A Correct, Precise and Efficient Integration of Set-Sharing, Freeness and Linearity for the Analysis of Finite and Rational Tree Languages∗

PATRICIA M. HILL
School of Computing, University of Leeds, Leeds, U.K.
(*e-mail:* `hill@comp.leeds.ac.uk`)

ENEA ZAFFANELLA, ROBERTO BAGNARA
Department of Mathematics, University of Parma, Italy
(*e-mail:* `{zaffanella,bagnara}@cs.unipr.it`)

Abstract

It is well-known that freeness and linearity information positively interact with aliasing information, allowing both the precision and the efficiency of the sharing analysis of logic programs to be improved. In this paper we present a novel combination of set-sharing with freeness and linearity information, which is characterized by an improved abstract unification operator. We provide a new abstraction function and prove the correctness of the analysis for both the finite tree and the rational tree cases. Moreover, we show that the same notion of redundant information as identified in (Bagnara et al. 2002; Zaffanella et al. 2002) also applies to this abstract domain combination: this allows for the implementation of an abstract unification operator running in polynomial time and achieving the same precision on all the considered observable properties.

KEYWORDS: Abstract Interpretation; Logic Programming; Abstract Unification; Rational Trees; Set-Sharing; Freeness; Linearity.

1 Introduction

Even though the set-sharing domain is, in a sense, remarkably precise, more precision is attainable by combining it with other domains. In particular, freeness and linearity information has received much attention by the literature on sharing analysis (recall that a variable is said to be free if it is not bound to a non-variable term; it is linear if it is not bound to a term containing multiple occurrences of another variable).

∗ The present work has been funded by MURST projects "Automatic Program Certification by Abstract Interpretation", "Abstract Interpretation, type systems and control-flow analysis", and "Automatic Aggregate- and Number-Reasoning for Computing: from Decision Algorithms to Constraint Programming with Multisets, Sets, and Maps"; by the Integrated Action Italy-Spain "Advanced Development Environments for Logic Programs"; by the University of Parma's FIL scientific research project (ex 60%) "Pure and applied mathematics"; and by the UK's Engineering and Physical Sciences Research Council (EPSRC) under grant M05645.

As argued informally by Søndergaard (Søndergaard 1986), the mutual interaction between linearity and aliasing information can improve the accuracy of a sharing analysis. This observation has been formally applied in (Codish et al. 1991) to the specification of the abstract mgu operator for the domain ASub. In his PhD thesis (Langen 1990), Langen proposed a similar integration with linearity, but for the set-sharing domain. He has also shown how the aliasing information allows to compute freeness with a good degree of accuracy (however, freeness information was not exploited to improve aliasing). King (King 1994) has also shown how a more refined tracking of linearity allows for further precision improvements.

The synergy attainable from a bi-directional interaction between aliasing and freeness information was initially pointed out by Muthukumar and Hermenegildo (Muthukumar and Hermenegildo 1991; Muthukumar and Hermenegildo 1992). Since then, several authors considered the integration of set-sharing with freeness, sometimes also including additional explicit structural information (Codish et al. 1993; Codish et al. 1996; Filé 1994; King and Soper 1994).

Building on the results obtained in (Søndergaard 1986), (Codish et al. 1991) and (Muthukumar and Hermenegildo 1991), but independently from (Langen 1990), Hans and Winkler (Hans and Winkler 1992) proposed a combined integration of freeness and linearity information with set-sharing. Similar combinations have been proposed in (Bruynooghe and Codish 1993; Bruynooghe et al. 1994a; Bruynooghe et al. 1994b). From a more pragmatic point of view, Codish et al. (Codish et al. 1993; Codish et al. 1995) integrate the information captured by the domains of (Søndergaard 1986) and (Muthukumar and Hermenegildo 1991) by performing the analysis with both domains at the same time, exchanging information between the two components at each step.

Most of the above proposals differ in the carrier of the underlying abstract domain. Even when considering the simplest domain combinations where explicit structural information is ignored, there is no general consensus on the specification of the abstract unification procedure. From a theoretical point of view, once the abstract domain has been related to the concrete one by means of a Galois connection, it is always possible to specify the best correct approximation of each operator of the concrete semantics. However, empirical observations suggest that sub-optimal operators are likely to result in better complexity/precision trade-offs (Bagnara et al. 2000). As a consequence, it is almost impossible to identify "the right combination" of variable aliasing with freeness and linearity information, at least when practical issues, such as the complexity of the abstract unification procedure, are taken into account.

Given this state of affairs, we will now consider a domain combination whose carrier is essentially the same as specified by Langen (Langen 1990) and Hans and Winkler (Hans and Winkler 1992). (The same domain combination was also considered by Bruynooghe et al. (Bruynooghe et al. 1994a; Bruynooghe et al. 1994b), but with the addition of compoundness and explicit structural information.) The novelty of our proposal lies in the specification of an improved abstract unification procedure, better exploiting the interaction between sharing and linearity. As a matter of fact, we provide an example showing that all previous approaches to the combination of set-sharing with freeness and linearity are not uniformly more precise than the analysis based on the ASub domain (Codish et al. 1991; King 2000; Søndergaard 1986), whereas such a property is enjoyed by our proposal.

By extending the results of (Hill et al. 2002) to this combination, we provide a new abstraction function that can be applied to any logic language computing on domains of syntactic structures, with or without the occurs-check; by using this abstraction function, we also prove the correctness of the new abstract unification procedure. Moreover, we show that the same notion of redundant information as identified in (Bagnara et al. 2002; Zaffanella et al. 2002) also applies to this abstract domain combination. As a consequence, it is possible to implement an algorithm for abstract unification running in polynomial time and still obtain the same precision on all the considered observables: groundness, independence, freeness and linearity.

This paper is based on (Zaffanella 2001, Chapter 6), the PhD thesis of the second author. In Section 2, we define some notation and recall the basic concepts used later in the paper. In Section 3, we present the domain *SFL* that integrates set-sharing, freeness and linearity. In Section 4, we show that *SFL* is uniformly more precise than the domain ASub, whereas all the previous proposals for a domain integrating set-sharing and linearity fail to satisfy such a property. In Section 5, we show that the domain *SFL* can be simplified by removing some redundant information. In Section 6, we provide an experimental evaluation using the China analyzer (Bagnara 1997). In Section 7, we discuss some related work. Section 8 concludes with some final remarks. The proofs of the results stated here are not included but all of them are available in an extended version of this paper (Hill et al. 2003).

2 Preliminaries

For a set S, $\wp(S)$ is the powerset of S. The cardinality of S is denoted by $\# S$ and the empty set is denoted by $\varnothing$. The notation $\wp_{\mathrm{f}}(S)$ stands for the set of all the *finite* subsets of S, while the notation $S \subseteq_{\mathrm{f}} T$ stands for $S \in \wp_{\mathrm{f}}(T)$. The set of all finite sequences of elements of S is denoted by S^*, the empty sequence by ϵ, and the concatenation of $s_1, s_2 \in S^*$ is denoted by $s_1 \mathbin{.} s_2$.

2.1 Terms and Trees

Let *Sig* denote a possibly infinite set of function symbols, ranked over the set of natural numbers. Let *Vars* denote a denumerable set of variables, disjoint from *Sig*. Then *Terms* denotes 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 inner 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). It is assumed that *Sig* contains at least two distinct function symbols, with one of them having rank 0.

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 $\mathrm{vars}(s) \cap \mathrm{vars}(t) = \varnothing$; we say that variable y *occurs linearly in* t, more briefly written using the predication $\mathrm{occ\_lin}(y, t)$, if y occurs exactly once in $\mathrm{mvars}(t)$; t is said to be *ground* if $\mathrm{vars}(t) = \varnothing$; t is *free* if $t \in \mathit{Vars}$; t is *linear* if, for all $y \in \mathrm{vars}(t)$, we have $\mathrm{occ\_lin}(y, t)$; 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.

2.2 Substitutions

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,

$$\mathrm{dom}(\sigma) \stackrel{\mathrm{def}}{=} \bigl\{\, x \in \mathit{Vars} \bigm| \sigma(x) \neq x \,\bigr\},$$

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 $t \in \mathit{HTerms}$:

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

If $t \in \mathit{HTerms}$, we write $t\sigma$ to denote $\sigma(t)$. Note that, for each substitution σ and each finite term $t \in \mathit{HTerms}$, if $t\sigma \in \mathit{Vars}$, then $t \in \mathit{Vars}$.

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

$$\bigl\{\, x \mapsto x\sigma \bigm| x \in \mathrm{dom}(\sigma) \,\bigr\}.$$

We denote by $\mathrm{vars}(\sigma)$ the set of variables occurring in the bindings of σ. We also define $\mathrm{range}(\sigma) \stackrel{\mathrm{def}}{=} \bigcup \bigl\{\, \mathrm{vars}(x\sigma) \bigm| x \in \mathrm{dom}(\sigma) \,\bigr\}$.

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, ..., 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*. A substitution σ is *idempotent* if, for all $t \in \mathit{Terms}$, we have $t\sigma\sigma = t\sigma$. Equivalently, σ is idempotent if and only if $\mathrm{dom}(\sigma) \cap \mathrm{range}(\sigma) = \varnothing$. The set of all idempotent substitutions is denoted by *ISubst* and $\mathit{ISubst} \subset \mathit{RSubst}$.

