau)$. By Lemma 41, we have $\mathcal{RT} \vdash \forall\bigl(\tau \to (z = z\tau^j)\bigr)$; thus, as $\mathcal{RT}$ is a first-order theory, $\mathcal{RT} \vdash \forall\bigl(\exists W \,.\, \tau \to \exists W \,.\, (z = z\tau^j)\bigr)$. Therefore, by transitivity, we obtain

$$\mathcal{RT} \vdash \forall\bigl(\sigma' \to \exists W \,.\, (z = z\tau^j)\bigr). \tag{24}$$

Observe now that $\mathrm{vars}(z = z\sigma^i\sigma') = \{z\}$ and, as a consequence, we have $\mathrm{vars}(z = z\sigma^i\sigma') \cap W = \varnothing$. Therefore, by (23) and (24), we obtain

$$\begin{aligned}
&\mathcal{RT} \vdash \forall\bigl(\sigma' \to (z = z\sigma^i\sigma' \wedge \exists W \,.\, z = z\tau^j)\bigr)\\
&\quad\iff \mathcal{RT} \vdash \forall\bigl(\sigma' \to \exists W \,.\, (z = z\sigma^i\sigma' \wedge z = z\tau^j)\bigr)\\
&\quad\iff \mathcal{RT} \vdash \forall\bigl(\sigma' \to \exists W \,.\, (z\sigma^i\sigma' = z\tau^j)\bigr).
\end{aligned}$$

But this contradicts (22), so that the assumption was false and $z \in \mathrm{hvars}(\tau)$. As the choice of z was arbitrary, we have

$$\mathrm{hvars}(\sigma) \setminus W \subseteq \mathrm{hvars}(\tau) \setminus W.$$

The reverse inclusion follows by symmetry. ∎

B.5. Abstracting Finiteness

LEMMA 62. *Suppose* $\sigma, \tau \in \mathit{RSubst}$ *such that* $T \vdash \forall(\sigma \leftrightarrow \tau)$ *for any syntactic equality theory* T*. Then* $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\tau)$*.*

Proof. We assume that the congruence and the identity axioms hold. By Theorem 48 and Lemma 59, there exists $\sigma', \tau' \in \mathit{VSubst}$ such that $\sigma \iff \sigma'$, $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma')$, $\tau \iff \tau'$ and $\mathrm{hvars}(\tau) = \mathrm{hvars}(\tau')$. By hypothesis, $\sigma \iff \tau$ so that $\sigma' \iff \tau'$. By Lemma 60, $\mathrm{hvars}(\sigma') = \mathrm{hvars}(\tau')$. Therefore $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\tau)$. ∎

COROLLARY 63. *Let* $e \subseteq \mathit{Eqs}$ *be satisfiable in the syntactic equality theory* T*. If* $\sigma, \tau \in \mathrm{mgs}(e)$*, then* $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\tau)$*.*

Proof. By definition of mgs, we have $\sigma, \tau \in \mathit{RSubst}$ and $\sigma \iff e \iff \tau$. Thus, the result follows by Lemma 62. ∎

Proof of Theorem 17 on page 15. By Definition 16, we have $\alpha_H(\sigma) = \mathrm{hvars}(\sigma) \cap \mathit{VI}$ and $\alpha_H(\sigma') = \mathrm{hvars}(\sigma') \cap \mathit{VI}$. The result is a simple consequence of Lemma 62, since $\mathcal{RT}$ is a syntactic equality theory and $\mathcal{RT} \vdash \forall(\sigma \leftrightarrow \sigma')$. ∎

B.6. Correctness of Abstract Unification on $H \times P$

LEMMA 64. *Let* $\sigma \in \mathit{VSubst}$ *be satisfiable in a syntactic equality theory* T*. Let* $s \in \mathit{HTerms} \cap \mathit{GTerms}$ *and* $t \in \mathit{HTerms}$ *and suppose that* $T \vdash \forall(\sigma \rightarrow s = t)$*. Then* $s = t\sigma$*.*

Proof. Since $s \in \mathit{GTerms}$, we must have $s = f(s_1, \ldots, s_m)$ where $m \geq 0$. Moreover, by the assumption of the existence of two different function symbols in the signature *Sig*, there exists a term $r \in \mathit{HTerms} \cap \mathit{GTerms}$ whose top-level function symbol is distinct from that in s. Thus we have, by the identity axioms, $T \vdash \forall(r \neq s)$. Note also that, by Lemma 41 and the congruence axioms, we have $T \vdash \forall(\sigma \rightarrow s = t\sigma)$.

We show that $s = t\sigma$ by induction on the size of s.

First we show that $t\sigma$ is not a variable. In order to prove this, we suppose that $t\sigma = y \in \mathit{Vars}$ and derive a contradiction. If $y \notin \mathrm{dom}(\sigma)$ then, by Lemma 40, $\sigma' = \sigma \cup \{y \mapsto r\} \in \mathit{RSubst}$ and σ' is satisfiable in T. Therefore, using the congruence axioms, $T \vdash \forall(\sigma' \rightarrow r = s)$, which is a contradiction. If otherwise $t\sigma = y \in \mathrm{dom}(\sigma)$ then, since $\sigma \in \mathit{VSubst}$, we have $y \in \mathrm{vars}(y\sigma)$ so that, for all $i > 0$, $\mathrm{size}(t\sigma^{i+1}) > \mathrm{size}(t\sigma^i)$. Thus, by Lemma 44, there exists an index $j > 0$ such that $T \vdash \forall(s \neq t\sigma^j)$. However, by the hypothesis and Lemma 41, we have $T \vdash \forall(\sigma \rightarrow s = t\sigma^i)$ for all $i \geq 0$, therefore obtaining a contradiction. Thus $t\sigma \notin \mathit{Vars}$.

Therefore, by the identity axioms, we can assume that $t\sigma = f(t_1, \ldots, t_m)$. If $\mathrm{size}(s) = 1$, then $m = 0$ so that, by the congruence axioms, $s = t\sigma$. If $\mathrm{size}(s) > 1$, then $m > 0$ and, by the identity axioms, we have that $T \vdash \forall(\sigma \rightarrow s_i = t_i)$, for each $i = 1, \ldots, m$. Note that, for each $i = 1, \ldots, m$, we have $s_i \in \mathit{HTerms} \cap \mathit{GTerms}$, $t_i \in \mathit{HTerms}$ and $\mathrm{size}(s_i) < \mathrm{size}(s)$, so that we can apply the inductive hypothesis, obtaining $s_i = t_i\sigma$. Thus, by the congruence axioms, $s = t\sigma\sigma$. Thus $t\sigma\sigma \in \mathit{GTerms}$ so that $\mathrm{vars}(t\sigma\sigma) = \varnothing$. As $\sigma \in \mathit{VSubst}$, we have $\mathrm{vars}(t\sigma) = \varnothing$ so that $t\sigma\sigma = t\sigma$. Hence $s = t\sigma$. ∎

Lemma 65. *Let $\bar{s} = (s_1, \ldots, s_n) \in HTerms^n$ be linear, and suppose the tuple of terms $\bar{t} = (t_1, \ldots, t_n) \in HTerms^n$ is such that* $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$ *and* $\mathrm{mgs}(\bar{s} = \bar{t}) \neq \varnothing$. *Then there exists* $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$ *such that, for each variable* $z \in \mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})\bigr)$, *we have* $\mathrm{vars}(z\mu) \cap \mathrm{dom}(\mu) = \varnothing$.

Proof. We assume that the congruence and identity axioms hold. The proof is by induction on the number of variables in $\mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t})$.

Suppose first that, for some $i = 1, \ldots, n$, we have $s_i = f(r_1, \ldots, r_m)$ and $t_i = f(u_1, \ldots, u_m)$ (with $m \geq 0$). Let

$$\bar{s}' \stackrel{\mathrm{def}}{=} (s_1, \ldots, s_{i-1}, r_1, \ldots, r_m, s_{i+1}, \ldots, s_n),$$
$$\bar{t}' \stackrel{\mathrm{def}}{=} (t_1, \ldots, t_{i-1}, u_1, \ldots, u_m, t_{i+1}, \ldots, t_n).$$

Then $\mathrm{mvars}(\bar{s}') = \mathrm{mvars}(\bar{s})$ and $\mathrm{mvars}(\bar{t}') = \mathrm{mvars}(\bar{t})$ so that, as $\bar{s}$ is linear, $\bar{s}'$ is linear, $\mathrm{vars}(\bar{s}') \cap \mathrm{nlvars}(\bar{t}') = \varnothing$ and $\mathrm{vars}(\bar{s}') \cap \mathrm{vars}(\bar{t}') = \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})$. Moreover, by the congruence axiom (9), $\mathrm{mgs}(\bar{s}' = \bar{t}') = \mathrm{mgs}(\bar{s} = \bar{t})$. We repeat this process until all terms in $\bar{s}'$ and $\bar{t}'$ can not be decomposed any further. (Note that in the case that s_i and t_i are identical constants, we can remove them from $\bar{s}'$ and $\bar{t}'$, since the corresponding equation $s_i = t_i$ holds vacuously.) Thus, as $\bar{s}$ and $\bar{t}$ are finite sequences of finite terms, we can assume that, for all $i = 1, \ldots, n$, either $s_i \in Vars$ or $t_i \in Vars$.

Secondly, suppose that for some $i = 1, \ldots, n$, $s_i = t_i$. By the previous paragraph, we can assume that $s_i \in Vars$. Let

$$\bar{s}_i \stackrel{\mathrm{def}}{=} (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n),$$
$$\bar{t}_i \stackrel{\mathrm{def}}{=} (t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n).$$

Then $\mathrm{mvars}(\bar{s}_i) \cup \{s_i\} = \mathrm{mvars}(\bar{s})$ and $\mathrm{mvars}(\bar{t}_i) \cup \{s_i\} = \mathrm{mvars}(\bar{t})$ so that, as $\bar{s}$ is linear, $\bar{s}_i$ is linear, $\mathrm{vars}(\bar{s}_i) \cap \mathrm{nlvars}(\bar{t}_i) = \varnothing$ and

$$\bigl(\mathrm{vars}(\bar{s}_i) \cap \mathrm{vars}(\bar{t}_i)\bigr) \cup \{s_i\} = \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t}).$$

As $\bar{s}$ is linear and $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$, $s_i \notin \mathrm{vars}(\bar{s}_i) \cup \mathrm{vars}(\bar{t}_i)$ and hence, for all $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$, we have $s_i \notin \mathrm{dom}(\mu)$. Therefore

$$\mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})\bigr) = \mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}_i) \cap \mathrm{vars}(\bar{t}_i)\bigr).$$

Furthermore, by the congruence axiom (6), $\mathrm{mgs}(\bar{s}_i = \bar{t}_i) = \mathrm{mgs}(\bar{s} = \bar{t})$. Thus, as $\bar{s}$ and $\bar{t}$ are sequences of finite length n, we can assume that $s_i \neq t_i$, for all $i = 1, \ldots, n$.

Therefore, for the rest of the proof, we will assume that for each $i = 1, \ldots, n$, $s_i \neq t_i$ and either $s_i \in Vars$ or $t_i \in Vars$.

For the base case, we have $\mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t}) = \varnothing$ and the result holds.

For the inductive step, $\mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t}) \neq \varnothing$ so that $n > 0$. As the order of the equations in $\bar{s} = \bar{t}$ is not relevant to the hypothesis, we assume, without loss of generality that if, for some $i = 1, \ldots, n$, $\mathrm{vars}(s_i) \cap \mathrm{vars}(t_i) = \varnothing$, then $\mathrm{vars}(s_1) \cap \mathrm{vars}(t_1) = \varnothing$. There are three cases we consider separately:

a. for all $i = 1, \ldots, n$, $\mathrm{vars}(s_i) \cap \mathrm{vars}(t_i) \neq \varnothing$;

b. $s_1 \in Vars \setminus \mathrm{vars}(t_1)$;

c. $t_1 \in \mathit{Vars} \setminus \mathrm{vars}(s_1)$.

Case a. For all $i = 1, \ldots, n$, $\mathrm{vars}(s_i) \cap \mathrm{vars}(t_i) \neq \varnothing$.

For each $i = 1, \ldots, n$, we are assuming that either $s_i \in \mathit{Vars}$ or $t_i \in \mathit{Vars}$, Therefore, for each $i = 1, \ldots, n$, $s_i \in \mathrm{vars}(t_i)$ or $t_i \in \mathrm{vars}(s_i)$ so that, without loss of generality, we can assume, for some k, where $0 \leq k \leq n$, $s_i \in \mathit{Vars}$ if $1 \leq i \leq k$ and $t_i \in \mathit{Vars}$ if $k+1 \leq i \leq n$.

Let

$$\mu \stackrel{\mathrm{def}}{=} \{s_1 = t_1, \ldots, s_k = t_k\} \cup \{t_{k+1} = s_{k+1}, \ldots, t_n = s_n\}.$$

We now show that $\mu \subseteq \mathit{Eqs}$ is in rational solved form. As $\bar{s}$ is linear, $(s_1, \ldots, s_k)$ is linear. As $\bar{s}$ is linear and $t_i \in \mathrm{vars}(s_i)$ if $k+1 \leq i \leq n$, then $(t_{k+1}, \ldots, t_n)$ is linear and $\{s_1, \ldots, s_k\} \cap \{t_{k+1}, \ldots, t_n\} = \varnothing$. As we are assuming that, for all $i = 1$, $\ldots$, n, $s_i \neq t_i$ and $\mathrm{vars}(s_i) \cap \mathrm{vars}(t_i) \neq \varnothing$, it follows that $t_i \notin \mathit{Vars}$ when $1 \leq i \leq k$ and $s_i \notin \mathit{Vars}$ when $k+1 \leq i \leq n$, so that each equation in μ is a binding and μ has no circular subsets. Thus $\mu \in \mathit{RSubst}$ and hence, by the congruence axiom (7), $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$.

As $s_i \in \mathrm{vars}(t_i)$ when $1 \leq i \leq k$ and $t_i \in \mathrm{vars}(s_i)$ when $k+1 \leq i \leq n$, $\mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})\bigr) = \varnothing$. Therefore the required result holds.

Case b. $s_1 \in \mathit{Vars} \setminus \mathrm{vars}(t_1)$.

Let

$$\begin{aligned} \bar{s}_1 &\stackrel{\mathrm{def}}{=} (s_2, \ldots, s_n), \\ \bar{t}_1 &\stackrel{\mathrm{def}}{=} \bigl(t_2\{s_1 \mapsto t_1\}, \ldots, t_n\{s_1 \mapsto t_1\}\bigr). \end{aligned} \tag{25}$$

As $\bar{s}$ is linear, $s_1 \notin \mathrm{vars}(\bar{s}_1)$. Also, all occurrences of s_1 in $\bar{t}$ are replaced in $\bar{t}_1$ by t_1 so that, as $s_1 \notin \mathrm{vars}(t_1)$, $s_1 \notin \mathrm{vars}(\bar{t}_1)$. Thus

$$s_1 \notin \mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1). \tag{26}$$

Therefore $\mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1) \subset \mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t})$. Now since $\bar{s}$ is linear, $\bar{s}_1$ is linear. Thus, to apply the inductive hypothesis to $\bar{s}_1$ and $\bar{t}_1$, we have to show that

$$\mathrm{vars}(\bar{s}_1) \cap \mathrm{nlvars}(\bar{t}_1) = \varnothing. \tag{27}$$

Suppose that $u \in \mathrm{vars}(\bar{s}_1)$ so that $u \in \mathrm{vars}(\bar{s})$. Now, by hypothesis, we have $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$. Thus $s_1, u \notin \mathrm{nlvars}(\bar{t})$. If $u \in \mathrm{vars}\bigl((t_2, \ldots, t_n)\bigr)$ so that $u \notin \mathrm{vars}(t_1)$, then $u \notin \mathrm{nlvars}(\bar{t}_1)$. On the other hand, if $u \notin \mathrm{vars}\bigl((t_2, \ldots, t_n)\bigr)$, then, as $s_1 \notin \mathrm{nlvars}\bigl((t_2, \ldots, t_n)\bigr)$ and $u \notin \mathrm{nlvars}(t_1)$, $u \notin \mathrm{nlvars}(\bar{t}_1)$. Thus, for all $u \in \mathrm{vars}(\bar{s}_1)$, $u \notin \mathrm{nlvars}(\bar{t}_1)$. Hence (27) holds. It follows that the inductive hypothesis for $\bar{s}_1$ and $\bar{t}_1$ holds. Therefore there exists $\mu_1 \in \mathit{RSubst}$ where

$$\mu_1 \in \mathrm{mgs}(\bar{s}_1 = \bar{t}_1)$$

such that, for each $z \in \mathrm{dom}(\mu_1) \setminus \bigl(\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)\bigr)$, $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$.

Let

$$\mu \stackrel{\mathrm{def}}{=} \{s_1 = t_1\mu_1\} \cup \mu_1. \tag{28}$$

We now show that $\mu \subseteq \mathit{Eqs}$ is in $\mathrm{mgs}(\bar{s} = \bar{t})$. First we show that μ is in rational solved form. By (26),

$$s_1 \notin \mathrm{vars}(\mu_1), \tag{29}$$

and, as $s_1 \notin \mathrm{vars}(t_1)$, we have

$$s_1 \notin \mathrm{vars}(t_1\mu_1). \tag{30}$$

Thus, as $\mu_1 \in \mathit{RSubst}$, μ has no identities or circular subsets so that $\mu \in \mathit{RSubst}$. By Lemma 42, $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$.

Let

$$z \in \mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})\bigr). \tag{31}$$

Then we have to show that

$$\mathrm{vars}(z\mu) \cap \mathrm{dom}(\mu) = \varnothing. \tag{32}$$

It follows from (28) and (31) that either $z \in \mathrm{dom}(\mu_1)$ so that $z\mu = z\mu_1$ or $z = s_1$ and $z\mu = t_1\mu_1$. We consider these two cases separately.

Suppose first that $z \in \mathrm{dom}(\mu_1)$. By (25), we have both $\mathrm{vars}(\bar{s}_1) \subseteq \mathrm{vars}(\bar{s})$ and $\mathrm{vars}(\bar{t}_1) \subseteq \mathrm{vars}(\bar{t})$, so that $\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1) \subseteq \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})$. Hence we have $z \in \mathrm{dom}(\mu_1) \setminus \bigl(\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)\bigr)$. Thus we obtain, by the inductive hypothesis, $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Now, as $z \in \mathrm{dom}(\mu_1)$ and (29) holds, $s_1 \notin \mathrm{vars}(z\mu_1)$. Thus, as $\mathrm{dom}(\mu) = \mathrm{dom}(\mu_1) \cup \{s_1\}$, $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu) = \varnothing$. Hence, as $z\mu = z\mu_1$, (32) holds.

Secondly suppose that $z = s_1$. Then we have that $s_1 \notin \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})$. Hence $\bar{t}_1 = (t_2, \ldots, t_n)$. Let u be any variable in $\mathrm{vars}(t_1)$. Then we have that $u \notin \mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)$, since $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$, If $u \in \mathrm{dom}(\mu_1)$, then we can apply the inductive hypothesis to obtain $\mathrm{vars}(u\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. On the other hand, if $u \notin \mathrm{dom}(\mu_1)$, we have $u = u\mu_1$ and $\mathrm{vars}(u\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Hence $\mathrm{vars}(t_1\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Thus, as $\mathrm{dom}(\mu) = \mathrm{dom}(\mu_1) \cup \{s_1\}$, by (30), $\mathrm{vars}(t_1\mu_1) \cap \mathrm{dom}(\mu) = \varnothing$. Therefore, as $z\mu = t_1\mu_1$, (32) holds.

Case c. $t_1 \in \mathit{Vars} \setminus \mathrm{vars}(s_1)$.

Let

$$\begin{aligned} \bar{s}_1 &\stackrel{\mathrm{def}}{=} \bigl(s_2\{t_1 \mapsto s_1\}, \ldots, s_n\{t_1 \mapsto s_1\}\bigr), \\ \bar{t}_1 &\stackrel{\mathrm{def}}{=} \bigl(t_2\{t_1 \mapsto s_1\}, \ldots, t_n\{t_1 \mapsto s_1\}\bigr). \end{aligned} \tag{33}$$

All occurrences of t_1 in $\bar{s}$ and $\bar{t}$ are replaced in $\bar{s}_1$ and $\bar{t}_1$ by s_1 so that, since $t_1 \notin \mathrm{vars}(s_1)$,

$$t_1 \notin \mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1). \tag{34}$$

Therefore $\mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1) \subset \mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t})$. Now, $\bar{s}_1$ is linear since $\bar{s}$ is linear. Thus, to apply the inductive hypothesis to $\bar{s}_1$ and $\bar{t}_1$, we have to show that

$$\mathrm{vars}(\bar{s}_1) \cap \mathrm{nlvars}(\bar{t}_1) = \varnothing. \tag{35}$$

Suppose u is any variable in $\mathrm{vars}(\bar{s}_1)$. Then either $u \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$ or we have $u \in \mathrm{vars}(s_1)$ and $t_1 \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$. By hypothesis, $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$, so that $u \notin \mathrm{nlvars}(\bar{t})$. If $u \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$, then, as $\bar{s}$ is linear, $u \notin \mathrm{vars}(s_1)$. Thus, it follows from (33) that $u \notin \mathrm{nlvars}(\bar{t}_1)$. If $t_1 \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$, then we have $t_1 \notin \mathrm{vars}\bigl((t_2, \ldots, t_n)\bigr)$ so that, again by (33), $\bar{t}_1 = (t_2, \ldots, t_n)$. Thus, for all $u \in \mathrm{vars}(\bar{s}_1)$, $u \notin \mathrm{nlvars}(\bar{t}_1)$. Hence (35) holds. It follows that the inductive hypothesis for $\bar{s}_1$ and $\bar{t}_1$ holds. Therefore there exists $\mu_1 \in \mathit{RSubst}$ where

$$\mu_1 \in \mathrm{mgs}(\bar{s}_1 = \bar{t}_1)$$

such that, for each $z \in \mathrm{dom}(\mu_1) \setminus \bigl(\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)\bigr)$, we have $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$.

Let

$$\mu \stackrel{\mathrm{def}}{=} \{t_1 = s_1\mu_1\} \cup \mu_1. \tag{36}$$

We now show that $\mu \subseteq \mathit{Eqs}$ is in $\mathrm{mgs}(\bar{s} = \bar{t})$. First we show that μ is in rational solved form. By (34),

$$t_1 \notin \mathrm{vars}(\mu_1), \tag{37}$$

and, as $t_1 \notin \mathrm{vars}(s_1)$, we have

$$t_1 \notin \mathrm{vars}(s_1\mu_1). \tag{38}$$

Thus, as $\mu_1 \in \mathit{RSubst}$, μ has no identities or circular subsets so that $\mu \in \mathit{RSubst}$. By Lemma 42, $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$.

Let

$$z \in \mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})\bigr). \tag{39}$$

Then we have to show that

$$\mathrm{vars}(z\mu) \cap \mathrm{dom}(\mu) = \varnothing. \tag{40}$$

It follows from (36) and (39) that either $z \in \mathrm{dom}(\mu_1)$ so that $z\mu = z\mu_1$ or $z = t_1$ and $z\mu = s_1\mu_1$. We consider these two cases separately.

Suppose first that $z \in \mathrm{dom}(\mu_1)$. To apply the inductive hypothesis to z, we need to show that,

$$\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1) \subseteq \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t}).$$

To see this, let $u \in \mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)$. Then, by (33), either $u \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$ or $u \in \mathrm{vars}(s_1)$ and $t_1 \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$. If $u \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$, then we have $u \in \mathrm{vars}(\bar{s})$ so that, as $\bar{s}$ is linear, we have also $u \notin \mathrm{vars}(s_1)$ and hence $u \in \mathrm{vars}\bigl((t_2, \ldots, t_n)\bigr)$. Alternatively, if $u \in \mathrm{vars}(s_1)$ and $t_1 \in \mathrm{vars}\bigl((s_2, \ldots, s_n)\bigr)$, then $u, t_1 \in \mathrm{vars}(\bar{s})$. Moreover, by hypothesis, $\mathrm{vars}(\bar{s}) \cap \mathrm{nlvars}(\bar{t}) = \varnothing$, so that $t_1 \notin \mathrm{vars}\bigl((t_2, \ldots, t_n)\bigr)$. Thus $\bar{t}_1 = (t_2, \ldots, t_n)$ and hence $u \in \mathrm{vars}(\bar{t})$. Therefore, in both cases, $u \in \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})$. It follows that $z \in \mathrm{dom}(\mu_1) \setminus \bigl(\mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)\bigr)$. Thus, by the inductive hypothesis, we have $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Now, as $z \in \mathrm{dom}(\mu_1)$ and (37) holds, $t_1 \notin \mathrm{vars}(z\mu_1)$. Thus, as $\mathrm{dom}(\mu) = \mathrm{dom}(\mu_1) \cup \{t_1\}$, $\mathrm{vars}(z\mu_1) \cap \mathrm{dom}(\mu) = \varnothing$. Hence, as $z\mu = z\mu_1$, (40) holds.

Secondly, suppose that $z = t_1$. Then $t_1 \notin \mathrm{vars}(\bar{s}) \cap \mathrm{vars}(\bar{t})$ and, consequently, $\bar{s}_1 = (s_2, \ldots, s_n)$. Let u be any variable in $\mathrm{vars}(s_1)$. Then, as $\bar{s}$ is linear, we have $u \notin \mathrm{vars}(\bar{s}_1)$ so that $u \notin \mathrm{vars}(\bar{s}_1) \cap \mathrm{vars}(\bar{t}_1)$. Thus, if $u \in \mathrm{dom}(\mu_1)$, we can apply the inductive hypothesis to u and obtain $\mathrm{vars}(u\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. On the other hand, if $u \notin \mathrm{dom}(\mu_1)$, $u = u\mu_1$ and $\mathrm{vars}(u\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Hence $\mathrm{vars}(s_1\mu_1) \cap \mathrm{dom}(\mu_1) = \varnothing$. Thus, as $\mathrm{dom}(\mu) = \mathrm{dom}(\mu_1) \cup \{t_1\}$, by (38), $\mathrm{vars}(s_1\mu_1) \cap \mathrm{dom}(\mu) = \varnothing$. Therefore, as $z\mu = s_1\mu_1$, (40) holds. ∎

Lemma 66. *Suppose that the tuple of terms $\bar{s} \stackrel{\mathrm{def}}{=} (s_1, \ldots, s_n) \in \mathit{HTerms}^n$ is linear, $\bar{t} \stackrel{\mathrm{def}}{=} (t_1, \ldots, t_n) \in \mathit{HTerms}^n$ and $\mathrm{mgs}(\bar{s} = \bar{t}) \neq \varnothing$. Then there exists $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$ and, for each $z \in \mathrm{dom}(\mu) \setminus \mathrm{vars}(\bar{s})$, the following properties hold:*

1. $\mathrm{vars}(z\mu) \subseteq \mathrm{vars}(\bar{s})$;

2. $\text{vars}(z\mu) \cap \text{dom}(\mu) = \varnothing$.

Proof. We assume that the congruence and identity axioms hold. The proof is by induction on the number of variables in $\text{vars}(\bar{s}) \cup \text{vars}(\bar{t})$.

Suppose first that, for some $i = 1, \ldots, n$, we have $s_i = f(r_1, \ldots, r_m)$ and $t_i = f(u_1, \ldots, u_m)$ $(m \geq 0)$. Let

$$\bar{s}' \stackrel{\text{def}}{=} (s_1, \ldots, s_{i-1}, r_1, \ldots, r_m, s_{i+1}, \ldots, s_n),$$
$$\bar{t}' \stackrel{\text{def}}{=} (t_1, \ldots, t_{i-1}, u_1, \ldots, u_m, t_{i+1}, \ldots, t_n).$$

Then $\text{mvars}(\bar{s}') = \text{mvars}(\bar{s})$ and $\text{mvars}(\bar{t}') = \text{mvars}(\bar{t})$ so that, as $\bar{s}$ is linear, $\bar{s}'$ is linear. Moreover, by the congruence axiom (9), $\text{mgs}(\bar{s}' = \bar{t}') = \text{mgs}(\bar{s} = \bar{t})$. We repeat this process until all terms in $\bar{s}'$ and $\bar{t}'$ can not be decomposed any further. (Note that in the case that s_i and t_i are identical constants, we can remove them from $\bar{s}'$ and $\bar{t}'$, since the corresponding equation $s_i = t_i$ holds vacuously.) Thus, as $\bar{s}$ and $\bar{t}$ are finite sequences of finite terms, we can assume that, for all $i = 1, \ldots, n$, either $s_i \in \mathit{Vars}$ or $t_i \in \mathit{Vars}$.

Secondly, suppose that for some $i = 1, \ldots, n$, $s_i = t_i$. By the previous paragraph, we can assume that $s_i \in \mathit{Vars}$. Let

$$\bar{s}_i \stackrel{\text{def}}{=} (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n),$$
$$\bar{t}_i \stackrel{\text{def}}{=} (t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n).$$

Then $\text{mvars}(\bar{s}_i) \cup \{s_i\} = \text{mvars}(\bar{s})$ and $\text{mvars}(\bar{t}_i) \cup \{s_i\} = \text{mvars}(\bar{t})$ so that, as $\bar{s}$ is linear, $\bar{s}_i$ is linear. Therefore

$$\text{dom}(\mu) \setminus \text{vars}(\bar{s}) \subseteq \text{dom}(\mu) \setminus \text{vars}(\bar{s}_i).$$

Furthermore, by the congruence axiom (6), $\text{mgs}(\bar{s}_i = \bar{t}_i) = \text{mgs}(\bar{s} = \bar{t})$. Thus, as $\bar{s}$ and $\bar{t}$ are sequences of finite length n, we can assume that $s_i \neq t_i$, for all $i = 1, \ldots, n$.

Therefore, for the rest of the proof, we will assume that $s_i \neq t_i$ and either $s_i \in \mathit{Vars}$ or $t_i \in \mathit{Vars}$, for all $i = 1, \ldots, n$.

For the base case, we have $\text{vars}(\bar{s}) \cup \text{vars}(\bar{t}) = \varnothing$ and the result holds.