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

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

and has the formulation

$$\tau \circ \sigma = \{\, x \mapsto x\sigma\tau \mid x \in \mathrm{dom}(\sigma) \cup \mathrm{dom}(\tau), x \neq x\sigma\tau \,\}. \tag{1}$$

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

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

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

converges to a (possibly infinite) term, denoted $\sigma^\infty(s)$ (Intrigila and Zilli 1996; King 2000). Therefore, the function $\mathrm{rt}\colon \mathit{HTerms} \times \mathit{RSubst} \to \mathit{Terms}$ such that

$$\mathrm{rt}(s, \sigma) \stackrel{\mathrm{def}}{=} \sigma^\infty(s)$$

is well defined. Note that, in general, this function is not a substitution: while having a finite domain, its "bindings" $x \mapsto \mathrm{rt}(x, \sigma)$ can map a domain variable x into a term $\mathrm{rt}(x, \sigma) \in \mathit{Terms} \setminus \mathit{HTerms}$. However, as the name of the function suggests, the term $\mathrm{rt}(x, \sigma)$ is granted to be *rational*, meaning that it can only have a finite number of distinct subterms and hence, be finitely represented.

Example 1
Consider the substitutions

$$\begin{aligned}
\sigma_1 &= \{x \mapsto f(z), y \mapsto a\} && \in \mathit{ISubst},\\
\sigma_2 &= \{x \mapsto f(y), y \mapsto a\} && \in \mathit{RSubst} \setminus \mathit{ISubst},\\
\sigma_3 &= \{x \mapsto f(x)\} && \in \mathit{RSubst} \setminus \mathit{ISubst},\\
\sigma_4 &= \{x \mapsto f(y), y \mapsto f(x)\} && \in \mathit{RSubst} \setminus \mathit{ISubst},\\
\sigma_5 &= \{x \mapsto y, y \mapsto x\} && \notin \mathit{RSubst}.
\end{aligned}$$

Note that there are substitutions, such as σ_2, that are not idempotent and nonetheless define finite trees only; namely, $\mathrm{rt}(x, \sigma_2) = f(a)$. Similarly, there are other substitutions, such as σ_4, whose bindings are not explicitly cyclic and nonetheless define rational trees that are infinite; namely, $\mathrm{rt}(x, \sigma_4) = f(f(f(\cdots)))$. Finally note that the 'rt' function is not defined on $\sigma_5 \notin \mathit{RSubst}$.

2.3 Equality Theories

An *equation* is 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 $\{\, s \mapsto t \mid (s = t) \in e \,\} \in \mathit{RSubst}$. 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). As is common in research work involving equality, we overload the symbol '=' and use it to denote both equality and to represent syntactic identity. The context makes it clear what is intended.

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

$$s = s, \tag{2}$$

$$s = t \leftrightarrow t = s, \tag{3}$$

$$r = s \wedge s = t \rightarrow r = t, \tag{4}$$

$$s_1 = t_1 \wedge \cdots \wedge s_n = t_n \rightarrow f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n). \tag{5}$$

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 $n \neq m$:

$$f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \rightarrow s_1 = t_1 \wedge \cdots \wedge s_n = t_n, \tag{6}$$

$$\neg\bigl(f(s_1, \ldots, s_n) = g(t_1, \ldots, t_m)\bigr). \tag{7}$$

The axioms characterized by schemata (6) and (7) 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 (Clark 1978), denoted $\mathcal{FT}$, on which pure logic programming is based, usually called the *Herbrand* equality theory, is given by the congruence axioms, the identity axioms, and the axiom schema

$$\forall z \in \mathit{Vars} : \forall t \in (\mathit{HTerms} \setminus \mathit{Vars}) : z \in \operatorname{vars}(t) \rightarrow \neg(z = t). \tag{8}$$

Axioms characterized by the schema (8) 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 logic programming systems, such as Prolog II, SICStus and Oz, does not require the occurs-check axioms. This approach is based on the theory of rational trees (Colmerauer 1982; Colmerauer 1984), denoted $\mathcal{RT}$. 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 variable which is not in the domain, the substitution uniquely defines a ground rational tree for each of its domain variables. 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 expect. We refer the interested reader to (Jaffar et al. 1987; Keisu 1994; Maher 1988) for details on the subject.

In the sequel we use the expression "equality theory" to denote any consistent, decidable theory T satisfying the congruence axioms. We also use the expression "syntactic equality theory" to denote any equality theory T also satisfying the identity axioms.

We say that a substitution $\sigma \in \mathit{RSubst}$ is *satisfiable* in an equality theory T if, when interpreting σ as an equation system in rational solved form,

$$T \vdash \forall\bigl(\mathit{Vars} \setminus \operatorname{dom}(\sigma)\bigr) : \exists \operatorname{dom}(\sigma) \,.\, \sigma.$$

Let $e \in \wp_{\mathrm{f}}(\mathit{Eqs})$ be a set of equations in an equality theory T. A substitution $\sigma \in \mathit{RSubst}$ is called a *solution for e in T* if σ is satisfiable in T and $T \vdash \forall(\sigma \rightarrow e)$; we say that e is satisfiable if it has a solution. If $\operatorname{vars}(\sigma) \subseteq \operatorname{vars}(e)$, 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, a most general solution is always a relevant solution of e. When the theory T is clear from the context, the set of all the relevant most general solutions for e in T is denoted by $\mathrm{mgs}(e)$.

Example 2
Let $e = \bigl\{g(x) = g(f(y)), f(x) = y, z = g(w)\bigr\}$ and

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

Then, for any syntactic equality theory T, we have $T \vdash \forall(\sigma \leftrightarrow e)$. Since $\sigma \in \mathit{RSubst}$, then σ and hence e is satisfiable in $\mathcal{RT}$. Intuitively, whatever rational tree t_w is assigned to the parameter variable w, there exist rational trees t_x, t_y and t_z that, when assigned to the domain variables x, y and z, will turn σ into a set of trivial identities; namely, let t_x and t_y be both equal to the infinite rational tree $f(f(f(\cdots)))$, which is usually denoted by f^ω, and let t_z be the rational tree $g(t_w)$. Thus σ is a relevant most general solution for e in $\mathcal{RT}$. In contrast,

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

is just a relevant solution for e in $\mathcal{RT}$. Also observe that, for any equality theory T,

$$T \vdash \forall\Bigl(\sigma \rightarrow \bigl\{x = f(f(x))\bigr\}\Bigr)$$

so that σ does not satisfy the occurs-check axioms. Therefore, neither σ nor e are satisfiable in the Herbrand equality theory $\mathcal{FT}$. Intuitively, there is no finite tree t_x such that $t_x = f(f(t_x))$.

We have the following useful result regarding 'rt' and satisfiable substitutions that are equivalent with respect to any given syntactic equality theory.

Proposition 3
Let $\sigma, \tau \in \mathit{RSubst}$ be satisfiable in the syntactic equality theory T and suppose that $T \vdash \forall(\sigma \leftrightarrow \tau)$. Then

$$\mathrm{rt}(y, \sigma) \in \mathit{Vars} \iff \mathrm{rt}(y, \tau) \in \mathit{Vars}, \tag{9}$$
$$\mathrm{rt}(y, \sigma) \in \mathit{GTerms} \iff \mathrm{rt}(y, \tau) \in \mathit{GTerms}, \tag{10}$$
$$\mathrm{rt}(y, \sigma) \in \mathit{LTerms} \iff \mathrm{rt}(y, \tau) \in \mathit{LTerms}. \tag{11}$$

2.4 Galois Connections and Upper Closure Operators

Given two complete lattices $(C, \leq_C)$ and $(A, \leq_A)$, a *Galois connection* is a pair of monotonic functions $\alpha\colon C \rightarrow A$ and $\gamma\colon A \rightarrow C$ such that

$$\forall c \in C : c \leq_C \gamma\bigl(\alpha(c)\bigr), \qquad \forall a \in A : \alpha\bigl(\gamma(a)\bigr) \leq_A a.$$

The functions α and γ are said to be the abstraction and concretization functions, respectively. A *Galois insertion* is a Galois connection where the concretization function γ is injective.

An *upper closure operator* (uco) $\rho\colon C \rightarrow C$ on the complete lattice $(C, \leq_C)$ is a monotonic, idempotent and extensive[1] self-map. The set of all uco's on C, denoted by $\mathrm{uco}(C)$, is itself a complete lattice. For any $\rho \in \mathrm{uco}(C)$, the set $\rho(C)$, i.e., the image under ρ of the lattice carrier, is a complete lattice under the same partial order $\leq_C$ defined on C. Given a Galois connection, the function $\rho \stackrel{\mathrm{def}}{=} \gamma \circ \alpha$ is an element of $\mathrm{uco}(C)$. The presentation of abstract interpretation in terms of Galois connections can be rephrased by using uco's. In particular, the partial order $\sqsubseteq$ defined on $\mathrm{uco}(C)$ formalizes the intuition of an abstract domain being more precise than another one; moreover, given two elements $\rho_1, \rho_2 \in \mathrm{uco}(C)$, their reduced product (Cousot and Cousot 1979), denoted $\rho_1 \sqcap \rho_2$, is their glb on $\mathrm{uco}(C)$.

2.5 The Set-Sharing Domain

The set-sharing domain of Jacobs and Langen (Jacobs and Langen 1989), encodes both aliasing and groundness information. Let $\mathit{VI} \subseteq_{\mathrm{f}} \mathit{Vars}$ be a fixed and finite set of variables of interest. An element of the set-sharing domain (a *sharing set*) is a set of subsets of VI (the *sharing groups*). Note that the empty set is not a sharing group.

Definition 4
(The *set-sharing* lattice.) Let $\mathit{SG} \stackrel{\mathrm{def}}{=} \wp(\mathit{VI}) \setminus \{\varnothing\}$ be the set of *sharing groups*. The set-sharing lattice is defined as $\mathit{SH} \stackrel{\mathrm{def}}{=} \wp(\mathit{SG})$, ordered by subset inclusion.

The following operators on SH are needed for the specification of the abstract semantics.

Definition 5
(Auxiliary operators on SH.) For each $\mathit{sh}, \mathit{sh}_1, \mathit{sh}_2 \in \mathit{SH}$ and each $V \subseteq \mathit{VI}$, we define the following functions:
the *star-union* function $(\cdot)^\star \colon \mathit{SH} \to \mathit{SH}$, is defined as

$$\mathit{sh}^\star \stackrel{\mathrm{def}}{=} \bigl\{\, S \in \mathit{SG} \bigm| \exists n \geq 1 \,.\, \exists S_1, \ldots, S_n \in \mathit{sh} \,.\, S = S_1 \cup \cdots \cup S_n \,\bigr\};$$

the extraction of the *relevant component of sh with respect to V* is encoded by $\mathrm{rel} \colon \wp(\mathit{VI}) \times \mathit{SH} \to \mathit{SH}$ defined as

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

the *irrelevant component of sh with respect to V* is thus defined as

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

the *binary union* function $\mathrm{bin} \colon \mathit{SH} \times \mathit{SH} \to \mathit{SH}$ is defined as

$$\mathrm{bin}(\mathit{sh}_1, \mathit{sh}_2) \stackrel{\mathrm{def}}{=} \{\, S_1 \cup S_2 \mid S_1 \in \mathit{sh}_1, S_2 \in \mathit{sh}_2 \,\};$$

[1] Namely, $c \leq_C \rho(c)$ for each $c \in C$.

the *self-bin-union* operation on SH is defined as

$$sh^2 \stackrel{\text{def}}{=} \operatorname{bin}(sh, sh);$$

the *abstract existential quantification* function aexists: $SH \times \wp(VI) \to SH$ is defined as

$$\operatorname{aexists}(sh, V) \stackrel{\text{def}}{=} \{\, S \setminus V \mid S \in sh, S \setminus V \neq \varnothing \,\} \cup \{\, \{x\} \mid x \in V \,\}.$$

In (Bagnara et al. 1997; Bagnara et al. 2002) it was shown that the domain SH contains many elements that are redundant for the computation of the actual *observable* properties of the analysis, definite groundness and definite independence. The following formalization of these observables is a rewording of the definitions provided in (Zaffanella et al. 1999; Zaffanella et al. 2002).

Definition 6
(The observables of SH.) The *groundness* and *independence* observables (on SH) $\rho_{Con}, \rho_{PS} \in \operatorname{uco}(SH)$ are defined, for each $sh \in SH$, by

$$\rho_{Con}(sh) \stackrel{\text{def}}{=} \{\, S \in SG \mid S \subseteq \operatorname{vars}(sh) \,\},$$
$$\rho_{PS}(sh) \stackrel{\text{def}}{=} \{\, S \in SG \mid (P \subseteq S \land \#P = 2) \implies (\exists T \in sh \,.\, P \subseteq T) \,\}.$$

Note that, as usual in sharing analysis domains, definite groundness and definite independence are both represented by encoding possible non-groundness and possible pair-sharing information.

The abstract domain PSD (Bagnara et al. 2002; Zaffanella et al. 2002) is the simplest abstraction of the domain SH that still preserves the same precision on groundness and independence.

Definition 7
(The *pair-sharing dependency* lattice PSD.) The operator $\rho_{PSD} \in \operatorname{uco}(SH)$ is defined, for each $sh \in SH$, by

$$\rho_{PSD}(sh) \stackrel{\text{def}}{=} \left\{\, S \in SG \;\middle|\; \forall y \in S : S = \bigcup \{\, U \in sh \mid y \in U \subseteq S \,\} \,\right\}.$$

The *pair-sharing dependency* lattice is $PSD \stackrel{\text{def}}{=} \rho_{PSD}(SH)$.

In the following example we provide an intuitive interpretation of the approximation induced by the three upper closure operators of Definitions 6 and 7.

Example 8
Let $VI = \{v, w, x, y, z\}$ and consider[2] $sh = \{vx, vy, xy, xyz\}$. Then

$$\rho_{Con}(sh) = \{v, vx, vxy, vxyz, vxz, vy, vyz, vz, x, xy, xyz, xz, y, yz, z\},$$
$$\rho_{PS}(sh) = \{v, vx, vxy, vy, w, x, xy, xyz, xz, y, yz, z\},$$

[2] In this and all the following examples, we will adopt a simplified notation for a set-sharing element sh, omitting inner braces. For instance, we will write $\{xy, xz, yz\}$ to denote $\{\{x, y\}, \{x, z\}, \{y, z\}\}$.

$$\rho_{PSD}(sh) = \{vx, vxy, vy, xy, xyz\}.$$

When observing $\rho_{Con}(sh)$, the only information available is that variable w does not occur in a sharing group; intuitively, this means that w is definitely ground. All the other information encoded in sh is lost; for instance, in sh variables v and z never occur in the *same* sharing group (i.e., they are definitely independent), while this happens in $\rho_{Con}(sh)$.

When observing $\rho_{PS}(sh)$, it should be noted that two distinct variables occur in the same sharing group if and only if they were also occurring together in a sharing group of sh, so that the definite independence information is preserved (e.g., v and z keep their independence). On the other hand, all the variables in VI occur as singletons in $\rho_{PS}(sh)$ whether or not they are known to be ground; for instance, $\{w\}$ occurs in $\rho_{PS}(sh)$ although w does not occur in any sharing group in sh.

By noting that $\rho_{PSD}(sh) \subset \rho_{Con}(sh) \cap \rho_{PS}(sh)$, it follows that $\rho_{PSD}(sh)$ preserves both the definite groundness and the definite independence information of sh; moreover, as the inclusion is strict, $\rho_{PSD}(sh)$ encodes other information, such as variable covering (the interested reader is referred to (Bagnara et al. 2002; Zaffanella et al. 2002) for a more formal discussion).

2.6 Variable-Idempotent Substitutions

One of the key concepts used in (Hill et al. 2003) for the proofs of the correctness results stated in this paper is that of variable-idempotence. For the interested reader, we provide here a brief introduction to variable-idempotent substitutions, although these are not referred to elsewhere in the paper.

The definition of idempotence requires that repeated applications of a substitution do not change the syntactic structure of a term and idempotent substitutions are normally the preferred form of a solution to a set of equations. However, in the domain of rational trees, a set of solvable equations does not necessarily have an idempotent solution (for instance, in Example 2, the set of equations e has no idempotent solution). On the other hand, several abstractions of terms, such as the ones commonly used for sharing analysis, are only interested in the set of variables occurring in a term and not in the concrete structure that contains them. Thus, for applications such as sharing analysis, a useful way to relax the definition of idempotence is to ignore the structure of terms and just require that the repeated application of a substitution leaves the set of variables in a term invariant.

Definition 9
(Variable-idempotence.) A substitution $\sigma \in RSubst$ is *variable-idempotent*[3] if and only if for all $t \in HTerms$ we have

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

[3] This definition, which is the same as that originally provided in (Hill et al. 1998), is slightly stronger than the one adopted in (Hill et al. 2002), which disregarded the domain variables of the substitution. The adoption of this stronger definition allows for some simplifications in the correctness proofs for freeness and linearity.

The set of variable-idempotent substitutions is denoted *VSubst*.

As any idempotent substitution is also variable-idempotent, we have $\mathit{ISubst} \subset \mathit{VSubst} \subset \mathit{RSubst}$.

Example 10
Consider the following substitutions which are all in *RSubst*.

$$\begin{aligned}
\sigma_1 &= \bigl\{x \mapsto f(y)\bigr\} && \in \mathit{ISubst} \subset \mathit{VSubst},\\
\sigma_2 &= \bigl\{x \mapsto f(x)\bigr\} && \in \mathit{VSubst} \setminus \mathit{ISubst},\\
\sigma_3 &= \bigl\{x \mapsto f(y,z), y \mapsto f(z,y)\bigr\} && \in \mathit{VSubst} \setminus \mathit{ISubst},\\
\sigma_4 &= \bigl\{x \mapsto y, y \mapsto f(x,y)\bigr\} && \notin \mathit{VSubst}.
\end{aligned}$$

3 The Domain *SFL*

The abstract domain *SFL* is made up of three components, providing different kinds of sharing information regarding the set of variables of interest VI: the first component is the set-sharing domain *SH* of Jacobs and Langen (Jacobs and Langen 1989); the other two components provide freeness and linearity information, each represented by simply recording those variables of interest that are known to enjoy the corresponding property.