For the inductive step, $\text{vars}(\bar{s}) \cup \text{vars}(\bar{t}) \neq \varnothing$ so that $n > 0$. As the order of the equations in $\bar{s} = \bar{t}$ is not relevant to the hypothesis, we assume, without loss of generality that if, for some $i = 1, \ldots, n$, $\text{vars}(s_i) \cap \text{vars}(t_i) = \varnothing$ then, we have $\text{vars}(s_1) \cap \text{vars}(t_1) = \varnothing$. There are four cases we consider separately:

a. for all $i = 1, \ldots, n$, $\text{vars}(s_i) \cap \text{vars}(t_i) \neq \varnothing$;

b. $s_1 \in \mathit{Vars} \setminus \text{vars}(t_1)$;

c. $t_1 \in \mathit{Vars} \setminus \text{vars}(\bar{s})$ and $s_1 \notin \mathit{Vars}$;

d. $t_1 \in \text{vars}(\bar{s}) \setminus \text{vars}(s_1)$ and $s_1 \notin \mathit{Vars}$.

Case a. For all $i = 1, \ldots, n$, $\text{vars}(s_i) \cap \text{vars}(t_i) \neq \varnothing$.

For each $i = 1, \ldots, n$, we are assuming that either $s_i \in \mathit{Vars}$ or $t_i \in \mathit{Vars}$, Therefore, for each $i = 1, \ldots, n$, $s_i \in \text{vars}(t_i)$ or $t_i \in \text{vars}(s_i)$ so that, without loss of generality, we can assume, for some k, where $0 \leq k \leq n$, $s_i \in \mathit{Vars}$ if $1 \leq i \leq k$ and $t_i \in \mathit{Vars}$ if $k + 1 \leq i \leq n$.

Let

$$\mu \stackrel{\text{def}}{=} \{s_1 = t_1, \dots, s_k = t_k\} \cup \{t_{k+1} = s_{k+1}, \dots, t_n = s_n\}.$$

We show that $\mu \subseteq \mathit{Eqs}$ is in $\mathrm{mgs}(\bar{s} = \bar{t})$. First we must show that $\mu \in \mathit{RSubst}$. As $\bar{s}$ is linear, $(s_1, \dots, s_k)$ is linear. As $\bar{s}$ is linear and $t_i \in \mathrm{vars}(s_i)$ if $k+1 \leq i \leq n$, then $(t_{k+1}, \dots, t_n)$ is linear and $\{s_1, \dots, s_k\} \cap \{t_{k+1}, \dots, t_n\} = \varnothing$. As we are assuming that, for all $i = 1, \dots, n$, $s_i \neq t_i$ and $\mathrm{vars}(s_i) \cap \mathrm{vars}(t_i) \neq \varnothing$, it follows that $t_i \notin \mathit{Vars}$ when $1 \leq i \leq k$ and $s_i \notin \mathit{Vars}$ when $k+1 \leq i \leq n$, so that each equation in μ is a binding and μ has no circular subsets. Thus $\mu \in \mathit{RSubst}$ and hence, by the congruence axiom (7), $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$.

As $\{t_{k+1}, \dots, t_n\} \subseteq \mathrm{vars}\big((s_{k+1}, \dots, s_n)\big)$, we have $\mathrm{dom}(\mu) \setminus \mathrm{vars}(\bar{s}) = \varnothing$. Therefore the required result holds.

Case b. $s_1 \in \mathit{Vars} \setminus \mathrm{vars}(t_1)$.

Let

$$\bar{s}_1 \stackrel{\text{def}}{=} (s_2, \dots, s_n),$$
$$\bar{t}_1 \stackrel{\text{def}}{=} \big(t_2\{s_1 \mapsto t_1\}, \dots, t_n\{s_1 \mapsto t_1\}\big).$$

As $\bar{s}$ is linear, $\bar{s}_1$ is linear and $s_1 \notin \mathrm{vars}(\bar{s}_1)$. Also, all occurrences of s_1 in $\bar{t}$ are replaced in $\bar{t}_1$ by t_1 so that, as $s_1 \notin \mathrm{vars}(t_1)$ (by the assumption for this case), $s_1 \notin \mathrm{vars}(\bar{t}_1)$. Thus

$$s_1 \notin \mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1). \tag{41}$$

It follows that $\mathrm{vars}(\bar{s}_1) \cup \mathrm{vars}(\bar{t}_1) \subset \mathrm{vars}(\bar{s}) \cup \mathrm{vars}(\bar{t})$ so that the inductive hypothesis applies to $\bar{s}_1$ and $\bar{t}_1$. Thus there exists $\mu_1 \in \mathit{RSubst}$ where

$$\mu_1 \in \mathrm{mgs}(\bar{s}_1 = \bar{t}_1)$$

such that, for each $z \in \mathrm{dom}(\mu_1) \setminus \mathrm{vars}(\bar{s}_1)$, properties 1 and 2 hold using μ_1 and $\bar{s}_1$.

Let

$$\mu \stackrel{\text{def}}{=} \{s_1 = t_1\mu_1\} \cup \mu_1.$$

We show that $\mu \subseteq \mathit{Eqs}$ is in $\mathrm{mgs}(\bar{s} = \bar{t})$. By (41), we have $s_1 \notin \mathrm{vars}(\mu_1)$ so that $s_1 \notin \mathrm{dom}(\mu_1)$. Also, since $\mu_1 \in \mathit{RSubst}$, μ has no identities or circular subsets. Thus we have $\mu \in \mathit{RSubst}$. By Lemma 42, $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$.

Suppose that $z \in \mathrm{dom}(\mu) \setminus \mathrm{vars}(\bar{s})$. As

$$\mathrm{vars}(\bar{s}_1) \cup \{s_1\} = \mathrm{vars}(\bar{s})$$

and

$$\mathrm{dom}(\mu_1) \cup \{s_1\} = \mathrm{dom}(\mu),$$

we have

$$\mathrm{dom}(\mu_1) \setminus \mathrm{vars}(\bar{s}_1) = \mathrm{dom}(\mu) \setminus \mathrm{vars}(\bar{s}). \tag{42}$$

Therefore $z \in \mathrm{dom}(\mu_1) \setminus \mathrm{vars}(\bar{s}_1)$ and $z\mu_1 = z\mu$. Thus the inductive properties 1 and 2 using μ_1 and $\bar{s}_1$ can be applied to z. We show that properties 1 and 2 using μ and $\bar{s}$ can be applied to z.

1. By property 1, $\mathrm{vars}(z\mu) \subseteq \mathrm{vars}(\bar{s}_1)$ and hence, $\mathrm{vars}(z\mu) \subseteq \mathrm{vars}(\bar{s})$.

2. By property 2, we have $\text{vars}(z\mu) \cap \text{dom}(\mu_1) = \varnothing$. Now $s_1 \notin \text{vars}(z\mu)$ because $s_1 \notin \text{vars}(\bar{s}_1)$ (since $\bar{s}$ is linear) and $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s}_1)$ (by property 1). Thus, as $\text{dom}(\mu) = \text{dom}(\mu_1) \cup \{s_1\}$, we have $\text{vars}(z\mu) \cap \text{dom}(\mu) = \varnothing$.

Case c. Assume that $t_1 \in \mathit{Vars} \setminus \text{vars}(\bar{s})$ and $s_1 \notin \mathit{Vars}$.
Let

$$\bar{s}_1 \stackrel{\text{def}}{=} (s_2, \ldots, s_n),$$
$$\bar{t}_1 \stackrel{\text{def}}{=} \bigl(t_2\{t_1 \mapsto s_1\}, \ldots, t_n\{t_1 \mapsto s_1\}\bigr).$$

As $\bar{s}$ is linear, $\bar{s}_1$ is linear. By the assumption for this case, $t_1 \notin \text{vars}(\bar{s}_1)$. Also, all occurrences of t_1 in $\bar{t}$ are replaced in $\bar{t}_1$ by s_1 so that $t_1 \notin \text{vars}(\bar{t}_1)$. Thus

$$t_1 \notin \text{vars}(\bar{s}_1) \cup \text{vars}(\bar{t}_1). \tag{43}$$

It follows that $\text{vars}(\bar{s}_1) \cup \text{vars}(\bar{t}_1) \subset \text{vars}(\bar{s}) \cup \text{vars}(\bar{t})$ so that we can apply the inductive hypothesis to $\bar{s}_1$ and $\bar{t}_1$. Thus there exists $\mu_1 \in \mathit{RSubst}$ where

$$\mu_1 \in \text{mgs}(\bar{s}_1 = \bar{t}_1)$$

such that, for each $z \in \text{dom}(\mu_1) \setminus \text{vars}(\bar{s}_1)$, properties 1 and 2 hold using μ_1 and $\bar{s}_1$. Note that, by (43), $t_1 \notin \text{vars}(\mu_1)$ and, in particular, $t_1 \notin \text{dom}(\mu_1)$.

Let

$$\mu \stackrel{\text{def}}{=} \{t_1 = s_1\mu_1\} \cup \mu_1. \tag{44}$$

As $s_1 \notin \mathit{Vars}$ and $\mu_1 \in \mathit{RSubst}$, $\mu \in \mathit{Eqs}$ has no identities or circular subsets so that $\mu \in \mathit{RSubst}$. By Lemma 42, $\mu \in \text{mgs}(\bar{s} = \bar{t})$.

As $t_1 \in \text{dom}(\mu)$ (by (44)) and $t_1 \notin \text{vars}(\bar{s})$ (by the assumption for this case), we have

$$\text{dom}(\mu_1) \setminus \text{vars}(\bar{s}_1) \cup \{t_1\} = \text{dom}(\mu) \setminus \text{vars}(\bar{s}).$$

Suppose that $z \in \text{dom}(\mu) \setminus \text{vars}(\bar{s})$. Then either $z \neq t_1$ so that $z\mu = z\mu_1$ and the inductive properties 1 and 2 using μ_1 and $\bar{s}_1$ can be applied to z or $z = t_1$ and $z\mu = s_1\mu_1$. We show that properties 1 and 2 using μ and $\bar{s}$ can be applied to z.

1. Suppose $z \neq t_1$ so that $z\mu = z\mu_1$. Using property 1, $\text{vars}(z\mu_1) \subseteq \text{vars}(\bar{s}_1)$. As $\text{vars}(\bar{s}_1) \subseteq \text{vars}(\bar{s})$, it follows that $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s})$.

   Suppose that $z = t_1$ so that $z\mu = s_1\mu_1$. Let u be any variable in s_1. As $\bar{s}$ is linear, $u \notin \text{vars}(\bar{s}_1)$. Thus, if $u \in \text{dom}(\mu_1)$, we can use property 1 to derive that $\text{vars}(u\mu_1) \subseteq \text{vars}(\bar{s}_1)$. If $u \notin \text{dom}(\mu_1)$, then $u\mu_1 = u$ so that $\text{vars}(u\mu_1) \subseteq \text{vars}(s_1)$. Moreover $\text{vars}(s_1) \cup \text{vars}(\bar{s}_1) = \text{vars}(\bar{s})$ so that

   $$\text{vars}(s_1\mu_1) \subseteq \text{vars}(\bar{s}). \tag{45}$$

   Hence $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s})$.

2. Suppose $z \neq t_1$ so that $z\mu = z\mu_1$. Then, as property 2 holds, we have $\text{vars}(z\mu) \cap \text{dom}(\mu_1) = \varnothing$. Now $t_1 \notin \text{vars}(z\mu)$ because $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s}_1)$ (by property 1) and $t_1 \notin \text{vars}(\bar{s}_1)$ (by (43)). Thus, as $\text{dom}(\mu) = \text{dom}(\mu_1) \cup \{t_1\}$, we have $\text{vars}(z\mu) \cap \text{dom}(\mu) = \varnothing$.

   Suppose that $z = t_1$ so that $z\mu = s_1\mu_1$. Let u be any variable in $\text{vars}(s_1)$. Then, as $\bar{s}$ is linear, $u \notin \text{vars}(\bar{s}_1)$. Then either $u \in \text{dom}(\mu_1)$, and we can apply property 2 to u to obtain $\text{vars}(u\mu_1) \cap \text{dom}(\mu_1) = \varnothing$, or $u = u\mu_1$, and

$\text{vars}(u\mu_1) \cap \text{dom}(\mu_1) = \varnothing$. Hence we have $\text{vars}(s_1\mu_1) \cap \text{dom}(\mu_1) = \varnothing$. Now $t_1 \notin \text{vars}(s_1\mu_1)$ because $\text{vars}(s_1\mu_1) \subseteq \text{vars}(\bar{s})$ (by (45)) and $t_1 \notin \text{vars}(\bar{s})$ (by the assumption for this case). Thus, as $\text{dom}(\mu) = \text{dom}(\mu_1) \cup \{t_1\}$, we have $\text{vars}(z\mu) \cap \text{dom}(\mu) = \varnothing$.

Case d. Assume that $t_1 \in \text{vars}(\bar{s}) \setminus \text{vars}(s_1)$ and $s_1 \notin \mathit{Vars}$.
Let

$$\bar{s}_1 \stackrel{\text{def}}{=} \bigl(s_2\{t_1 \mapsto s_1\}, \ldots, s_n\{t_1 \mapsto s_1\}\bigr),$$
$$\bar{t}_1 \stackrel{\text{def}}{=} \bigl(t_2\{t_1 \mapsto s_1\}, \ldots, t_n\{t_1 \mapsto s_1\}\bigr).$$

As $\bar{s}$ is linear, there is only one occurrence of t_1 in $\{s_2, \ldots, s_n\}$, and, in $\bar{s}_1$, this is replaced by s_1 which is also linear. Thus $\bar{s}_1$ is linear, $\bar{s}_1 \subseteq \bar{s}$ and $t_1 \notin \text{vars}(\bar{s}_1)$. Also, all occurrences of t_1 in $\bar{t}$ are replaced in $\bar{t}_1$ by s_1 so that $t_1 \notin \text{vars}(\bar{t}_1)$. Thus

$$t_1 \notin \text{vars}(\bar{s}_1) \cup \text{vars}(\bar{t}_1). \tag{46}$$

It follows that $\text{vars}(\bar{s}_1) \cup \text{vars}(\bar{t}_1) \subset \text{vars}(\bar{s}) \cup \text{vars}(\bar{t})$ so that we can apply the inductive hypothesis to $\bar{s}_1$ and $\bar{t}_1$. Thus, there exists $\mu_1 \in \mathit{RSubst}$ where

$$\mu_1 \in \text{mgs}(\bar{s}_1 = \bar{t}_1)$$

such that, for each $z \in \text{dom}(\mu_1) \setminus \text{vars}(\bar{s}_1)$, properties 1 and 2 hold using μ_1 and $\bar{s}_1$.
Let

$$\mu \stackrel{\text{def}}{=} \{t_1 = s_1\mu_1\} \cup \mu_1.$$

By (46), $t_1 \notin \text{vars}(\mu_1)$. Moreover $\mu_1 \in \mathit{RSubst}$ and $s_1 \notin \mathit{Vars}$ so that $\mu \in \mathit{Eqs}$ has no identities or circular subset. Thus $\mu \in \mathit{RSubst}$. By Lemma 42, $\mu \in \text{mgs}(\bar{s} = \bar{t})$.
As $\text{vars}(\bar{s}_1) \cup \{t_1\} = \text{vars}(\bar{s})$ and $\text{dom}(\mu_1) \cup \{t_1\} = \text{dom}(\mu)$, we have

$$\text{dom}(\mu_1) \setminus \text{vars}(\bar{s}_1) = \text{dom}(\mu) \setminus \text{vars}(\bar{s}).$$

Suppose $z \in \text{dom}(\mu) \setminus \text{vars}(\bar{s})$. Then $z \neq t_1$, $z\mu = z\mu_1$ and the inductive properties 1 and 2 using μ_1 and $\bar{s}_1$ can be applied to z. We show that the properties 1 and 2 using μ and $\bar{s}$ can be applied to z.

1. By property 1, $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s}_1)$ and hence, as $\bar{s}_1 \subseteq \bar{s}$, $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s})$.
2. By property 2, we have $\text{vars}(z\mu) \cap \text{dom}(\mu_1) = \varnothing$. Now $t_1 \notin \text{vars}(z\mu)$ because $t_1 \notin \text{vars}(\bar{s}_1)$ (by (46)) and $\text{vars}(z\mu) \subseteq \text{vars}(\bar{s}_1)$ (by property 1). It follows that $\text{vars}(z\mu) \cap \text{dom}(\mu) = \varnothing$, since $\text{dom}(\mu_1) \cup \{t_1\} = \text{dom}(\mu)$.

∎

Proposition 67. *Let $p \in P$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \text{vars}(t) \subseteq \mathit{VI}$. Let also $\sigma \in \gamma_P(p) \cap \mathit{VSubst}$ and suppose that $\{r, r'\} = \{x, t\}$, $\text{vars}(r) \subseteq \text{hvars}(\sigma)$ and $\text{rt}(r, \sigma) \in \mathit{GTerms}$. Then, for all $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T, we have*

$$\text{hvars}(\sigma) \cup \text{vars}(r') \subseteq \text{hvars}(\tau). \tag{47}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that

1. $\text{vars}(r') \subseteq \text{hvars}(\tau)$, for some $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$;

2. $\text{hvars}(\sigma) \subseteq \text{hvars}(\tau)$, for some $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

From these, we can then conclude that, for all $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$, (47) holds.

Note that, in both cases, since $\sigma \in \mathit{VSubst}$ and $\text{vars}(r) \subseteq \text{hvars}(\sigma)$, by Proposition 52 we have $\text{rt}(r, \sigma) = r\sigma$, so that $r\sigma \in \mathit{HTerms} \cap \mathit{GTerms}$.

We first prove statement 1. We must show that there exists $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that $\text{vars}(r') \subseteq \text{hvars}(\tau)$.

As $\text{mgs}\bigl(\sigma \cup \{x = t\}\bigr) \neq \varnothing$, by Theorem 49 and the definition of mgs we can assume that there exists $\tau \in \mathit{VSubst} \cap \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$. Thus

$$\tau \implies \bigl(\sigma \cup \{r = r'\}\bigr).$$

By Lemma 41 and the congruence axioms, we have $\tau \implies \{r\sigma = r'\}$. Since $\tau \in \mathit{VSubst}$ and $r\sigma \in \mathit{HTerms} \cap \mathit{GTerms}$, Lemma 64 applies (with $s = r\sigma$) so that $r\sigma = r'\tau \in \mathit{HTerms} \cap \mathit{GTerms}$. Thus, by Proposition 51, $\text{vars}(r') \subseteq \text{hvars}(\tau)$.

We now prove statement 2. In this case, we show that there exists $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that $\text{hvars}(\sigma) \subseteq \text{hvars}(\tau)$.

Let

$$\begin{aligned}
\{u_1, \ldots, u_l\} &\stackrel{\text{def}}{=} \text{dom}(\sigma) \cap \text{vars}(r'\sigma), \\
\bar{s} &\stackrel{\text{def}}{=} (u_1, \ldots, u_l, r\sigma), \\
\bar{t} &\stackrel{\text{def}}{=} (u_1\sigma, \ldots, u_l\sigma, r'\sigma).
\end{aligned}$$

By Lemma 42 and the congruence axioms, $\sigma \cup \{x = t\} \implies \bar{s} = \bar{t}$. Thus, as $\sigma \cup \{x = t\}$ is satisfiable, $\text{mgs}(\bar{s} = \bar{t}) \neq \varnothing$. Then, by Theorem 49, there exists $\mu \in \mathit{VSubst} \cap \text{mgs}(\bar{s} = \bar{t})$. Therefore, since $r\sigma \in \mathit{HTerms} \cap \mathit{GTerms}$ and $\mu \implies \{r\sigma = r'\sigma\}$, Lemma 64 applies (with $s = r\sigma$) so that we can conclude $r\sigma = r'\sigma\mu \in \mathit{HTerms} \cap \mathit{GTerms}$. Hence, for all $w \in \text{dom}(\mu)$,

$$\text{vars}(w\mu) = \varnothing. \tag{48}$$

Let

$$\begin{aligned}
\nu &\stackrel{\text{def}}{=} \bigl\{\, z = z\sigma\mu \bigm| z \in \text{dom}(\sigma) \setminus \text{vars}(r'\sigma) \,\bigr\}, \\
\tau &\stackrel{\text{def}}{=} \nu \cup \mu.
\end{aligned}$$

Then, as $\sigma, \mu \in \mathit{RSubst}$, it follows from (48) that $\nu, \tau \in \mathit{Eqs}$ have no identities or circular subsets so that $\nu, \tau \in \mathit{RSubst}$. By Lemma 42, $\tau \in \text{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

Suppose that $y \in \text{hvars}(\sigma)$. Then we show that $y \in \text{hvars}(\tau)$. Using Proposition 52, $\text{rt}(y, \sigma) = y\sigma$ and

$$\text{vars}(y\sigma) \cap \text{dom}(\sigma) = \varnothing. \tag{49}$$

We show that $\text{vars}(y\tau) \cap \text{dom}(\tau) = \varnothing$. Now, if $y \notin \text{dom}(\tau)$, the result holds trivially. Suppose that $y \in \text{dom}(\nu)$, then $y\tau = y\sigma\mu$ and $y \in \text{dom}(\sigma)$. Let w be any variable in $\text{vars}(y\sigma)$ so that, by (49), $w \notin \text{dom}(\sigma)$. If $w \notin \text{dom}(\mu)$, then $w = w\mu \notin \text{dom}(\tau)$. If $w \in \text{dom}(\mu)$, then, by (48), $\text{vars}(w\mu) = \varnothing$. Therefore, $\text{vars}(w\mu) \cap \text{dom}(\tau) = \varnothing$. It follows that $\text{vars}(y\nu) \cap \text{dom}(\tau) = \varnothing$. Finally, suppose $y \in \text{dom}(\mu)$. Then, by (48), $\text{vars}(y\mu) = \varnothing$. Therefore $\text{vars}(y\mu) \cap \text{dom}(\tau) = \varnothing$.

Therefore, using Definition 12, we have that $y \in \text{hvars}(\tau)$ as required. ∎

PROPOSITION 68. *Let $p \in P$ and $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Let also $\sigma \in \gamma_P(p) \cap VSubst$ and suppose that $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Suppose also that $\mathrm{ind}_p(x,t)$ and that $\mathrm{or\_lin}_p(x,t)$ hold. Then, for all substitutions $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T,*

$$\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\tau). \tag{50}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that there exists $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that (50) holds.

As $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$, by using Proposition 52 we obtain $\mathrm{rt}(x,\sigma) = x\sigma$ and $\mathrm{rt}(t,\sigma) = t\sigma$. Also

$$\begin{aligned} \mathrm{vars}(x\sigma) \cap \mathrm{dom}(\sigma) &= \varnothing, \\ \mathrm{vars}(t\sigma) \cap \mathrm{dom}(\sigma) &= \varnothing. \end{aligned} \tag{51}$$

As $\mathrm{ind}_p(x,t)$ holds,

$$\mathrm{vars}(x\sigma) \cap \mathrm{vars}(t\sigma) = \varnothing. \tag{52}$$

By hypothesis, $\mathrm{or\_lin}(x,t)$ holds so that, by Definition 8, for some $r \in \{x,t\}$, $r\sigma$ is linear. Let $r' \stackrel{\mathrm{def}}{=} \{x,t\} \setminus \{r\}$.

By Lemma 42 and the congruence axioms, $\sigma \cup \{x = t\} \implies \{r\sigma = r'\sigma\}$. Thus, as $\sigma \cup \{x = t\}$ is satisfiable, $\mathrm{mgs}(r\sigma = r'\sigma) \neq \varnothing$. Thus we can apply Lemma 65 (where $\bar{s} = r\sigma$ and $\bar{t} = r'\sigma$) so that, using (52), there exists $\mu \in \mathrm{mgs}(x\sigma = t\sigma)$ such that, for all $w \in \mathrm{dom}(\mu)$,

$$\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing. \tag{53}$$

Note that, by (51),

$$\mathrm{dom}(\sigma) \cap \mathrm{vars}(\mu) = \varnothing. \tag{54}$$

Let

$$\begin{aligned} \nu &\stackrel{\mathrm{def}}{=} \bigl\{\, z = z\sigma\mu \bigm| z \in \mathrm{dom}(\sigma) \,\bigr\}, \\ \tau &\stackrel{\mathrm{def}}{=} \nu \cup \mu. \end{aligned}$$

Then, as $\sigma, \mu \in RSubst$, it follows from (54) that $\nu, \tau \in Eqs$ have no identities or circular subsets so that $\nu, \tau \in RSubst$. By Lemma 42, $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

Suppose $y \in \mathrm{hvars}(\sigma)$. Then we show that $y \in \mathrm{hvars}(\tau)$. As $y \in HTerms$, we have, using Proposition 52, $\mathrm{rt}(y,\sigma) = y\sigma$ and

$$\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{55}$$

We show that $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$. If $y \notin \mathrm{dom}(\tau)$, the result holds trivially. Suppose that $y \in \mathrm{dom}(\nu)$, then $y\tau = y\sigma\mu$. Let w be any variable in $\mathrm{vars}(y\sigma)$. Then, by (55), $w \notin \mathrm{dom}(\sigma)$. If $w \notin \mathrm{dom}(\mu)$, then $w = w\mu \notin \mathrm{dom}(\tau)$. If $w \in \mathrm{dom}(\mu)$, then $\mathrm{vars}(w\mu) \subseteq \mathrm{vars}(\mu)$ so that, by (54), $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\nu) = \varnothing$. Moreover (53) applies so that $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Therefore we have $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\tau) = \varnothing$. It follows that $\mathrm{vars}(y\nu) \cap \mathrm{dom}(\tau) = \varnothing$. Finally, suppose $y \in \mathrm{dom}(\mu)$. Then $y\tau = y\mu$ and, by (54), we have $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\nu) = \varnothing$. Also (53) applies where w is replaced by y so that $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Thus $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\tau) = \varnothing$.

Therefore, using Definition 12, we have that $y \in \mathrm{hvars}(\tau)$ as required. ∎

PROPOSITION 69. *Let $p \in P$ and $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Let also $\sigma \in \gamma_P(p) \cap VSubst$ and suppose that $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Suppose also that $\mathrm{gfree}_p(x)$ and $\mathrm{gfree}_p(t)$ hold. Then, for all $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T, we have*

$$\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\tau). \tag{56}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that there exists $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that (56) holds.

By Definition 8, $\mathrm{gfree}_p(x)$ and $\mathrm{gfree}_p(t)$ imply that either $\mathrm{rt}(x, \sigma) \in GTerms$ or $\mathrm{rt}(x, \sigma) \in Vars$, and either $\mathrm{rt}(t, \sigma) \in GTerms$ or $\mathrm{rt}(t, \sigma) \in Vars$. Since we have $\mathrm{rt}(x, \sigma), \mathrm{rt}(t, \sigma) \in HTerms$ and $\sigma \in VSubst$, as a consequence of Proposition 52, we have $\mathrm{rt}(x, \sigma) = x\sigma$, $\mathrm{rt}(t, \sigma) = t\sigma$ and $x\sigma, t\sigma \notin \mathrm{dom}(\sigma)$. There are three cases:

- $\mathrm{vars}(x\sigma) = \varnothing \vee \mathrm{vars}(t\sigma) = \varnothing$. Then the result follows from Proposition 67.
- $x\sigma = t\sigma \in Vars$. Then letting $\tau = \sigma$ gives the required result.
- $x\sigma, t\sigma \in Vars$ are distinct variables. Let $\tau = \sigma \cup \{x\sigma = t\sigma\}$. Then, as $x\sigma, t\sigma \notin \mathrm{dom}(\sigma)$, $\tau \in RSubst$. Hence, by Lemma 42, $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$. Let y be any variable in $\mathrm{hvars}(\sigma)$. We show that $y \in \mathrm{hvars}(\tau)$.

  Suppose first that $y \neq x\sigma$. Then $y\tau = y\sigma$. Thus using Proposition 52, $\mathrm{rt}(y, \sigma) = y\tau$ and $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\sigma) = \varnothing$. Thus $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) \subseteq \{x\sigma\}$. However, $x\sigma\tau = t\sigma \notin \mathrm{dom}(\tau)$ so that, by Definition 11, $\mathrm{vars}(y\tau) \subseteq \mathrm{hvars}_1(\tau)$ and hence $y \in \mathrm{hvars}_2(\tau)$. Therefore, by Lemma 57 and Definition 12, we have $y \in \mathrm{hvars}(\tau)$.

  Secondly, suppose that $y = x\sigma$. Then $y\tau = t\sigma$. So that, as $t\sigma \in Vars \setminus \mathrm{dom}(\sigma)$ and $x\sigma \neq t\sigma$, $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$. Therefore, using Definition 12, we have that $y \in \mathrm{hvars}(\tau)$ as required.

▮

PROPOSITION 70. *Let $p \in P$ and $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Let $\sigma \in \gamma_P(p) \cap VSubst$ and suppose that $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Furthermore, suppose that $\mathrm{or\_lin}_p(x, t)$ and $\mathrm{share\_lin}_p(x, t)$ hold. Then, for all substitutions $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T, we have*

$$\mathrm{hvars}(\sigma) \setminus \mathrm{share\_same\_var}_p(x, t) \subseteq \mathrm{hvars}(\tau). \tag{57}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that there exists $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that (57) holds.