Definition 11
(The domain *SFL*.) Let $F \stackrel{\mathrm{def}}{=} \wp(\mathit{VI})$ and $L \stackrel{\mathrm{def}}{=} \wp(\mathit{VI})$ be partially ordered by reverse subset inclusion. The abstract domain *SFL* is defined as

$$\mathit{SFL} \stackrel{\mathrm{def}}{=} \bigl\{\, \langle sh, f, l\rangle \bigm| sh \in \mathit{SH}, f \in F, l \in L \,\bigr\}$$

and is ordered by $\leq_S$, the component-wise extension of the orderings defined on the sub-domains. With this ordering, *SFL* is a complete lattice whose least upper bound operation is denoted by alub_S. The bottom element $\langle \varnothing, \mathit{VI}, \mathit{VI}\rangle$ will be denoted by $\bot_S$.

3.1 The Abstraction Function

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.[4] 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

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

[4] As usual, this is modulo the possible renaming of variables.

for $n = 1, 2, \dots,$ all map the variable x into the same infinite rational tree f^ω.

Ideally, a strong normal form for the set of rational trees described by a substitution $\sigma \in \mathit{RSubst}$ can be obtained by computing the limit σ^∞. The problem is that σ^∞ can map domain variables to infinite rational terms and may not be in RSubst.

This poses a non-trivial problem when trying to define "good" abstraction functions, since it would be really desirable for this function to map any two equivalent concrete elements to the same abstract element. As shown in (Hill et al. 2002), the classical abstraction function for set-sharing analysis (Cortesi and Filé 1999; Jacobs and Langen 1989), which was defined only for substitutions that are idempotent, does not enjoy this property when applied, as it is, to arbitrary substitutions in rational solved form. In (Hill et al. 1998; Hill et al. 2002), this problem is solved by replacing the sharing group operator 'sg' of (Jacobs and Langen 1989) by an occurrence operator, 'occ', defined by means of a fixpoint computation. However, to simplify the presentation, here we define 'occ' directly by exploiting the fact that the number of iterations needed to reach the fixpoint is bounded by the number of bindings in the substitution.

Definition 12

(Occurrence operator.) For each $\sigma \in \mathit{RSubst}$ and $v \in \mathit{Vars}$, the *occurrence operator* $\mathrm{occ}\colon \mathit{RSubst} \times \mathit{Vars} \to \wp_\mathrm{f}(\mathit{Vars})$ is defined as

$$\mathrm{occ}(\sigma, v) \stackrel{\mathrm{def}}{=} \bigl\{\, y \in \mathit{Vars} \bigm| n = \#\sigma, v \in \mathrm{vars}(y\sigma^n) \setminus \mathrm{dom}(\sigma) \,\bigr\}.$$

For each $\sigma \in \mathit{RSubst}$, the operator $\mathrm{ssets}\colon \mathit{RSubst} \to \mathit{SH}$ is defined as

$$\mathrm{ssets}(\sigma) \stackrel{\mathrm{def}}{=} \bigl\{\, \mathrm{occ}(\sigma, v) \cap \mathit{VI} \bigm| v \in \mathit{Vars} \,\bigr\} \setminus \{\varnothing\}.$$

The operator 'ssets' is introduced for notational convenience only.

Example 13

Let

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

Then $\mathrm{dom}(\sigma) = \mathrm{dom}(\tau) = \{x_1, x_2, x_3\}$ so that $\mathrm{occ}(\sigma, x_i) = \mathrm{occ}(\tau, x_i) = \varnothing$, for $i = 1$, 2, 3 and $\mathrm{occ}(\sigma, x_4) = \mathrm{occ}(\tau, x_4) = \{x_1, x_2, x_3, x_4\}$. As a consequence, supposing that $\mathit{VI} = \{x_1, x_2, x_3, x_4\}$, we obtain $\mathrm{ssets}(\sigma) = \mathrm{ssets}(\tau) = \{\mathit{VI}\}$.

In a similar way, it is possible to define suitable operators for groundness, freeness and linearity. As all ground trees are linear, a knowledge of the definite groundness information can be useful for proving properties concerning the linearity abstraction. Groundness is already encoded in the abstraction for set-sharing provided in Definition 12; nonetheless, for both a simplified notation and a clearer intuitive reading, we now explicitly define the set of variables that are associated to ground trees by a substitution in RSubst.

Definition 14
(Groundness operator.) The *groundness operator* $\mathrm{gvars}\colon \mathit{RSubst} \to \wp_{\mathrm{f}}(\mathit{Vars})$ is defined, for each $\sigma \in \mathit{RSubst}$, by

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

Example 15
Consider $\sigma \in \mathit{RSubst}$ where

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

Then $\mathrm{gvars}(\sigma) = \{x_1, x_2, x_3, x_4\}$. Observe that $x_1 \in \mathrm{gvars}(\sigma)$ although $x_1\sigma \in \mathit{Vars}$. Also, $x_3 \in \mathrm{gvars}(\sigma)$ although $\mathrm{vars}(x_3\sigma^i) = \{x_2, x_4\} \neq \varnothing$ for all $i \geq 2$.

As for possible sharing, the definite freeness information can be extracted from a substitution in rational solved form by observing the result of a bounded number of applications of the substitution.

Definition 16
(Freeness operator.) The *freeness operator* $\mathrm{fvars}\colon \mathit{RSubst} \to \wp(\mathit{Vars})$ is defined, for each $\sigma \in \mathit{RSubst}$, by

$$\mathrm{fvars}(\sigma) \stackrel{\mathrm{def}}{=} \{\, y \in \mathit{Vars} \mid n = \#\sigma, y\sigma^n \in \mathit{Vars} \,\}.$$

As $\sigma \in \mathit{RSubst}$ has no circular subset, $y \in \mathrm{fvars}(\sigma)$ implies $y\sigma^n \in \mathit{Vars} \setminus \mathrm{dom}(\sigma)$.

Example 17
Let $\mathit{VI} = \{x_1, x_2, x_3, x_4, x_5\}$ and consider $\sigma \in \mathit{RSubst}$ where

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

Then $\mathrm{fvars}(\sigma) \cap \mathit{VI} = \{x_3, x_4, x_5\}$. Thus $x_1 \notin \mathrm{fvars}(\sigma)$ although $x_1\sigma \in \mathit{Vars}$. Also, $x_3 \in \mathrm{fvars}(\sigma)$ although $x_3\sigma \in \mathrm{dom}(\sigma)$.

As in previous cases, the definite linearity information can be extracted by observing the result of a bounded number of applications of the considered substitution.

Definition 18
(Linearity operator.) The *linearity operator* $\mathrm{lvars}\colon \mathit{RSubst} \to \wp(\mathit{Vars})$ is defined, for each $\sigma \in \mathit{RSubst}$, by

$$\mathrm{lvars}(\sigma) \stackrel{\mathrm{def}}{=} \bigl\{\, y \in \mathit{Vars} \bigm| n = \#\sigma, \forall z \in \mathrm{vars}(y\sigma^n) \setminus \mathrm{dom}(\sigma) : \mathrm{occ\_lin}(z, y\sigma^{2n}) \,\bigr\}.$$

In the next example we consider the extraction of linearity from two substitutions. The substitution σ shows that, in contrast with the case of set-sharing and freeness, for linearity we may need to compute up to $2n$ applications, where $n = \#\sigma$; the substitution τ shows that, when observing the term $y\tau^{2n}$, multiple occurrences of domain variables have to be disregarded.

Example 19
Let $VI = \{x_1, x_2, x_3, x_4\}$ and consider $\sigma \in \mathit{RSubst}$ where

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

Then $\mathrm{lvars}(\sigma) \cap VI = \{x_4\}$. Observe that $x_1 \notin \mathrm{lvars}(\sigma)$. This is because $x_4 \notin \mathrm{dom}(\sigma)$, $x_1\sigma^3 = f(x_1, x_4)$ so that $x_4 \in \mathrm{vars}(x_1\sigma^3)$ and $x_1\sigma^6 = f\bigl(f(x_1, x_4), x_4\bigr)$ so that $\mathrm{occ\_lin}(x_4, x_1\sigma^6)$ does not hold. Note also that $\mathrm{occ\_lin}(x_4, x_1\sigma^i)$ holds for $i = 3$, 4, 5.

Consider now $\tau \in \mathit{RSubst}$ where

$$\tau = \bigl\{x_1 \mapsto f(x_2, x_2), x_2 \mapsto f(x_2)\bigr\}.$$

Then $\mathrm{lvars}(\tau) \cap VI = VI$. Note that we have $x_1 \in \mathrm{lvars}(\tau)$ although, for all $i > 0$, $x_2 \in \mathrm{dom}(\tau)$ occurs more than once in the term $x_1\tau^i$.

The occurrence, groundness, freeness and linearity operators are invariant with respect to substitutions that are equivalent in the given syntactic equality theory.