As $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$, by using Proposition 52 we obtain $\mathrm{rt}(x, \sigma) = x\sigma$ and $\mathrm{rt}(t, \sigma) = t\sigma$. Also

$$\mathrm{vars}(x\sigma) \cap \mathrm{dom}(\sigma) = \varnothing, \quad \mathrm{vars}(t\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{58}$$

By hypothesis, $\mathrm{or\_lin}_p(x, t)$ holds so that, by Definition 8, for some $r \in \{x, t\}$, $r\sigma$ is linear. Also by hypothesis, $\mathrm{share\_lin}_p(x, t)$ holds so that, by Definition 8, if $r' = \{x, t\} \setminus \{r\}$, for all $z \in \mathrm{vars}(r\sigma) \cap \mathrm{vars}(r'\sigma)$, $\mathrm{occ\_lin}(z, r'\sigma)$ holds. Therefore,

$$\mathrm{vars}(r\sigma) \cap \mathrm{nlvars}(r'\sigma) = \varnothing. \tag{59}$$

By Lemma 42 and the congruence axioms, $\sigma \cup \{x = t\} \implies \{r\sigma = r'\sigma\}$. Thus, as $\sigma \cup \{x = t\}$ is satisfiable, $\mathrm{mgs}(r\sigma = r'\sigma) \neq \varnothing$. Thus, as $r\sigma$ is linear and (59) holds, we can apply Lemma 65 (where $\bar{s} = r\sigma$ and $\bar{t} = r'\sigma$) so that there exists $\mu \in \mathrm{mgs}(x\sigma = t\sigma)$ such that, for all $w \in \mathrm{dom}(\mu) \setminus \bigl(\mathrm{vars}(x\sigma) \cap \mathrm{vars}(t\sigma)\bigr)$,

$$\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing. \tag{60}$$

Note that, by (58),

$$\mathrm{dom}(\sigma) \cap \mathrm{vars}(\mu) = \varnothing. \tag{61}$$

Let

$$\begin{aligned} \nu &\stackrel{\mathrm{def}}{=} \bigl\{\, z = z\sigma\mu \bigm| z \in \mathrm{dom}(\sigma) \,\bigr\}, \\ \tau &\stackrel{\mathrm{def}}{=} \nu \cup \mu. \end{aligned}$$

Then, as $\sigma, \mu \in \mathit{RSubst}$, it follows from (61) that $\nu, \tau \in \mathit{Eqs}$ have no identities or circular subsets so that $\nu, \tau \in \mathit{RSubst}$. By Lemma 42, $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

Suppose $y \in \mathrm{hvars}(\sigma) \setminus \mathrm{share\_same\_var}_p(x, t)$. We show that $y \in \mathrm{hvars}(\tau)$. As $y \in \mathrm{hvars}(\sigma)$, using Proposition 52, $\mathrm{rt}(y, \sigma) = y\sigma$ and

$$\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{62}$$

As $y \notin \mathrm{share\_same\_var}_p(x, t)$, by Definition 8,

$$\mathrm{vars}(y\sigma) \cap \mathrm{vars}(x\sigma) \cap \mathrm{vars}(t\sigma) = \varnothing. \tag{63}$$

Therefore, using (63) if $y \notin \mathrm{dom}(\sigma)$ and (58) if $y \in \mathrm{dom}(\sigma)$, it follows that

$$y \notin \mathrm{vars}(x\sigma) \cap \mathrm{vars}(t\sigma). \tag{64}$$

We show that $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$. Now, if $y \notin \mathrm{dom}(\tau)$, the result holds trivially. Suppose that $y \in \mathrm{dom}(\nu)$, then $y\tau = y\sigma\mu$. Let w be any variable in $\mathrm{vars}(y\sigma)$. Then, by (63), $w \notin \bigl(\mathrm{vars}(x\sigma) \cap \mathrm{vars}(t\sigma)\bigr)$ and, by (62), $w \notin \mathrm{dom}(\sigma)$. If $w \notin \mathrm{dom}(\mu)$, then $w = w\mu \notin \mathrm{dom}(\tau)$. If $w \in \mathrm{dom}(\mu)$, then $\mathrm{vars}(w\mu) \subseteq \mathrm{vars}(\mu)$ so that, by (61), we also have $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\nu) = \varnothing$. Moreover (60) applies so that $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Therefore, $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\tau) = \varnothing$. It follows that $\mathrm{vars}(y\nu) \cap \mathrm{dom}(\tau) = \varnothing$. Finally, suppose $y \in \mathrm{dom}(\mu)$. Then $y\tau = y\mu$ and, by (61), $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\nu) = \varnothing$. As (64) holds, (60) applies where w is replaced by y so that $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Thus $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\tau) = \varnothing$.

Therefore, using Definition 12, we have that $y \in \mathrm{hvars}(\tau)$ as required. ∎

PROPOSITION 71. *Let $p \in P$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Let also $\sigma \in \gamma_P(p) \cap \mathit{VSubst}$ and suppose that $\{r, r'\} = \{x, t\}$, $\mathrm{vars}(r) \subseteq \mathrm{hvars}(\sigma)$ and $\mathrm{lin}_p(r)$ holds. Then, for all $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T, we have*

$$\mathrm{hvars}(\sigma) \setminus \mathrm{share\_with}_p(r) \subseteq \mathrm{hvars}(\tau). \tag{65}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that there exists $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that (65) holds.

By hypothesis, $\mathrm{vars}(r) \subseteq \mathrm{hvars}(\sigma)$. Hence, by Proposition 52, $\mathrm{rt}(r, \sigma) = r\sigma$ and

$$\mathrm{vars}(r\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{66}$$

By hypothesis, $\mathrm{lin}_p(r)$ holds, so that, by Definition 8, $r\sigma$ is linear.

Let

$$\begin{aligned}
\{u_1, \ldots, u_l\} &\stackrel{\mathrm{def}}{=} \mathrm{dom}(\sigma) \cap \bigl(\mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma)\bigr), \\
\bar{s} &\stackrel{\mathrm{def}}{=} (u_1, \ldots, u_l, r\sigma), \\
\bar{t} &\stackrel{\mathrm{def}}{=} (u_1\sigma, \ldots, u_l\sigma, r'\sigma).
\end{aligned}$$

Since $r\sigma$ is linear, it follows from (66) that $\bar{s}$ is linear. By Lemma 42 and the congruence axioms, $\sigma \cup \{x = t\} \implies \bar{s} = \bar{t}$. Thus, as $\sigma \cup \{x = t\}$ is satisfiable, we have $\mathrm{mgs}(\bar{s} = \bar{t}) \neq \varnothing$. Therefore, we can apply Lemma 66 so that there exists $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$ such that, for all $w \in \mathrm{dom}(\mu) \setminus \mathrm{vars}(\bar{s})$,

$$\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing. \tag{67}$$

Note that, since $\sigma \in \mathit{VSubst}$, for each $i = 1, \ldots, l$, we have

$$\mathrm{vars}(u_i\sigma) \subseteq \mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma).$$

Thus

$$\mathrm{vars}(\mu) \subseteq \mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma). \tag{68}$$

Let

$$\begin{aligned}
\nu &\stackrel{\mathrm{def}}{=} \Bigl\{\, z = z\sigma\mu \Bigm| z \in \mathrm{dom}(\sigma) \setminus \bigl(\mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma)\bigr) \,\Bigr\}, \\
\tau &\stackrel{\mathrm{def}}{=} \nu \cup \mu.
\end{aligned}$$

Then, as $\sigma, \mu \in \mathit{RSubst}$, it follows from (68) that $\nu, \tau \in \mathit{Eqs}$ have no identities or circular subsets so that $\nu, \tau \in \mathit{RSubst}$. By Lemma 42, $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

Suppose $y \in \mathrm{hvars}(\sigma) \setminus \mathrm{share\_with}_p(r)$. Then we show that $y \in \mathrm{hvars}(\tau)$. As $y \in \mathrm{hvars}(\sigma)$, by Proposition 52, $\mathrm{rt}(y, \sigma) = y\sigma$ and

$$\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{69}$$

As $y \notin \mathrm{share\_with}_p(r)$, by Definition 8, $y \notin \mathrm{share\_same\_var}_p(y, r)$ so that, using the same definition,

$$\mathrm{vars}(y\sigma) \cap \mathrm{vars}(r\sigma) = \varnothing. \tag{70}$$

Therefore using (70) if $y \notin \mathrm{dom}(\sigma)$ and (66) if $y \in \mathrm{dom}(\sigma)$, it follows that

$$y \notin \mathrm{vars}(r\sigma). \tag{71}$$

We show that $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$. Now, if $y \notin \mathrm{dom}(\tau)$, the result holds trivially. Suppose that $y \in \mathrm{dom}(\nu)$. Then $y\tau = y\sigma\mu$ and $y \in \mathrm{dom}(\sigma)$. It follows from (69) and (70) that $\mathrm{vars}(y\sigma) \cap \mathrm{vars}(\bar{s}) = \varnothing$. Let w be any variable in $\mathrm{vars}(y\sigma)$ so that $w \notin \mathrm{vars}(\bar{s})$. By (69), we have $w \notin \mathrm{dom}(\sigma)$. If $w \notin \mathrm{dom}(\mu)$, then we have $w = w\mu \notin \mathrm{dom}(\tau)$. If $w \in \mathrm{dom}(\mu)$, then $\mathrm{vars}(w\mu) \subseteq \mathrm{vars}(\mu)$ so that, by (68), $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\nu) = \varnothing$. Moreover (67) applies so that $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Therefore, $\mathrm{vars}(w\mu) \cap \mathrm{dom}(\tau) = \varnothing$. It follows that $\mathrm{vars}(y\nu) \cap \mathrm{dom}(\tau) = \varnothing$. Finally, suppose $y \in \mathrm{dom}(\mu)$. Then $y\tau = y\mu$ and, by (68), $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\nu) = \varnothing$. Since $\sigma \in \mathit{VSubst}$ and $y \in \mathrm{hvars}(\sigma)$, we have $y \notin \mathrm{dom}(\sigma) \cap \bigl(\mathrm{vars}(r\sigma) \cup \mathrm{vars}(r'\sigma)\bigr)$ and hence $y \notin \mathrm{vars}(\bar{s})$. Therefore (67) applies and $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Thus $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\tau) = \varnothing$.

Therefore, using Definition 12, we have that $y \in \mathrm{hvars}(\tau)$ as required. ∎

PROPOSITION 72. *Let $p \in P$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Let also $\sigma \in \gamma_P(p) \cap \mathit{VSubst}$. Then, for all $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in a syntactic equality theory T,*

$$\mathrm{hvars}(\sigma) \setminus \bigl(\mathrm{share\_with}_p(x) \cup \mathrm{share\_with}_p(t)\bigr) \subseteq \mathrm{hvars}(\tau). \tag{72}$$

Proof. We assume that the congruence and identity axioms hold. If $\sigma \cup \{x = t\}$ is not satisfiable, the result is trivial. We therefore assume, for the rest of the proof, that $\sigma \cup \{x = t\}$ is satisfiable in T. It follows from Corollary 63 that we just have to show that there exists $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ such that (72) holds.

Let

$$\begin{aligned}
\{u_1, \ldots, u_l\} &\stackrel{\mathrm{def}}{=} \mathrm{dom}(\sigma) \cap \bigl(\mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma)\bigr),\\
\bar{s} &\stackrel{\mathrm{def}}{=} (u_1, \ldots, u_l, x\sigma),\\
\bar{t} &\stackrel{\mathrm{def}}{=} (u_1\sigma, \ldots, u_l\sigma, t\sigma).
\end{aligned}$$

Note that, since $\sigma \in \mathit{VSubst}$, for each $i = 1, \ldots, l$, we have

$$\mathrm{vars}(u_i\sigma) \subseteq \mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma).$$

Thus, for any $\mu \in \mathrm{mgs}(\bar{s} = \bar{t})$, we have

$$\mathrm{vars}(\mu) \subseteq \mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma). \tag{73}$$

Let

$$\begin{aligned}
\nu &\stackrel{\mathrm{def}}{=} \Bigl\{\, z = z\sigma\mu \Bigm| z \in \mathrm{dom}(\sigma) \setminus \bigl(\mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma)\bigr) \,\Bigr\},\\
\tau &\stackrel{\mathrm{def}}{=} \nu \cup \mu.
\end{aligned}$$

Then, as $\sigma, \mu \in \mathit{RSubst}$, it follows from (73) that $\nu, \tau \in \mathit{Eqs}$ have no identities or circular subsets so that $\nu, \tau \in \mathit{RSubst}$. Thus, using Lemma 42 and the assumption that $\sigma \cup \{x = t\}$ is satisfiable, $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$.

Suppose that $y \in \mathrm{hvars}(\sigma) \setminus \bigl(\mathrm{share\_with}_p(x) \cup \mathrm{share\_with}_p(t)\bigr)$. We show that $y \in \mathrm{hvars}(\tau)$. As $y \in \mathrm{hvars}(\sigma)$, by Proposition 52, $\mathrm{rt}(y, \sigma) = y\sigma$ and

$$\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing. \tag{74}$$

As $y \notin \mathrm{share\_with}_p(x) \cup \mathrm{share\_with}_p(t)$, it follows from Definition 8 that

$$y \notin \mathrm{share\_same\_var}_p(y, x) \cup \mathrm{share\_same\_var}_p(y, t)$$

so that, using the same definition with the result that $\mathrm{rt}(y, \sigma) = y\sigma$, we obtain

$$\mathrm{vars}(y\sigma) \cap \bigl(\mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma)\bigr) = \varnothing. \tag{75}$$

Therefore, using (75) if $y \notin \mathrm{dom}(\sigma)$ and using the fact that $\sigma \in \mathit{VSubst}$, if $y \in \mathrm{dom}(\sigma)$, it follows that

$$y \notin \mathrm{vars}(x\sigma) \cup \mathrm{vars}(t\sigma). \tag{76}$$

We show that $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$. Now, if $y \notin \mathrm{dom}(\tau)$, the result holds trivially. Suppose that $y \in \mathrm{dom}(\tau)$. Then, by (73) and (76), $y \notin \mathrm{vars}(\mu)$ so that

$y \notin \mathrm{dom}(\mu)$ and $\mathrm{vars}(y\mu) \cap \mathrm{dom}(\mu) = \varnothing$. Thus we must have $y \in \mathrm{dom}(\nu)$ and $y\tau = y\sigma$. Then, by (73) and (75), $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\mu) = \varnothing$. Moreover, by (74), $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\sigma) = \varnothing$. It follows that $\mathrm{vars}(y\sigma) \cap \mathrm{dom}(\tau) = \varnothing$ and hence, as $y\sigma = y\tau$, $\mathrm{vars}(y\tau) \cap \mathrm{dom}(\tau) = \varnothing$.

Therefore, using Definition 12, we have that $y \in \mathrm{hvars}(\tau)$ as required. ∎

Proof of Theorem 19 on page 16. By hypothesis, $\sigma \in \gamma_P(p)$. By Theorem 49, there exists $\sigma' \in \mathit{VSubst}$ such that $\sigma \iff \sigma'$. By Lemma 62, we have that $\mathrm{hvars}(\sigma) = \mathrm{hvars}(\sigma')$. By Definition 7, $\sigma \in \gamma_P(p)$ if and only if $\sigma' \in \gamma_P(p)$. We therefore safely assume that $\sigma \in \mathit{VSubst}$.

By hypothesis, we have $\sigma \in \gamma_H(h)$. Therefore, it follows from Definition 16 that $h \subseteq \mathrm{hvars}(\sigma)$. Similarly, by Definition 16, in order to prove $\tau \in \gamma_H(h')$, we just need to show that $h' \subseteq \mathrm{hvars}(\tau)$ where h' is as defined in Definition 18. There are eight cases that have to be considered.

1. $\mathrm{hterm}_h(x) \land \mathrm{ground}_p(x)$ holds.

   As $\mathrm{hterm}_h(x)$ holds, by Definition 18, $x \in h$. Hence, by Definition 16, we have $x \in \mathrm{hvars}(\sigma)$. As $\mathrm{ground}_p(x)$ holds, by Definition 8, $\mathrm{rt}(x, \sigma) \in \mathit{GTerms}$. Therefore we can apply Proposition 67, where r is replaced by x and r' by t, to conclude that
   $$\mathrm{hvars}(\sigma) \cup \mathrm{vars}(t) \subseteq \mathrm{hvars}(\tau).$$

2. $\mathrm{hterm}_h(t) \land \mathrm{ground}_p(t)$ holds.

   As $\mathrm{hterm}_h(t)$ holds, by Definition 18, $\mathrm{vars}(t) \subseteq h$. Hence, by Definition 16, $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. As $\mathrm{ground}_p(t)$ holds, by Definition 8, $\mathrm{rt}(t, \sigma) \in \mathit{GTerms}$. Therefore we can apply Proposition 67, where r is replaced by t and r' by x, to conclude that
   $$\mathrm{hvars}(\sigma) \cup \{x\} \subseteq \mathrm{hvars}(\tau).$$

3. $\mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \land \mathrm{ind}_p(x, t) \land \mathrm{or\_lin}_p(x, t)$ holds.