Proposition 20
Let $\sigma, \tau \in \mathit{RSubst}$ be satisfiable in the syntactic equality theory T and suppose that $T \vdash \forall(\sigma \leftrightarrow \tau)$. Then

$$\mathrm{ssets}(\sigma) = \mathrm{ssets}(\tau), \tag{12}$$
$$\mathrm{gvars}(\sigma) = \mathrm{gvars}(\tau), \tag{13}$$
$$\mathrm{fvars}(\sigma) = \mathrm{fvars}(\tau), \tag{14}$$
$$\mathrm{lvars}(\sigma) = \mathrm{lvars}(\tau). \tag{15}$$

Moreover, these operators precisely capture the intended properties over the domain of rational trees.

Proposition 21
If $\sigma \in \mathit{RSubst}$ and $y, v \in \mathit{Vars}$ then

$$y \in \mathrm{occ}(\sigma, v) \iff v \in \mathrm{vars}\bigl(\mathrm{rt}(y, \sigma)\bigr), \tag{16}$$
$$y \in \mathrm{gvars}(\sigma) \iff \mathrm{rt}(y, \sigma) \in \mathit{GTerms}, \tag{17}$$
$$y \in \mathrm{fvars}(\sigma) \iff \mathrm{rt}(y, \sigma) \in \mathit{Vars}, \tag{18}$$
$$y \in \mathrm{lvars}(\sigma) \iff \mathrm{rt}(y, \sigma) \in \mathit{LTerms}. \tag{19}$$

It follows from (16) and (18) that any free variable necessarily shares (at least, with itself). Also, as $\mathit{Vars} \cup \mathit{GTerms} \subset \mathit{LTerms}$, it follows from (17), (18) and (19) that any variable that is either ground or free is also necessarily linear. Thus we have the following corollary.

Corollary 22
If $\sigma \in \mathit{RSubst}$, then

$$\mathrm{fvars}(\sigma) \subseteq \mathrm{vars}\bigl(\mathrm{ssets}(\sigma)\bigr),$$
$$\mathrm{fvars}(\sigma) \cup \mathrm{gvars}(\sigma) \subseteq \mathrm{lvars}(\sigma).$$

We are now in position to define the abstraction function mapping rational trees to elements of the domain *SFL*.

Definition 23
(The abstraction function for *SFL*.) For each substitution $\sigma \in \mathit{RSubst}$, the function $\alpha_S \colon \mathit{RSubst} \to \mathit{SFL}$ is defined by

$$\alpha_S(\sigma) \stackrel{\text{def}}{=} \bigl\langle \operatorname{ssets}(\sigma), \operatorname{fvars}(\sigma) \cap \mathit{VI}, \operatorname{lvars}(\sigma) \cap \mathit{VI} \bigr\rangle,$$

The concrete domain $\wp(\mathit{RSubst})$ is related to *SFL* by means of the *abstraction function* $\alpha_S \colon \wp(\mathit{RSubst}) \to \mathit{SFL}$ such that, for each $\Sigma \in \wp(\mathit{RSubst})$,

$$\alpha_S(\Sigma) \stackrel{\text{def}}{=} \operatorname{alub}_S \bigl\{\, \alpha_S(\sigma) \bigm| \sigma \in \Sigma \,\bigr\}.$$

Since the abstraction function α_S is additive, the concretization function is given by the adjoint (Cousot and Cousot 1977)

$$\gamma_S\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\text{def}}{=} \bigl\{\, \sigma \in \mathit{RSubst} \bigm| \operatorname{ssets}(\sigma) \subseteq sh, \operatorname{fvars}(\sigma) \supseteq f, \operatorname{lvars}(\sigma) \supseteq l \,\bigr\}.$$

With Definition 23 and Proposition 20, one of our objectives is fulfilled: substitutions in *RSubst* that are equivalent have the same abstraction.

Corollary 24
Let $\sigma, \tau \in \mathit{RSubst}$ be satisfiable in the syntactic equality theory T and suppose $T \vdash \forall(\sigma \leftrightarrow \tau)$. Then $\alpha_S(\sigma) = \alpha_S(\tau)$.

Observe that the Galois connection defined by the functions α_S and γ_S is not a Galois insertion since different abstract elements are mapped by γ_S to the same set of concrete computation states. To see this it is sufficient to observe that, by Corollary 22, any abstract element $d = \langle sh, f, l\rangle \in \mathit{SFL}$ such that $f \nsubseteq \operatorname{vars}(sh)$, as is the case for the bottom element $\bot_S$, satisfies $\gamma_S(d) = \gamma_S(\bot_S) = \varnothing$; thus, all such d's will represent the semantics of those program fragments that have no successful computations. Similarly, by letting $V = \bigl(\mathit{VI} \setminus \operatorname{vars}(sh)\bigr) \cup f$, it can be seen that, for any l' such that $V \cup l = V \cup l'$, we have, again by Corollary 22, $\gamma_S(d) = \gamma_S\bigl(\langle sh, f, l'\rangle\bigr)$.

Of course, by taking the abstract domain as the subset of *SFL* that is the co-domain of α_S, we would have a Galois insertion. However, apart from the simple cases shown above, it is somehow difficult to *explicitly* characterize such a set. For instance, as observed in (Filé 1994), if

$$d = \bigl\langle \{xy, xz, yz\}, \{x, y, z\}, \{x, y, z\} \bigr\rangle \in \mathit{SFL}$$

we have $\gamma_S(d) = \gamma_S(\bot_S) = \varnothing$. It is worth stressing that these "spurious" elements do not compromise the correctness of the analysis and, although they can affect the precision of the analysis, they rarely occur in practice (Bagnara et al. 2000; Zaffanella 2001).

3.2 The Abstract Operators

The specification of the abstract unification operator on the domain *SFL* is rather complex, since it is based on a very detailed case analysis. To achieve some modularity, that will be also useful when proving its correctness, in the next definition we introduce several auxiliary abstract operators.

Definition 25
(Auxiliary operators in *SFL*.) Let $s, t \in \mathit{HTerms}$ be finite terms such that $\mathrm{vars}(s) \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. For each $d = \langle sh, f, l \rangle \in \mathit{SFL}$ we define the following predicates:
s and t are *independent in d* if and only if $\mathrm{ind}_d \colon \mathit{HTerms}^2 \to \mathit{Bool}$ holds for (s, t), where

$$\mathrm{ind}_d(s, t) \stackrel{\mathrm{def}}{=} \Bigl(\mathrm{rel}\bigl(\mathrm{vars}(s), sh\bigr) \cap \mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr) = \varnothing\Bigr);$$

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

$$\mathrm{ground}_d(t) \stackrel{\mathrm{def}}{=} \bigl(\mathrm{vars}(t) \subseteq \mathit{VI} \setminus \mathrm{vars}(sh)\bigr);$$

$y \in \mathrm{vars}(t)$ *occurs linearly (in t) in d* if and only if $\mathrm{occ\_lin}_d \colon \mathit{VI} \times \mathit{HTerms} \to \mathit{Bool}$ holds for (y, t), where

$$\begin{aligned}\mathrm{occ\_lin}_d(y, t) \stackrel{\mathrm{def}}{=} \mathrm{ground}_d(y) \lor \Bigl(&\mathrm{occ\_lin}(y, t) \land (y \in l)\\ &\land \forall z \in \mathrm{vars}(t) : \bigl(y \neq z \implies \mathrm{ind}_d(y, z)\bigr)\Bigr);\end{aligned}$$

t is *free in d* if and only if $\mathrm{free}_d \colon \mathit{HTerms} \to \mathit{Bool}$ holds for t, where

$$\mathrm{free}_d(t) \stackrel{\mathrm{def}}{=} (t \in f);$$

t is *linear in d* if and only if $\mathrm{lin}_d \colon \mathit{HTerms} \to \mathit{Bool}$ holds for t, where

$$\mathrm{lin}_d(t) \stackrel{\mathrm{def}}{=} \forall y \in \mathrm{vars}(t) : \mathrm{occ\_lin}_d(y, t).$$

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

$$\mathrm{share\_with}_d(t) \stackrel{\mathrm{def}}{=} \mathrm{vars}\Bigl(\mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr)\Bigr).$$

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

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

As a first correctness result, we have that the auxiliary operators correctly approximate the corresponding concrete properties.

Theorem 26
Let $d \in \mathit{SFL}$, $\sigma \in \gamma_S(d)$ and $y \in \mathit{VI}$. Let also $s, t \in \mathit{HTerms}$ be two finite terms such that $\mathrm{vars}(s) \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Then

$$\mathrm{ind}_d(s, t) \implies \mathrm{vars}\bigl(\mathrm{rt}(s, \sigma)\bigr) \cap \mathrm{vars}\bigl(\mathrm{rt}(t, \sigma)\bigr) = \varnothing; \tag{20}$$

$$\mathrm{ind}_d(y, t) \iff y \notin \mathrm{share\_with}_d(t); \tag{21}$$

$$\mathrm{free}_d(t) \implies \mathrm{rt}(t, \sigma) \in \mathit{Vars}; \tag{22}$$

$$\mathrm{ground}_d(t) \implies \mathrm{rt}(t, \sigma) \in \mathit{GTerms}; \tag{23}$$

$$\mathrm{lin}_d(t) \implies \mathrm{rt}(t, \sigma) \in \mathit{LTerms}. \tag{24}$$

Example 27
Let $VI = \{v, w, x, y, z\}$ and consider the abstract element $d = \langle sh, f, l\rangle \in SFL$, where

$$sh = \{v, wz, xz, z\}, \qquad f = \{v\}, \qquad l = \{v, x, y, z\}.$$

Then, by applying Definition 25, we obtain the following.