   As $\mathrm{hterm}_h(x)$ and $\mathrm{hterm}_h(t)$ hold, by Definition 18, $x \in h$ and $\mathrm{vars}(t) \subseteq h$. Hence, by Definition 16, $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Therefore we can apply Proposition 68 to conclude that
   $$\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\tau).$$

4. $\mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \land \mathrm{gfree}_p(x) \land \mathrm{gfree}_p(t)$ holds.

   As $\mathrm{hterm}_h(x)$ and $\mathrm{hterm}_h(t)$ hold, by Definition 18, $x \in h$ and $\mathrm{vars}(t) \subseteq h$. Hence, by Definition 16, $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Therefore we can apply Proposition 69 to conclude that
   $$\mathrm{hvars}(\sigma) \subseteq \mathrm{hvars}(\tau).$$

5. $\mathrm{hterm}_h(x) \land \mathrm{hterm}_h(t) \land \mathrm{share\_lin}_p(x, t) \land \mathrm{or\_lin}_p(x, t)$ holds.

   As $\mathrm{hterm}_h(x)$ and $\mathrm{hterm}_h(t)$ hold, by Definition 18, $x \in h$ and $\mathrm{vars}(t) \subseteq h$. Hence, by Definition 16, $x \in \mathrm{hvars}(\sigma)$ and $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Therefore we can apply Proposition 70 to conclude that
   $$\mathrm{hvars}(\sigma) \setminus \mathrm{share\_same\_var}_p(x, t) \subseteq \mathrm{hvars}(\tau).$$

6. $\mathrm{hterm}_h(x) \land \mathrm{lin}_p(x)$ holds.

   As $\mathrm{hterm}_h(x)$ holds, by Definition 18, $x \in h$. Hence, by Definition 16, we have $x \in \mathrm{hvars}(\sigma)$. Therefore we can apply Proposition 71 where r is replaced by x and r' by t, to conclude that

   $$\mathrm{hvars}(\sigma) \setminus \mathrm{share\_with}_p(x) \subseteq \mathrm{hvars}(\tau).$$

7. $\mathrm{hterm}_h(t) \land \mathrm{lin}_p(t)$ holds.

   As $\mathrm{hterm}_h(t)$ holds, by Definition 18, $\mathrm{vars}(t) \subseteq h$. Hence, by Definition 16, $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\sigma)$. Therefore we can apply Proposition 71 where r is replaced by t and r' by x, to conclude that

   $$\mathrm{hvars}(\sigma) \setminus \mathrm{share\_with}_p(t) \subseteq \mathrm{hvars}(\tau).$$

8. For all $(x \mapsto t) \in \mathit{Bind}$ where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$, Proposition 72 applies so that

   $$\mathrm{hvars}(\sigma) \setminus \bigl(\mathrm{share\_with}_p(x) \cup \mathrm{share\_with}_p(t)\bigr) \subseteq \mathrm{hvars}(\tau).$$

∎

Proof of Theorem 21 on page 17. Suppose that $\tau \in \exists x \,.\, \{\sigma\}$. We need to show that $\tau \in \gamma_H\bigl(\mathrm{proj}_H(h, x)\bigr)$.

Let $\overline{V} = \mathit{Vars} \setminus \mathit{VI}$. Then, by Definition 5, $\mathcal{RT} \vdash \forall\bigl(\exists \overline{V} \,.\, (\tau \leftrightarrow \exists x \,.\, \sigma)\bigr)$. Thus we have

$$\mathcal{RT} \vdash \forall\Bigl(\bigl(\exists \overline{V} \,.\, \tau\bigr) \leftrightarrow \bigl(\exists \overline{V} \cup \{x\} \,.\, \sigma\bigr)\Bigr). \tag{77}$$

Suppose $v \in \overline{V} \setminus \mathrm{vars}(\sigma)$. As we assumed that *Vars* is denumerable and that *VI* is finite, such a v will exist. Moreover, as $x \in \mathit{VI}$, we have $x \neq v$. Let $\sigma' \in \mathit{RSubst}$ be obtained from σ by replacing every occurrence of x by v. Formally, if $\rho = \{x \mapsto v\}$, let

$$\sigma' \stackrel{\mathrm{def}}{=} \bigl\{\, y \mapsto y\sigma\rho \bigm| y \in \mathrm{dom}(\sigma) \setminus \{x\} \,\bigr\} \cup \sigma'',$$

where $\sigma'' = \{v \mapsto x\sigma\rho\}$ if $x \in \mathrm{dom}(\sigma)$ and $\varnothing$ otherwise. Then $\sigma' \in \mathit{RSubst}$ and

$$\mathcal{RT} \vdash \forall\Bigl(\bigl(\exists \overline{V} \,.\, \sigma'\bigr) \leftrightarrow \bigl(\exists \overline{V} \cup \{x\} \,.\, \sigma\bigr)\Bigr).$$

Thus, by (77), $\mathcal{RT} \vdash \forall\bigl((\exists \overline{V} \,.\, \tau) \leftrightarrow (\exists \overline{V} \,.\, \sigma')\bigr)$. Therefore, by Proposition 61,

$$\mathrm{hvars}(\tau) \cap \mathit{VI} = \mathrm{hvars}(\sigma') \cap \mathit{VI}. \tag{78}$$

As $\sigma' \in \mathit{RSubst}$ and $x \notin \mathrm{dom}(\sigma')$, $\mathrm{rt}(x, \sigma') = x$ so that, by Proposition 12, $x \in \mathrm{hvars}(\sigma')$. Also, as σ' is obtained from σ by renaming x to the new variable v, $\mathrm{hvars}(\sigma') \supseteq \mathrm{hvars}(\sigma) \setminus \{v\}$. Since $v \notin \mathit{VI}$, we have

$$\mathrm{hvars}(\sigma') \cap \mathit{VI} \supseteq \bigl(\mathrm{hvars}(\sigma) \cup \{x\}\bigr) \cap \mathit{VI}.$$

Therefore, by (78),

$$\mathrm{hvars}(\tau) \cap \mathit{VI} \supseteq \bigl(\mathrm{hvars}(\sigma) \cup \{x\}\bigr) \cap \mathit{VI}. \tag{79}$$

By hypothesis, $\sigma \in \gamma_H(h)$, so that, by Definition 16, $\mathrm{hvars}(\sigma) \supseteq h$. Therefore, by (79), $\mathrm{hvars}(\tau) \cap \mathit{VI} \supseteq \bigl(h \cup \{x\}\bigr) \cap \mathit{VI}$. Thus, by applying Definition 16, we can conclude that $\tau \in \gamma_H\bigl(h \cup \{x\}\bigr)$. ∎

B.7. Finite-Tree Dependencies

PROPOSITION 73. *Let $\sigma, \tau \in RSubst$ and $\phi \in Bfun$, where $\sigma \in \gamma_F(\phi)$ and $\tau \in \downarrow\sigma$. Then $\tau \in \gamma_F(\phi)$.*

Proof. By the hypothesis, $\tau \in \downarrow\sigma$, so that, for each $\upsilon \in \downarrow\tau$, $\upsilon \in \downarrow\sigma$. Therefore, as $\sigma \in \gamma_F(\phi)$, it follows from Definition 22 that, for all $\upsilon \in \downarrow\tau$, $\phi\bigl(\mathrm{hval}(\upsilon)\bigr) = 1$ and hence $\tau \in \gamma_F(\phi)$. ∎

LEMMA 74. *Let $\phi_1, \phi_2 \in Bfun$. Then*

$$\gamma_F(\phi_1 \wedge \phi_2) = \gamma_F(\phi_1) \cap \gamma_F(\phi_2).$$

Proof.

$$\begin{aligned}
\gamma_F(\phi_1 \wedge \phi_2) &= \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : (\phi_1 \wedge \phi_2)\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \forall i \in \{1,2\} : \phi_i\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \phi_1\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&\qquad \cap \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \phi_2\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \gamma_F(\phi_1) \cap \gamma_F(\phi_2).
\end{aligned}$$

∎

Proof of Theorem 23 on page 19. Assuming the hypothesis of the theorem, we will prove each relation separately.

(23a). Let $\sigma = \{x \mapsto t\}$ and suppose that $\tau \in \downarrow\sigma$. Then, by Proposition 2, $\mathcal{RT} \vdash \forall(\tau \to \sigma)$. It follows from Lemma 43 that $\mathrm{rt}(x,\tau) = \mathrm{rt}(t,\tau)$ and thus, by case (56b) of Corollary 56, $x \in \mathrm{hvars}(\tau)$ if and only if $\mathrm{vars}(t) \subseteq \mathrm{hvars}(\tau)$. This is equivalent to $\bigl(x \leftrightarrow \bigwedge \mathrm{vars}(t)\bigr)\bigl(\mathbf{0}\bigl[1/\mathrm{hvars}(\tau)\bigr]\bigr) = 1$ and, by Definition 22, to $\bigl(x \leftrightarrow \bigwedge \mathrm{vars}(t)\bigr)\bigl(\mathrm{hval}(\tau)\bigr) = 1$. As this holds for all $\tau \in \downarrow\sigma$, by Definition 22, $\sigma \in \gamma_F\bigl(x \leftrightarrow \bigwedge \mathrm{vars}(t)\bigr)$.

(23b). Let $\sigma = \{x \mapsto t\}$, where $x \in \mathrm{vars}(t)$. By Definition 12, $x \notin \mathrm{hvars}(\sigma)$. By case (15a) of Proposition 15, for all $\tau \in \downarrow\sigma$, we have $\mathrm{hvars}(\tau) \subseteq \mathrm{hvars}(\sigma)$. Thus $x \notin \mathrm{hvars}(\tau)$ and $(\neg x)\bigl(\mathrm{hval}(\tau)\bigr) = 1$. Therefore, by Definition 22, $\sigma \in \gamma_F(\neg x)$.

(23c). Let $\sigma \in RSubst$ such that $x \in \mathrm{gvars}(\sigma) \cap \mathrm{hvars}(\sigma)$. By case (15b) of Proposition 15, we have $x \in \mathrm{hvars}(\tau)$ for all $\tau \in \downarrow\sigma$. So $(x)\bigl(\mathrm{hval}(\tau)\bigr) = 1$. Therefore, by Definition 22, $\sigma \in \gamma_F(x)$.

(23d). Let $\sigma_1 \in \Sigma_1$ and $\sigma_2 \in \Sigma_2$. Then, by hypothesis $\sigma_1 \in \gamma_F(\phi_1)$ and $\sigma_2 \in \gamma_F(\phi_2)$. Let $\tau \in \mathrm{mgs}(\sigma_1 \cup \sigma_2)$. By definition of mgs, $\mathcal{RT} \vdash \forall(\tau \to \sigma_1)$ and $\mathcal{RT} \vdash \forall(\tau \to \sigma_2)$. Thus, by Proposition 2, we have $\tau \in \downarrow\sigma_1 \cap \downarrow\sigma_2$. Therefore, by Proposition 73, $\tau \in \gamma_F(\phi_1) \cap \gamma_F(\phi_2)$. The result then follows by Lemma 74.

(23e). We have

$$\begin{aligned}
\gamma_F(\phi_1 \vee \phi_2) &= \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : (\phi_1 \vee \phi_2)\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \exists i \in \{1,2\} \,.\, \phi_i\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&\supseteq \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \phi_1\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&\qquad \cup \bigl\{\, \sigma \in RSubst \bigm| \forall\tau \in \downarrow\sigma : \phi_2\bigl(\mathrm{hval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \gamma_F(\phi_1) \cup \gamma_F(\phi_2) \\
&\supseteq \Sigma_1 \cup \Sigma_2.
\end{aligned}$$

(23f). Let $\sigma \in \Sigma$ and let $\sigma' \in \exists x \,.\, \{\sigma\}$. We will show that $\sigma' \in \gamma_F(\exists x \,.\, \phi)$.

Let $\tau' \in {\downarrow}\, \sigma'$. Then there exists $\sigma_1' \in \mathit{RSubst}$ such that $\mathcal{RT} \vdash \forall\bigl(\tau' \leftrightarrow (\sigma' \cup \sigma_1')\bigr)$. Let $\sigma_1 \in \exists x \,.\, \{\sigma_1'\}$ and let $W \stackrel{\mathrm{def}}{=} (\mathit{Vars} \setminus \mathit{VI}) \cup \{x\}$. Then, by Definition 5, it follows $\mathcal{RT} \vdash \forall\bigl(\exists W \,.\, (\sigma' \leftrightarrow \sigma)\bigr)$ and $\mathcal{RT} \vdash \forall\bigl(\exists W \,.\, (\sigma_1' \leftrightarrow \sigma_1)\bigr)$. As a consequence

$$\mathcal{RT} \vdash \forall\bigl(\exists W \,.\, (\sigma' \cup \sigma_1') \leftrightarrow \exists W \,.\, (\sigma \cup \sigma_1)\bigr).$$

Therefore $\sigma \cup \sigma_1$ is satisfiable so that, for some $\tau \in \mathit{RSubst}$, $\mathcal{RT} \vdash \forall\bigl(\tau \leftrightarrow (\sigma \cup \sigma_1)\bigr)$. Thus $\mathcal{RT} \vdash \forall(\exists W \,.\, \tau \leftrightarrow \exists W \,.\, \tau')$. By Proposition 61, $\mathrm{hvars}(\tau') \setminus W = \mathrm{hvars}(\tau) \setminus W$ so that

$$\bigl(\mathrm{hvars}(\tau') \cap \mathit{VI}\bigr) \cup \{x\} = (\mathrm{hvars}(\tau) \cap \mathit{VI}) \cup \{x\}. \tag{80}$$

Let $c \stackrel{\mathrm{def}}{=} \mathrm{hval}(\tau)(x)$. Then, since $\tau \in {\downarrow}\, \sigma$ and, by hypothesis, $\sigma \in \gamma_F(\phi)$, we have the following chain of implications:

$$\begin{aligned}
\phi\bigl(\mathrm{hval}(\tau)\bigr) &= 1 && \text{[by Defn. 22]}\\
\phi\bigl(\mathrm{hval}(\tau)[c/x]\bigr) &= 1 && \text{[by Defn. 3]}\\
\phi\bigl(\mathbf{0}\bigl[1/\,\mathrm{hvars}(\tau) \cap \mathit{VI}\bigr][c/x]\bigr) &= 1 && \text{[by Defn. 22]}\\
\phi\bigl(\mathbf{0}\bigl[1/\bigl(\mathrm{hvars}(\tau) \cap \mathit{VI}\bigr) \cup \{x\}\bigr][c/x]\bigr) &= 1 && \text{[by Defn. 3]}\\
\phi\bigl(\mathbf{0}\bigl[1/\bigl(\mathrm{hvars}(\tau') \cap \mathit{VI}\bigr) \cup \{x\}\bigr][c/x]\bigr) &= 1 && \text{[by (80)]}\\
\phi\bigl(\mathbf{0}\bigl[1/\,\mathrm{hvars}(\tau') \cap \mathit{VI}\bigr][c/x]\bigr) &= 1 && \text{[by Defn. 3]}\\
\phi\bigl(\mathrm{hval}(\tau')[c/x]\bigr) &= 1 && \text{[by Defn. 22]}\\
\phi[c/x]\bigl(\mathrm{hval}(\tau')\bigr) &= 1. && \text{[by Defn. 4]}
\end{aligned}$$

From this last relation, since $\phi[c/x] \models \exists x \,.\, \phi$, it follows that $(\exists x \,.\, \phi)\bigl(\mathrm{hval}(\tau')\bigr) = 1$. As this holds for all $\tau' \in {\downarrow}\, \sigma'$, by Definition 22, $\sigma' \in \gamma_F(\exists x \,.\, \phi)$. ∎

Proof of Theorem 25 on page 20. Since $h \subseteq h'$, by the monotonicity of γ_H we have $\gamma_H(h) \supseteq \gamma_H(h')$, whence one of the inclusions: $\gamma_H(h) \cap \gamma_F(\phi) \supseteq \gamma_H(h') \cap \gamma_F(\phi)$.

In order to establish the other inclusion, we now prove that $\sigma \in \gamma_H(h')$ assuming $\sigma \in \gamma_H(h) \cap \gamma_F(\phi)$. To this end, by Definition 16, it is sufficient to prove that $h' \subseteq \mathrm{hvars}(\sigma)$.

Let $z \in h'$ and let $\psi = \bigl(\phi \wedge \bigwedge h\bigr)$, so that, by hypothesis, $h' = \mathrm{true}(\psi)$. Therefore, we have $\psi \models z$. Consider now $\psi' = \bigl(\phi \wedge \bigwedge \mathrm{hvars}(\sigma)\bigr)$. Since $\sigma \in \gamma_H(h)$, by Definition 16 we have $h \subseteq \mathrm{hvars}(\sigma)$, so that $\psi' \models \psi$ and thus $\psi' \models z$.

Since $\sigma \in \gamma_F(\phi)$, by Definition 22 we have $\phi\bigl(\mathrm{hval}(\sigma)\bigr) = 1$. Also note that $\bigl(\bigwedge \mathrm{hvars}(\sigma)\bigr)\bigl(\mathrm{hval}(\sigma)\bigr) = 1$. From these, by the definition of conjunction for Boolean formulas, we obtain $\psi'\bigl(\mathrm{hval}(\sigma)\bigr) = 1$. Thus we can observe that

$$\begin{aligned}
\psi'\bigl(\mathrm{hval}(\sigma)\bigr) = 1 &\iff (\psi' \wedge z)\bigl(\mathrm{hval}(\sigma)\bigr) = 1\\
&\implies z \in \mathrm{hvars}(\sigma).
\end{aligned}$$

∎

THEOREM 75. *Let $x \in \mathit{VI}$, $h, h' \in H$ and $\phi, \phi' \in \mathit{Bfun}$, where $h \supseteq \mathrm{true}\bigl(\phi \wedge \bigwedge h\bigr)$ and $h' \supseteq \mathrm{true}\bigl(\phi' \wedge \bigwedge h'\bigr)$. Let also*

$$\begin{aligned}
h_1 &\stackrel{\mathrm{def}}{=} h \cap h', & h_2 &\stackrel{\mathrm{def}}{=} h \cup \{x\},\\
\phi_1 &\stackrel{\mathrm{def}}{=} \phi \vee \phi', & \phi_2 &\stackrel{\mathrm{def}}{=} \exists x \,.\, \phi.
\end{aligned}$$

Then, for $i = 1, 2$,

$$h_i \supseteq \mathrm{true}\Bigl(\phi_i \wedge \bigwedge h_i\Bigr).$$

Proof. We assume the hypotheses and prove each statement in turn. For the case where $i = 1$ we have:

$$\begin{aligned}
h_1 &\stackrel{\mathrm{def}}{=} h \cap h' \\
&\supseteq \mathrm{true}\Bigl(\phi \wedge \bigwedge h\Bigr) \cap \mathrm{true}\Bigl(\phi' \wedge \bigwedge h'\Bigr) \\
&\supseteq \mathrm{true}\Bigl(\phi \wedge \bigwedge (h \cap h')\Bigr) \cap \mathrm{true}\Bigl(\phi' \wedge \bigwedge (h \cap h')\Bigr) \\
&= \mathrm{true}\Bigl(\phi \wedge \bigwedge (h \cap h') \vee \phi' \wedge \bigwedge (h \cap h')\Bigr) \\
&= \mathrm{true}\Bigl((\phi \vee \phi') \wedge \bigwedge (h \cap h')\Bigr) \\
&= \mathrm{true}\Bigl(\phi_1 \wedge \bigwedge h_1\Bigr).
\end{aligned}$$

For the case where $i = 2$ we have:

$$\begin{aligned}
h_2 &\stackrel{\mathrm{def}}{=} h \cup \{x\} \\
&\supseteq \mathrm{true}\Bigl(\phi \wedge \bigwedge h\Bigr) \cup \{x\} \\
&\supseteq \mathrm{true}\Bigl((\exists x \,.\, \phi) \wedge \bigwedge h\Bigr) \cup \{x\} \\
&= \mathrm{true}\Bigl((\exists x \,.\, \phi) \wedge \bigwedge \bigl(h \cup \{x\}\bigr)\Bigr) \\
&= \mathrm{true}\Bigl(\phi_2 \wedge \bigwedge h_2\Bigr).
\end{aligned}$$

∎

Proof of Theorem 27 on page 20. Suppose that there exists $\sigma \in \gamma_H(h) \cap \gamma_F(\phi)$. By Definition 22, since $\sigma \in \downarrow \sigma$, we have $\phi\bigl(\mathrm{hval}(\sigma)\bigr) = 1$; therefore, we also have

$$\mathrm{hvars}(\sigma) \cap \mathrm{false}(\phi) = \varnothing;$$

by Definition 16, we have $h \subseteq \mathrm{hvars}(\sigma)$, so that we can conclude $h \cap \mathrm{false}(\phi) = \varnothing$. ∎

B.8. Relation Between Groundness Dependencies and Finite-Tree Dependencies

As was the case for finite-tree dependencies, groundness dependencies only capture permanent information, therefore preserving the equivalence relation induced by $\mathcal{RT}$. Moreover, the γ_G function is *meet-preserving*.

PROPOSITION 76. *Let $\sigma, \tau \in RSubst$ and $\psi \in Pos$, where we have $\sigma \in \gamma_G(\psi)$ and $\tau \in \downarrow \sigma$. Then $\tau \in \gamma_G(\psi)$.*

Proof. By the hypothesis, $\tau \in \downarrow \sigma$, so that, for each $\upsilon \in \downarrow \tau$, $\upsilon \in \downarrow \sigma$. Therefore, as $\sigma \in \gamma_G(\phi)$, it follows from Definition 28 that, for all $\upsilon \in \downarrow \tau$, $\psi\bigl(\mathrm{gval}(\upsilon)\bigr) = 1$ and hence $\tau \in \gamma_G(\phi)$. ∎

COROLLARY 77. *Let $\sigma, \tau \in RSubst$ and $\psi \in Pos$, where we have $\sigma \in \gamma_G(\psi)$ and $\mathcal{RT} \vdash \forall(\sigma \leftrightarrow \tau)$. Then $\tau \in \gamma_G(\psi)$.*

LEMMA 78. *Let* $\psi_1, \psi_2 \in \mathit{Pos}$. *Then*

$$\gamma_G(\psi_1 \wedge \psi_2) = \gamma_G(\psi_1) \cap \gamma_G(\psi_2).$$

Proof.

$$\begin{aligned}
\gamma_G(\psi_1 \wedge \psi_2) &= \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \forall \tau \in {\downarrow}\,\sigma : (\psi_1 \wedge \psi_2)\bigl(\mathrm{gval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \left\{\, \sigma \in \mathit{RSubst} \;\middle|\; \begin{array}{r} \forall \tau \in {\downarrow}\,\sigma : \forall i \in \{1,2\} : \\ \psi_i\bigl(\mathrm{gval}(\tau)\bigr) = 1 \end{array} \,\right\} \\
&= \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \forall \tau \in {\downarrow}\,\sigma : \psi_1\bigl(\mathrm{gval}(\tau)\bigr) = 1 \,\bigr\} \\
&\qquad \cap \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \forall \tau \in {\downarrow}\,\sigma : \psi_2\bigl(\mathrm{gval}(\tau)\bigr) = 1 \,\bigr\} \\
&= \gamma_G(\psi_1) \cap \gamma_G(\psi_2).
\end{aligned}$$

∎

Since non-ground terms can be made cyclic by instantiating their variables, those terms detected as definitely finite on *Bfun* are also definitely ground.

LEMMA 79. *Let* $x \in \mathit{VI}$. *Then* $\gamma_F(x) \subseteq \gamma_G(x)$.

Proof. Suppose that $\sigma \in \gamma_F(x)$. Then, by Definition 22, $(x)\bigl(\mathrm{hval}(\tau)\bigr) = 1$ for all $\tau \in {\downarrow}\,\sigma$, so that $x \in \mathrm{hvars}(\tau)$; in particular, $x \in \mathrm{hvars}(\sigma)$. We prove $x \in \mathrm{gvars}(\sigma)$ by contradiction. That is, we show that if $x \in \mathrm{hvars}(\sigma) \setminus \mathrm{gvars}(\sigma)$, then there exists $\tau \in {\downarrow}\,\sigma$ for which $x \notin \mathrm{hvars}(\tau)$.

Suppose that $x \in \mathrm{hvars}(\sigma) \setminus \mathrm{gvars}(\sigma)$. Then, by Propositions 54 and 55, $\mathrm{rt}(x, \sigma) \in \mathit{HTerms} \setminus \mathit{GTerms}$. Hence, by Proposition 53, there exists $i \in \mathbb{N}$ such that $\mathrm{rt}(x, \sigma) = x\sigma^i$ and there exists $y \in \mathrm{vars}(x\sigma^i) \setminus \mathrm{dom}(\sigma)$. As we assumed that *Sig* contains a function symbol of non-zero arity, there exists $t \in \mathit{HTerms} \setminus \{y\}$ for which $\{y\} = \mathrm{vars}(t)$. It follows that $\sigma' = \{y \mapsto t\} \in \mathit{RSubst}$ and, by Definition 12, $y \notin \mathrm{hvars}(\sigma')$. Since $y \notin \mathrm{dom}(\sigma)$, by Lemma 39, $\tau = \sigma \cup \sigma' \in \mathit{RSubst}$. Since $\tau \in {\downarrow}\,\sigma'$ then, by case (15a) of Proposition 15, we have $y \notin \mathrm{hvars}(\tau)$.

By Lemma 41, we have $\mathcal{RT} \vdash \forall\bigl(\sigma \rightarrow (x = x\sigma^i)\bigr)$. Thus, since we also have $\tau \in {\downarrow}\,\sigma$, we obtain $\mathcal{RT} \vdash \forall\bigl(\tau \rightarrow (x = x\sigma^i)\bigr)$. By applying Lemma 43, we have that $\mathrm{rt}(x, \tau) = \mathrm{rt}(x\sigma^i, \tau)$ and thus, by case (56b) of Corollary 56, we obtain $x \in \mathrm{hvars}(\tau)$ if and only if $\mathrm{vars}(x\sigma^i) \subseteq \mathrm{hvars}(\tau)$. However, as observed before, we know that $y \in \mathrm{vars}(x\sigma^i) \setminus \mathrm{hvars}(\tau)$, so that we also have $x \notin \mathrm{hvars}(\tau)$.

Therefore $x \in \mathrm{gvars}(\sigma) \cap \mathrm{hvars}(\sigma)$ and, by case (15b) of Proposition 15, for all $\tau \in {\downarrow}\,\sigma$, $x \in \mathrm{gvars}(\tau) \cap \mathrm{hvars}(\tau)$. As a consequence, for all $\tau \in {\downarrow}\,\sigma$, $(x)\bigl(\mathrm{gval}(\tau)\bigr) = 1$, so that, by Definition 28, we can conclude that $\sigma \in \gamma_G(x)$. ∎

THEOREM 80. *Let* $\phi \in \mathit{Bfun}$ *and* $\psi \in \mathit{Pos}$. *Let also* $\nu \in \mathit{Pos}$ *be defined as* $\nu \stackrel{\mathrm{def}}{=} \bigwedge \mathrm{true}(\phi)$. *Then*

$$\gamma_F(\phi) \cap \gamma_G(\psi) = \gamma_F(\phi) \cap \gamma_G(\psi \wedge \nu).$$

Proof. Since $\psi \wedge \nu \models \psi$, the inclusion

$$\gamma_F(\phi) \cap \gamma_G(\psi) \supseteq \gamma_F(\phi) \cap \gamma_G(\psi \wedge \nu)$$

follows by the monotonicity of γ_G. To prove the inclusion

$$\gamma_F(\phi) \cap \gamma_G(\psi) \subseteq \gamma_F(\phi) \cap \gamma_G(\psi \wedge \nu)$$

we will show that $\gamma_F(\phi) \subseteq \gamma_G(\nu)$. The thesis will follow as, by Lemma 78, we have $\gamma_G(\psi \wedge \nu) = \gamma_G(\psi) \cap \gamma_G(\nu)$. We have

$$\begin{aligned}
\gamma_F(\phi) &\subseteq \gamma_F(\nu) && \text{[since } \phi \models \nu\text{]} \\
&= \bigcap \{\, \gamma_F(x) \mid x \in \mathrm{true}(\phi) \,\} && \text{[by Lemma 74]} \\
&\subseteq \bigcap \{\, \gamma_G(x) \mid x \in \mathrm{true}(\phi) \,\} && \text{[by Lemma 79]} \\
&= \gamma_G(\nu). && \text{[by Lemma 78]}
\end{aligned}$$

∎

THEOREM 81. *Let $\phi, \phi' \in$ Bfun and $\psi, \psi' \in$ Pos, where $\psi \models \bigwedge \mathrm{true}(\phi)$ and $\psi' \models \bigwedge \mathrm{true}(\phi')$. Let also*

$$\phi_1 \stackrel{\text{def}}{=} \phi \vee \phi', \qquad \phi_2 \stackrel{\text{def}}{=} \exists x \,.\, \phi,$$
$$\psi_1 \stackrel{\text{def}}{=} \psi \vee \psi', \qquad \psi_2 \stackrel{\text{def}}{=} \exists x \,.\, \psi.$$

Then, for $i = 1, 2$, we have $\psi_i \models \bigwedge \mathrm{true}(\phi_i)$.

Proof. Let us assume the hypotheses hold and prove each statement in turn. For the case where $i = 1$ we have:

$$\begin{aligned}
\psi_1 &\stackrel{\text{def}}{=} \psi \vee \psi' \\
&\models \bigwedge \mathrm{true}(\phi) \vee \bigwedge \mathrm{true}(\phi') \\
&\models \bigwedge \mathrm{true}(\phi \vee \phi') \\
&\stackrel{\text{def}}{=} \bigwedge \mathrm{true}(\phi_1).
\end{aligned}$$

Since by hypothesis we have that $\psi \models \bigwedge \mathrm{true}(\phi)$ and existential quantification is a monotonic operation, for the case where $i = 2$ we have:

$$\begin{aligned}
\psi_2 &\stackrel{\text{def}}{=} \exists x \,.\, \psi \\
&\models \exists x \,.\, \bigwedge \mathrm{true}(\phi) \\
&= \bigwedge \bigl(\mathrm{true}(\phi) \setminus \{x\}\bigr) \\
&= \bigwedge \mathrm{true}(\exists x \,.\, \phi) \\
&\stackrel{\text{def}}{=} \bigwedge \mathrm{true}(\phi_2).
\end{aligned}$$

∎

Proof of Theorem 30 on page 21.