- $\mathrm{ground}_d(x)$ does not hold whereas $\mathrm{ground}_d\bigl(h(y)\bigr)$ holds.
- $\mathrm{free}_d(v)$ holds but $\mathrm{free}_d\bigl(h(v)\bigr)$ does not hold.
- Both $\mathrm{ind}_d(w, x)$ and $\mathrm{ind}_d\bigl(f(w, y), f(x, y)\bigr)$ hold whereas $\mathrm{ind}_d(x, z)$ does not hold; note that, in the second case, the two arguments of the predicate do share y, but this does not affect the independence of the corresponding terms, because y is definitely ground in the abstract element d.
- Let $t = f(w, x, x, y, y, z)$; then $\mathrm{occ\_lin}_d(w, t)$ does not hold because $w \notin l$; $\mathrm{occ\_lin}_d(x, t)$ does not hold because x occurs more than once in t; $\mathrm{occ\_lin}_d(y, t)$ holds, even though y occurs twice in t, because y is definitely ground in d; $\mathrm{occ\_lin}_d(z, t)$ does not hold because both x and z occur in term t and, as observed in the point above, $\mathrm{ind}_d(x, z)$ does not hold.
- For the reasons given in the point above, $\mathrm{lin}_d(t)$ does not hold; in contrast, $\mathrm{lin}_d\bigl(f(y, y, z)\bigr)$ holds.
- $\mathrm{share\_with}_d(w) = \{w, z\}$ and $\mathrm{share\_with}_d(x) = \{x, z\}$; thus, both w and x may share one or more variables with z; since we observed that w and x are definitely independent in d, this means that the set of variables that w shares with z is disjoint from the set of variables that x shares with z.
- Let $t = f(w, z)$; then

$$\begin{aligned}\mathrm{cyclic}_z^t(sh) &= \overline{\mathrm{rel}}\bigl(\{w, z\}, sh\bigr) \cup \mathrm{rel}\bigl(\{w\}, sh\bigr)\\ &= \{v\} \cup \{wz\}\\ &= sh \setminus \{xz, z\}.\end{aligned}$$

  An intuitive explanation of the usefulness of this operator is deferred until after the introduction of the abstract mgu operator (see also Example 31).

We now introduce the abstract mgu operator, specifying how a single binding affects each component of the domain *SFL* in the context of a syntactic equality theory T.

Definition 28
(amgu_S.) The function $\mathrm{amgu}_S \colon SFL \times Bind \to SFL$ captures the effects of a binding on an element of *SFL*. Let $d = \langle sh, f, l\rangle \in SFL$ and $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Let also

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

where

$$sh_x \stackrel{\mathrm{def}}{=} \mathrm{rel}\bigl(\{x\}, sh\bigr), \qquad sh_t \stackrel{\mathrm{def}}{=} \mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr),$$

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

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

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

$$f' \stackrel{\mathrm{def}}{=} \begin{cases} f, & \text{if } \mathrm{free}_d(x) \land \mathrm{free}_d(t); \\ f \setminus S_x, & \text{if } \mathrm{free}_d(x); \\ f \setminus S_t, & \text{if } \mathrm{free}_d(t); \\ f \setminus (S_x \cup S_t), & \text{otherwise;} \end{cases}$$

$$l' \stackrel{\mathrm{def}}{=} \bigl(\mathit{VI} \setminus \mathrm{vars}(sh')\bigr) \cup f' \cup l'',$$

where

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

Then

$$\mathrm{amgu}_S\bigl(d, x \mapsto t\bigr) \stackrel{\mathrm{def}}{=} \begin{cases} \bot_S, & \text{if } d = \bot_S \lor \bigl(T = \mathcal{FT} \land x \in \mathrm{vars}(t)\bigr); \\ \langle sh', f', l' \rangle & \text{otherwise.} \end{cases}$$

The next result states that the abstract mgu operator is a correct approximation of the concrete one.

Theorem 29
Let $d \in \mathit{SFL}$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Then, for all $\sigma \in \gamma_S(d)$ and $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$ in the syntactic equality theory T, we have $\tau \in \gamma_S\bigl(\mathrm{amgu}_S(d, x \mapsto t)\bigr)$.

We now highlight the similarities and differences of the operator amgu_S with respect to the corresponding ones defined in the "classical" proposals for the integration of set-sharing with freeness and linearity, such as (Bruynooghe et al. 1994a; Bruynooghe et al. 1995; Hans and Winkler 1992; Langen 1990). Note that, when comparing our domain with the proposal in (Bruynooghe et al. 1994a), we deliberately ignore all those enhancements that depend on properties that cannot be represented in *SFL* (i.e., compoundness and explicit structural information).

- In the computation of the set-sharing component, the main difference can be observed in the second, third and fourth cases of the definition of sh'': here we omit one of the star-unions even when the terms x and t possibly share. In contrast, in (Bruynooghe et al. 1994a; Hans and Winkler 1992; Langen 1990) the corresponding star-union is avoided only when $\mathrm{ind}_d(x, t)$ holds. Note that when $\mathrm{ind}_d(x, t)$ holds in the second case of sh'', then we have $sh_{xt} = \varnothing$; thus, the whole computation for this case reduces to $sh'' = \mathrm{bin}(sh_x, sh_t)$, as was the case in the previous proposals.

- Another improvement on the set-sharing component can be observed in the definition of sh': the cyclic_x^t operator allows the set-sharing description to be further enhanced when dealing with *explicitly cyclic bindings*, i.e., when $x \in \mathrm{vars}(t)$. This is the rewording of a similar enhancement proposed in (Bagnara 1997) for the domain *Pos* in the context of groundness analysis. Its net effect is to recover some groundness and sharing dependencies that would have been unnecessarily lost when using the standard operators. When $x \notin \mathrm{vars}(t)$, we have $\mathrm{cyclic}_x^t(sh_- \cup sh'') = sh_- \cup sh''$.
- The computation of the freeness component f' is the same as specified in (Bruynooghe et al. 1994a; Hans and Winkler 1992), and is more precise than the one defined in (Langen 1990).
- The computation of the linearity component l' is the same as specified in (Bruynooghe et al. 1994a), and is more precise than those defined in (Hans and Winkler 1992; Langen 1990).

In the following examples we show that the improvements in the abstract computation of the sharing component allow, in particular cases, to derive better information than that obtainable by using the classical abstract unification operators.

Example 30
Let $VI = \{x, x_1, x_2, y, y_1, y_2, z\}$ and $\sigma \in RSubst$ such that

$$\sigma \stackrel{\mathrm{def}}{=} \bigl\{x \mapsto f(x_1, x_2, z), y \mapsto f(y_1, z, y_2)\bigr\}.$$

By Definition 23, we have $d \stackrel{\mathrm{def}}{=} \alpha_S\bigl(\{\sigma\}\bigr) = \langle sh, f, l\rangle$, where

$$sh = \{xx_1, xx_2, xyz, yy_1, yy_2\}, \qquad f = VI \setminus \{x, y\}, \qquad l = VI.$$

Consider the binding $(x \mapsto y) \in Bind$. In the concrete domain, we compute (a substitution equivalent to) $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = y\}\bigr)$, where

$$\tau = \bigl\{x \mapsto f(y_1, y_2, y_2), y \mapsto f(y_1, y_2, y_2), x_1 \mapsto y_1, x_2 \mapsto y_2, z \mapsto y_2\bigr\}.$$

Note that $\alpha_S\bigl(\{\tau\}\bigr) = \langle sh_\tau, f_\tau, l_\tau\rangle$, where $sh_\tau = \{xx_1yy_1, xx_2yy_2z\}$, so that the pairs of variables $P_x = \{x_1, x_2\}$ and $P_y = \{y_1, y_2\}$ keep their independence.

When evaluating the sharing component of $\mathrm{amgu}_S(d, x \mapsto y)$, using the notation of Definition 28, we have

$$sh_x = \{xx_1, xx_2, xyz\}, \qquad sh_t = \{xyz, yy_1, yy_2\},$$
$$sh_{xt} = \{xyz\}, \qquad sh_- = \varnothing.$$

Since both $\mathrm{lin}_d(x)$ and $\mathrm{lin}_d(y)$ hold, we apply the second case of the definition of sh'' so that

$$sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^\star) = \{xx_1, xx_1yz, xx_2, xx_2yz, xyz\},$$

$$\begin{aligned}
sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^\star) &= \{xyy_1z, xyy_2z, xyz, yy_1, yy_2\},\\
sh'' &= \mathrm{bin}\bigl(sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^\star), sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^\star)\bigr)\\
&= \{xx_1yy_1, xx_1yy_1z, xx_1yy_2, xx_1yy_2z, xx_1yz,\\
&\qquad xx_2yy_1, xx_2yy_1z, xx_2yy_2, xx_2yy_2z, xx_2yz,\\
&\qquad xyy_1z, xyy_2z, xyz\}.
\end{aligned}$$

Finally, as the binding is not cyclic, we obtain $sh' = sh''$. Thus amgu_S captures the fact that pairs P_x and P_y keep their independence.