Proof of (30a). Since $\psi \wedge \nu \models \psi$, the inclusion

$$\gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi) \supseteq \gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi \wedge \nu)$$

follows by the monotonicity of γ_G.

We now prove the reverse inclusion. Let us assume $\sigma \in \gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi)$. By Lemma 78 we have that $\gamma_G(\psi \wedge \nu) = \gamma_G(\psi) \cap \gamma_G(\nu)$. Therefore it is enough to show that $\sigma \in \gamma_G(\nu)$. By hypothesis, $\nu = \exists VI \setminus h \,.\, \mathrm{pos}(\phi)$. Moreover, by Definition 22, $h \subseteq \mathrm{hvars}(\sigma)$. Thus, to prove the result, we will show, by contradiction, that $\sigma \in \gamma_G\bigl(\exists VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)\bigr)$.

Suppose therefore that $\sigma \notin \gamma_G\bigl(\exists VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)\bigr)$. Then there exists $\tau \in {\downarrow}\,\sigma$ such that

$$\bigl(\exists VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)\bigr)\bigl(\mathrm{gval}(\tau)\bigr) = 0. \tag{81}$$

Let $z \in \mathrm{hvars}(\sigma) \cap VI$. By Proposition 54, $\mathrm{rt}(z, \sigma) \in HTerms$. By Proposition 53, there exists $i \in \mathbb{N}$ such that $\mathrm{rt}(z, \sigma) = z\sigma^i$ and $\mathrm{vars}(z\sigma^i) \cap \mathrm{dom}(\sigma) = \varnothing$. Therefore, by Definition 12, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\sigma)$. Thus, we have

$$\mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\sigma) \setminus \mathrm{dom}(\sigma). \tag{82}$$

By Lemma 41, as $\tau \in {\downarrow}\,\sigma$, $\mathcal{RT} \vdash \forall\bigl(\tau \to (z = z\sigma^i)\bigr)$. By Lemma 43, we have $\mathrm{rt}(z, \tau) = \mathrm{rt}(z\sigma^i, \tau)$ so that, by case (56a) of Corollary 56,

$$z \in \mathrm{gvars}(\tau) \iff \mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\tau). \tag{83}$$

Take $t \in GTerms \cap HTerms$ and let

$$\upsilon_1 \stackrel{\mathrm{def}}{=} \Bigl\{\, y \mapsto t \Bigm| y \in \bigl(\mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\tau)\bigr) \setminus \mathrm{dom}(\sigma) \,\Bigr\}.$$

As we assumed that *Sig* contains a function symbol of non-zero arity, for each $y \in Vars$ there exists $t_y \in HTerms \setminus \{y\}$ such that $\mathrm{vars}(t_y) = \{y\}$. Thus let

$$\upsilon_2 \stackrel{\mathrm{def}}{=} \left\{\, y \mapsto t_y \;\middle|\; \begin{array}{l} y \in \bigl(VI \cup \mathrm{vars}(\sigma)\bigr) \cap \mathrm{hvars}(\sigma) \\ y \notin \mathrm{gvars}(\tau) \cup \mathrm{dom}(\sigma) \end{array} \right\}.$$

Note that υ_1, $\upsilon_2 \in RSubst$, $\mathrm{vars}(\upsilon_1) \cap \mathrm{vars}(\upsilon_2) = \varnothing$ and $\mathrm{vars}(\upsilon_i) \cap \mathrm{dom}(\sigma) = \varnothing$, for $i = 1, 2$. Thus, by Lemma 39, $\tau' \stackrel{\mathrm{def}}{=} (\sigma \cup \upsilon_1 \cup \upsilon_2) \in RSubst$ is satisfiable in $\mathcal{RT}$.

We now show that

$$z \in \mathrm{gvars}(\tau) \iff z \in \mathrm{hvars}(\tau'). \tag{84}$$

First, assume that $z \in \mathrm{gvars}(\tau)$. Then, by (83), we have $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\tau)$. From this, since also (82) holds, we obtain $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{dom}(\upsilon_1)$ so that, by Definitions 9 and 12, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\upsilon_1) \cap \mathrm{hvars}(\upsilon_1)$. Since $\tau' \in {\downarrow}\,\upsilon_1$, by case (15b) of Proposition 15, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\tau') \cap \mathrm{hvars}(\tau')$. Thus, by Corollary 56, $\mathrm{rt}(z\sigma^i, \tau') \in GTerms \cap HTerms$. Now $\tau' \in {\downarrow}\,\sigma$ so that, by Lemma 41, $\mathcal{RT} \vdash \forall\bigl(\tau' \to (z = z\sigma^i)\bigr)$. By Lemma 43, $\mathrm{rt}(z\sigma^i, \tau') = \mathrm{rt}(z, \tau') \in GTerms \cap HTerms$ so that, by Proposition 54 and Proposition 55, $z \in \mathrm{hvars}(\tau')$.

We prove the other direction by contraposition, assuming that $z \notin \mathrm{gvars}(\tau)$. By (83), there exists $y \in \mathrm{vars}(z\sigma^i) \setminus \mathrm{gvars}(\tau)$. Also note that $y \in VI \cup \mathrm{vars}(\sigma)$ and, by (82), $y \notin \mathrm{dom}(\sigma)$ so that $y \in \mathrm{dom}(\upsilon_2)$. By Definition 12, we have $y \notin \mathrm{hvars}(\upsilon_2)$ and, since $\tau' \in {\downarrow}\,\upsilon_2$, by case (15a) of Proposition 15, $y \notin \mathrm{hvars}(\tau')$. Thus, by case (56b) of Corollary 56, we have that $\mathrm{rt}(z\sigma^i, \tau') \notin HTerms$. Moreover, as $\mathcal{RT} \vdash \forall\bigl(\tau' \to (z = z\sigma^i)\bigr)$, by Lemma 43 we have $\mathrm{rt}(z\sigma^i, \tau') = \mathrm{rt}(z, \tau') \notin HTerms$ and therefore, by Proposition 54, $z \notin \mathrm{hvars}(\tau')$.

Since z was an arbitrary variable in $\mathrm{hvars}(\sigma) \cap VI$, it follows from (81) and (84) that,

$$\bigl(\exists VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)\bigr)\bigl(\mathrm{hval}(\tau')\bigr) = 0. \tag{85}$$

We have by hypothesis that $\sigma \in \gamma_F(\phi)$, so that, as $\tau' \in \downarrow\sigma$, by Definition 22 we have $\phi\bigl(\mathrm{hval}(\tau')\bigr) = 1$. Therefore, as $\phi \models \exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)$, $\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \mathrm{pos}(\phi)\bigr)\bigl(\mathrm{hval}(\tau')\bigr) = 1$, which contradicts (85).

Proof of (30b). Since $\phi \wedge \nu \models \phi$, the inclusion

$$\gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi) \supseteq \gamma_H(h) \cap \gamma_F(\phi \wedge \nu) \cap \gamma_G(\psi)$$

follows by the monotonicity of γ_G.

We now prove the reverse inclusion. Assume that $\sigma \in \gamma_H(h) \cap \gamma_F(\phi) \cap \gamma_G(\psi)$. By Lemma 74 we have that $\gamma_F(\phi \wedge \nu) = \gamma_F(\phi) \cap \gamma_F(\nu)$. Therefore it is enough to show that $\sigma \in \gamma_F(\nu)$. By hypothesis, $\nu = \exists\, VI \setminus h \,.\, \psi$. Moreover, by Definition 16, $h \subseteq \mathrm{hvars}(\sigma)$. Thus, to prove the result, we will show, by contradiction, that $\sigma \in \gamma_F\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi\bigr)$.

Suppose therefore that $\sigma \notin \gamma_F\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi\bigr)$. Then there exists $\tau \in \downarrow\sigma$ such that

$$\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi\bigr)\bigl(\mathrm{hval}(\tau)\bigr) = 0. \tag{86}$$

Take $t \in \mathit{GTerms} \cap \mathit{HTerms}$ and let

$$\upsilon \stackrel{\mathrm{def}}{=} \Bigl\{\, y \mapsto t \Bigm| y \in \mathrm{vars}(\sigma) \cap \bigl(\mathrm{hvars}(\tau) \setminus \mathrm{dom}(\sigma)\bigr) \,\Bigr\}. \tag{87}$$

By Lemma 39, $\tau' \stackrel{\mathrm{def}}{=} \sigma \cup \upsilon \in \mathit{RSubst}$ is satisfiable in $\mathcal{RT}$.

Let z be any variable in $\mathrm{hvars}(\sigma)$. By Proposition 54, we have $\mathrm{rt}(z, \sigma) \in \mathit{HTerms}$. Then, by Proposition 53, there must exists $i \in \mathbb{N}$ such that $\mathrm{rt}(z, \sigma) = z\sigma^i$ and $\mathrm{vars}(z\sigma^i) \cap \mathrm{dom}(\sigma) = \varnothing$. Therefore, by Definition 12, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\sigma)$. Thus, we have

$$\mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\sigma) \setminus \mathrm{dom}(\sigma). \tag{88}$$

By Lemma 41, as $\tau \in \downarrow\sigma$, $\mathcal{RT} \vdash \forall\bigl(\tau \rightarrow (z = z\sigma^i)\bigr)$. By Lemma 43, we have $\mathrm{rt}(z, \tau) = \mathrm{rt}(z\sigma^i, \tau)$ so that, by case (56b) of Corollary 56,

$$z \in \mathrm{hvars}(\tau) \iff \mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\tau). \tag{89}$$

We now show that

$$\mathrm{hvars}(\tau) = \mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\tau'). \tag{90}$$

Since $\tau \in \downarrow\sigma$, it follows from case (15a) of Proposition 15 that $\mathrm{hvars}(\tau) \subseteq \mathrm{hvars}(\sigma)$. Thus, as $z \in \mathrm{hvars}(\sigma)$, either $z \in \mathrm{hvars}(\tau)$ or $z \in \mathrm{hvars}(\sigma) \setminus \mathrm{hvars}(\tau)$. We consider these cases separately.

First, assume that $z \in \mathrm{hvars}(\tau)$. Then, by (89), we have $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{hvars}(\tau)$. Also, by case (15a) of Proposition 15, we have $z \in \mathrm{hvars}(\sigma)$, so that we can apply (88) to derive $\mathrm{vars}(z\sigma^i) \cap \mathrm{dom}(\sigma) = \varnothing$. Therefore, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{dom}(\upsilon)$ and, by Definitions 9 and 12, $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\upsilon) \cap \mathrm{hvars}(\upsilon)$. Since $\tau' \in \downarrow\upsilon$, by case (15b) of Proposition 15, we have $\mathrm{vars}(z\sigma^i) \subseteq \mathrm{gvars}(\tau') \cap \mathrm{hvars}(\tau')$. Thus, by Corollary 56, $\mathrm{rt}(z\sigma^i, \tau') \in \mathit{GTerms} \cap \mathit{HTerms}$. Now $\tau' \in \downarrow\sigma$ so that, by Lemma 41, we have $\mathcal{RT} \vdash \forall\bigl(\tau' \rightarrow (z = z\sigma^i)\bigr)$. Thus, by Lemma 43, $\mathrm{rt}(z\sigma^i, \tau') = \mathrm{rt}(z, \tau') \in \mathit{GTerms} \cap \mathit{HTerms}$ so that, by Propositions 54 and 55, $z \in \mathrm{hvars}(\tau') \cap \mathrm{gvars}(\tau')$. Hence, by case (15a) of Proposition 15, we can conclude $z \in \mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\tau')$. Thus $\mathrm{hvars}(\tau) \subseteq \mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\tau')$.

Secondly, we assume that $z \in \mathrm{hvars}(\sigma) \setminus \mathrm{hvars}(\tau)$. Since $z \notin \mathrm{hvars}(\tau)$, by (89), there exists $y \in \mathrm{vars}(z\sigma^i) \setminus \mathrm{hvars}(\tau)$. Also, since $z \in \mathrm{hvars}(\sigma)$, by (88), we have

$y \in \mathrm{hvars}(\sigma) \setminus \mathrm{dom}(\sigma)$ so that, by Definition 9, we have $y \notin \mathrm{gvars}(\sigma)$. By (87), since $y \notin \mathrm{dom}(\sigma) \cup \mathrm{hvars}(\tau)$, we have $y \notin \mathrm{dom}(\upsilon)$ so that $y \notin \mathrm{gvars}(\tau')$. Thus, by case (56a) of Corollary 56, we have $\mathrm{rt}(z\sigma^i, \tau') \notin \mathit{GTerms}$. Moreover, since we have $\mathcal{RT} \vdash \forall\bigl(\tau' \to (z = z\sigma^i)\bigr)$, we obtain, by Lemma 43, $\mathrm{rt}(z\sigma^i, \tau') = \mathrm{rt}(z, \tau') \notin \mathit{GTerms}$ and thus, by Proposition 55, $z \notin \mathrm{gvars}(\tau')$. Thus $\mathrm{hvars}(\tau) \supseteq \mathrm{hvars}(\sigma) \cap \mathrm{gvars}(\tau')$.

It follows from (86) and (90) that,

$$\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi\bigr)\bigl(\mathrm{gval}(\tau')\bigr) = 0. \tag{91}$$

We have by hypothesis that $\sigma \in \gamma_G(\psi)$, so that, as $\tau' \in {\downarrow}\,\sigma$, by Definition 28 we have $\psi\bigl(\mathrm{gval}(\tau')\bigr) = 1$. Therefore, as $\psi \models \exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi$,

$$\bigl(\exists\, VI \setminus \mathrm{hvars}(\sigma) \,.\, \psi\bigr)\bigl(\mathrm{gval}(\tau')\bigr) = 1.$$

which contradicts (91). ∎

Proof of Theorem 34 on page 23. Let us assume the hypotheses. For the case where $i = 1$ we have:

$$\begin{aligned}
\phi_1 &\stackrel{\text{def}}{=} \phi \vee \phi' \\
&\models (\exists\, VI \setminus h \,.\, \psi) \vee (\exists\, VI \setminus h' \,.\, \psi') \\
&\models \bigl(\exists\, VI \setminus (h \cap h') \,.\, \psi\bigr) \vee \bigl(\exists\, VI \setminus (h \cap h') \,.\, \psi'\bigr) \\
&= \exists\, VI \setminus (h \cap h') \,.\, \psi \vee \psi' \\
&\stackrel{\text{def}}{=} \exists\, VI \setminus h_1 \,.\, \psi_1.
\end{aligned}$$

Since by hypothesis we have that $\phi \models \exists\, VI \setminus h \,.\, \psi$ and existential quantification is a monotonic operation, for the case where $i = 2$ we have:

$$\begin{aligned}
\phi_2 &\stackrel{\text{def}}{=} \exists x \,.\, \phi \\
&\models \exists x \,.\, \exists\, VI \setminus h \,.\, \psi \\
&= \exists\, VI \setminus h \,.\, \exists x \,.\, \psi \\
&= \exists\, VI \setminus \bigl(h \cup \{x\}\bigr) \,.\, \exists x \,.\, \psi \\
&\stackrel{\text{def}}{=} \exists\, VI \setminus h_2 \,.\, \psi_2.
\end{aligned}$$

∎