In contrast, since $\mathrm{ind}_d(x, y)$ does not hold, all of the classical definitions of abstract unification would have required the star-closure of both sh_x and sh_t, resulting in an abstract element including, among the others, the sharing group $S = \{x, x_1, x_2, y, y_1, y_2\}$. Since $P_x \cup P_y \subset S$, this independence information would have been unnecessarily lost.

Similar examples can be devised for the third and fourth cases of the definition of sh'', where only one side of the binding is known to be linear. The next example shows the precision improvements arising from the use of the cyclic_x^t operator.

Example 31

Let $VI = \{x, x_1, x_2, y\}$ and $\sigma \stackrel{\mathrm{def}}{=} \bigl\{x \mapsto f(x_1, x_2)\bigr\}$. By Definition 23, we have $d \stackrel{\mathrm{def}}{=} \alpha_S\bigl(\{\sigma\}\bigr) = \langle sh, f, l\rangle$, where

$$sh = \{xx_1, xx_2, y\}, \qquad f = VI \setminus \{x\}, \qquad l = VI.$$

Let $t = f(x, y)$ and consider the cyclic binding $(x \mapsto t) \in \mathit{Bind}$. In the concrete domain, we compute (a substitution equivalent to) $\tau \in \mathrm{mgs}\bigl(\sigma \cup \{x = t\}\bigr)$, where

$$\tau = \bigl\{x \mapsto f(x_1, x_2), x_1 \mapsto f(x_1, x_2), y \mapsto x_2, \bigr\}.$$

Note that if we further instantiate τ by grounding y, then variables x, x_1 and x_2 would become ground too. Formally we have $\alpha_S\bigl(\{\tau\}\bigr) = \langle sh_\tau, f_\tau, l_\tau\rangle$, where $sh_\tau = \{xx_1x_2y\}$. Thus, as observed above, y covers x, x_1 and x_2. When abstractly evaluating the binding, we compute

$$\begin{aligned}
sh_x &= \{xx_1, xx_2\}, & sh_t &= \{xx_1, xx_2, y\},\\
sh_{xt} &= sh_x, & sh_- &= \varnothing.
\end{aligned}$$

Since both $\mathrm{lin}_d(x)$ and $\mathrm{lin}_d(t)$ hold, we apply the second case of the definition of sh'', so that

$$\begin{aligned}
sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^\star) &= sh_x^\star = \{xx_1, xx_1x_2, xx_2\},\\
sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^\star) &= \{xx_1, xx_1x_2, xx_1x_2y, xx_1y, xx_2, xx_2y, y\},\\
sh'' &= \mathrm{bin}\bigl(sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^\star), sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^\star)\bigr)\\
&= \{xx_1, xx_1x_2, xx_1x_2y, xx_1y, xx_2, xx_2y\}.
\end{aligned}$$

Thus, as $x \in \mathrm{vars}(t)$, we obtain

$$\begin{aligned}
sh' &= \mathrm{cyclic}_x^t(sh_- \cup sh'')\\
&= \overline{\mathrm{rel}}\bigl(\{x\} \cup \mathrm{vars}(t), sh''\bigr) \cup \mathrm{rel}\bigl(\mathrm{vars}(t) \setminus \{x\}, sh''\bigr)
\end{aligned}$$

$$
\begin{aligned}
&= \varnothing \cup \operatorname{rel}\bigl(\{y\}, sh''\bigr) \\
&= \{xx_1x_2y, xx_1y, xx_2y\}.
\end{aligned}
$$

Note that, in the element $sh_- \cup sh'' = sh''$ (which is the abstract element that would have been computed when not exploiting the cyclic_x^t operator) variable y covers none of variables x, x_1 and x_2. Thus, by applying the cyclic_x^t operator, this covering information is restored.

The full abstract unification operator aunify_S, capturing the effect of a sequence of bindings on an abstract element, can now be specified by a straightforward inductive definition using the operator amgu_S.

Definition 32
(aunify_S.) The operator $\mathrm{aunify}_S \colon \mathit{SFL} \times \mathit{Bind}^* \to \mathit{SFL}$ is defined, for each $d \in \mathit{SFL}$ and each sequence of bindings $bs \in \mathit{Bind}^*$, by

$$
\mathrm{aunify}_S(d, bs) \stackrel{\mathrm{def}}{=} \begin{cases} d, & \text{if } bs = \epsilon; \\ \mathrm{aunify}_S\bigl(\mathrm{amgu}_S(d, x \mapsto t), bs'\bigr), & \text{if } bs = (x \mapsto t) \,.\, bs'. \end{cases}
$$

Note that the second argument of aunify_S is a *sequence* of bindings (i.e., it is not a substitution, which is a *set* of bindings), because amgu_S is neither commutative nor idempotent, so that the multiplicity and the actual order of application of the bindings can influence the overall result of the abstract computation. The correctness of the aunify_S operator is simply inherited from the correctness of the underlying amgu_S operator. In particular, any reordering of the bindings in the sequence bs still results in a correct implementation of aunify_S.

The 'merge-over-all-path' operator on the domain *SFL* is provided by alub_S and is correct by definition. Finally, we define the abstract existential quantification operator for the domain *SFL*, whose correctness does not pose any problem.

Definition 33
($\mathrm{aexists}_S$.) The function $\mathrm{aexists}_S \colon \mathit{SFL} \times \wp_{\mathrm{f}}(\mathit{VI}) \to \mathit{SFL}$ provides the *abstract existential quantification* of an element with respect to a subset of the variables of interest. For each $d \stackrel{\mathrm{def}}{=} \langle sh, f, l\rangle \in \mathit{SFL}$ and $V \subseteq \mathit{VI}$,

$$
\mathrm{aexists}_S\bigl(\langle sh, f, l\rangle, V\bigr) \stackrel{\mathrm{def}}{=} \bigl\langle \mathrm{aexists}(sh, V), f \cup V, l \cup V \bigr\rangle.
$$

The intuition behind the definition of the abstract operator $\mathrm{aexists}_S$ is the following. As explained in Section 2, any substitution $\sigma \in \mathit{RSubst}$ can be interpreted, under the given equality theory T, as a first-order logical formula; thus, for each set of variables V, it is possible to consider the (concrete) existential quantification $\exists V \,.\, \sigma$. The goal of the abstract operator $\mathrm{aexists}_S$ is to provide a correct approximation of such a quantification starting from any correct approximation for σ.

Example 34
Let $\mathit{VI} = \{x, y, z\}$ and $\sigma = \{x \mapsto f(v_1, v_2), y \mapsto g(v_2, v_3), z \mapsto f(v_1, v_1)\}$, so that, by Definition 23,

$$
d = \alpha_S\bigl(\{\sigma\}\bigr) = \bigl\langle \{xy, xz, y\}, \varnothing, \{x, y\} \bigr\rangle.
$$

Let $V = \{y, z\}$ and consider the concrete element corresponding to the logical formula $\exists V \mathrel{.} \sigma$. Note that $T \vdash \forall(\tau \leftrightarrow \exists V \mathrel{.} \sigma)$, where $\tau = \{x \mapsto f(v_1, v_2)\}$. By applying Definition 33, we obtain

$$\mathrm{aexists}_S(d, V) = \bigl\langle \{x, y, z\}, \{y, z\}, \{x, y, z\} \bigr\rangle = \alpha_S\bigl(\{\tau\}\bigr).$$

It is worth stressing that such an operator does not affect the set VI of the variables of interest. In particular, the abstract element $\mathrm{aexists}_S(d, V)$ still has to provide correct information about variables y and z. Intuitively, since all the occurrences of y and z in $\exists V \mathrel{.} \sigma$ are bound by the existential quantifier, the two variables of interest are un-aliased, free and linear.

Note that an abstract *projection* operator, i.e., an operator that actually modifies the set of variables of interest, is easily specified by composing the operator $\mathrm{aexists}_S$ with an operator that simply removes, from all the components of *SFL and* from the set of variables of interest VI, those variables that have to be projected out.

4 A Formal Comparison Between *SFL* and ASub

As we have already observed, Example 30 shows that the abstract domain *SFL*, when equipped with the abstract mgu operator introduced in Section 3.2, can yield results that are strictly more precise than all the classical combinations of set-sharing with freeness and linearity information. In this section we show that the same example has another interesting, unexpected consequence, since it can be used to formally prove that all the classical combinations of set-sharing with freeness and linearity, including those presented in (Bagnara et al. 2000; Bruynooghe et al. 1994a; Hans and Winkler 1992; Langen 1990), are not *uniformly* more precise than the abstract domain ASub (Søndergaard 1986), which is based on pair-sharing.

To formalize the above observation, we now introduce the ASub domain and the corresponding abstract semantics operators as specified in (Codish et al. 1991). The elements of the abstract domain ASub have two components: the first one is a set of variables that are known to be definitely ground; the second one encodes both possible pair-sharing and possible non-linearity into a single relation defined on the set of variables. Intuitively, when $x \neq y$ and $(x, y) \in VI^2$ occurs in the second component, then x and y may share a variable; when $(x, x) \in VI^2$ occurs in the second component, then x may be non-linear. The second component always encodes a symmetric relation; thus, for notational convenience and without any loss of generality (King 2000), we will represent each pair (x, y) in such a relation as the sharing group $S = \{x, y\}$, which will have cardinality 1 or 2 depending on whether $x = y$ or not, respectively.

Definition 35
(The domain $\mathsf{ASub}_\bot$.) The abstract domain $\mathsf{ASub}_\bot$ is defined as $\mathsf{ASub}_\bot \stackrel{\mathrm{def}}{=} \{\bot_{\mathsf{ASub}}\} \cup \mathsf{ASub}$, where

$$\mathsf{ASub} \stackrel{\mathrm{def}}{=} \left\{ \langle G, R \rangle \in \wp(VI) \times SH \;\middle|\; \begin{array}{l} G \cap \mathrm{vars}(R) = \varnothing, \\ \forall S \in R : 1 \leq \# S \leq 2 \end{array} \right\}.$$

For $i \in \{1, 2\}$, let $\kappa_i = \langle G_i, R_i \rangle \in \mathsf{ASub}$. Then

$$\kappa_1 \preceq_{\mathsf{ASub}} \kappa_2 \quad \stackrel{\text{def}}{\iff} \quad G_1 \supseteq G_2 \wedge R_1 \subseteq R_2.$$

The partial order $\preceq_{\mathsf{ASub}}$ is extended on $\mathsf{ASub}_\perp$ by letting $\perp_{\mathsf{ASub}}$ be the bottom element.

Let $u, v \in \mathit{VI}$ and $\kappa = \langle G, R \rangle \in \mathsf{ASub}$. Then $u \stackrel{\kappa}{\longleftrightarrow} v$ is a shorthand for the condition $\{u, v\} \in R$, whereas $u \stackrel{\kappa}{\Longleftrightarrow} v$ is a shorthand for $u = v \vee \{u, v\} \in R$.

It is well-known that the domain $\mathsf{ASub}_\perp$ can be obtained by a further abstraction of any domain such as *SFL* that is based on set-sharing and enhanced with linearity information. The following definition formalizes this abstraction.

Definition 36

($\alpha_{\mathsf{ASub}} \colon \mathit{SFL} \to \mathsf{ASub}_\perp$.) Let $d = \langle sh, f, l \rangle \in \mathit{SFL}$. Then

$$\alpha_{\mathsf{ASub}}(d) \stackrel{\text{def}}{=} \begin{cases} \perp_{\mathsf{ASub}}, & \text{if } d = \perp_S; \\ \langle G, R \rangle, & \text{otherwise;} \end{cases}$$

where

$$\begin{aligned} G &\stackrel{\text{def}}{=} \bigl\{\, x \in \mathit{VI} \bigm| x \notin \operatorname{vars}(sh) \,\bigr\}, \\ R &\stackrel{\text{def}}{=} \bigl\{\, \{x\} \subseteq \mathit{VI} \bigm| x \in \operatorname{vars}(sh) \wedge x \notin l \,\bigr\} \\ &\qquad \cup \bigl\{\, \{x, y\} \subseteq \mathit{VI} \bigm| x \neq y \wedge \exists S \in sh \mathrel{.} \{x, y\} \subseteq S \,\bigr\}. \end{aligned}$$

The definition of abstract unification in (Codish et al. 1991) is based on a few auxiliary operators. The first of these introduces the concept of abstract multiplicity for a term under a given abstract substitution, therefore modeling the notion of definite groundness and definite linearity.

Definition 37

(Abstract multiplicity.) Let $\kappa = \langle G, R \rangle \in \mathsf{ASub}$ and let $t \in \mathit{HTerms}$ be a term such that $\operatorname{vars}(t) \subseteq \mathit{VI}$. We say that $y \in \operatorname{vars}(t)$ *occurs linearly (in t) in κ* if and only if $\mathrm{occ\_lin}_\kappa \colon \mathit{VI} \times \mathit{HTerms} \to \mathit{Bool}$ holds for (y, t), where

$$\mathrm{occ\_lin}_\kappa(y, t) \stackrel{\text{def}}{=} y \in G \vee \bigl(\mathrm{occ\_lin}(y, t) \wedge \forall z \in \operatorname{vars}(t) : \{y, z\} \notin R\bigr).$$

We say that t *has abstract multiplicity m in κ* if and only if $\chi_\kappa(t) = m$, where $\chi_\kappa \colon \mathit{HTerms} \to \{0, 1, 2\}$ is defined as follows

$$\chi_\kappa(t) \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } \operatorname{vars}(t) \subseteq G; \\ 1, & \text{if } \forall y \in \operatorname{vars}(t) : \mathrm{occ\_lin}_\kappa(y, t); \\ 2, & \text{otherwise.} \end{cases}$$

For any binding $x \mapsto t$, the function $\chi_\kappa \colon \mathit{Bind} \to \{0\} \cup \{1, 2\}^2$ is defined as follows

$$\chi_\kappa(x \mapsto t) \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } \chi_\kappa(x) = 0 \text{ or } \chi_\kappa(t) = 0; \\ \bigl(\chi_\kappa(x), \chi_\kappa(t)\bigr), & \text{otherwise;} \end{cases}$$

It is worth noting that, modulo a few insignificant differences in notation, the multiplicity operator χ_κ defined above corresponds to the abstract multiplicity operator $\chi^{\mathcal{A}}$, which was introduced in (Codish et al. 1991, Definition 3.4) and provided with an executable specification in (King 2000, Definition 4.3). Similarly, the next definition corresponds to (Codish et al. 1991, Definition 4.3).

Definition 38

(Sharing caused by an abstract equation.) For each $\kappa \in \mathsf{ASub}$ and $(x \mapsto t) \in \mathit{Bind}$, where $V_x = \{x\}$ and $V_t = \mathrm{vars}(t)$ are such that $V_x \cup V_t \subseteq \mathit{VI}$, the function $\mathrm{soln}\colon \mathsf{ASub} \times \mathit{Bind} \to \mathsf{ASub}$ is defined as follows

$$\mathrm{soln}(\kappa, x \mapsto t) \stackrel{\mathrm{def}}{=} \begin{cases} \langle V_x \cup V_t, \varnothing \rangle, & \text{if } \chi_\kappa(x \mapsto t) = 0; \\ \bigl\langle \varnothing, \mathrm{bin}(V_x, V_t) \bigr\rangle, & \text{if } \chi_\kappa(x \mapsto t) = (1,1); \\ \bigl\langle \varnothing, \mathrm{bin}(V_x, V_x \cup V_t) \bigr\rangle, & \text{if } \chi_\kappa(x \mapsto t) = (1,2); \\ \bigl\langle \varnothing, \mathrm{bin}(V_x \cup V_t, V_t) \bigr\rangle, & \text{if } \chi_\kappa(x \mapsto t) = (2,1); \\ \bigl\langle \varnothing, \mathrm{bin}(V_x \cup V_t, V_x \cup V_t) \bigr\rangle, & \text{if } \chi_\kappa(x \mapsto t) = (2,2); \end{cases}$$

where the function $\mathrm{bin}\colon \wp(\mathit{VI})^2 \to \mathit{SH}$, for each $V, W \subseteq \mathit{VI}$, is defined as follows

$$\mathrm{bin}(V, W) \stackrel{\mathrm{def}}{=} \bigl\{\, \{v, w\} \subseteq \mathit{VI} \bigm| v \in V, w \in W \,\bigr\}.$$

The next definition corresponds to (Codish et al. 1991, Definition 4.5).

Definition 39

(Abstract composition.) Let $\kappa, \kappa' \in \mathsf{ASub}$, where $\kappa = \langle G, R \rangle$ and $\kappa' = \langle G', R' \rangle$. Then $\kappa \circ \kappa' \stackrel{\mathrm{def}}{=} \langle G'', R'' \rangle$, where

$$\begin{aligned} G'' &\stackrel{\mathrm{def}}{=} G \cup G', \\ R'' &\stackrel{\mathrm{def}}{=} \left\{ \{u, v\} \in \mathit{SH} \;\middle|\; \begin{array}{l} \{u, v\} \cap G'' = \varnothing, \\ \bigl(u \stackrel{\kappa}{\longleftrightarrow} v\bigr) \vee \bigl(\exists x, y \,.\, u \stackrel{\kappa}{\Longleftrightarrow} x \stackrel{\kappa'}{\longleftrightarrow} y \stackrel{\kappa}{\Longleftrightarrow} v\bigr) \end{array} \right\}. \end{aligned}$$

We are now ready to define the abstract mgu operator for the domain $\mathsf{ASub}_\bot$. This operator can be viewed as a specialization of (Codish et al. 1991, Definition 4.6) for the case when we have to abstract a single binding.

Definition 40

(Abstract mgu **for** $\mathsf{ASub}_\bot$**.)** Let $\kappa \in \mathsf{ASub}_\bot$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Then

$$\mathrm{amgu}_{\mathsf{ASub}}(\kappa, x \mapsto t) \stackrel{\mathrm{def}}{=} \begin{cases} \bot_{\mathsf{ASub}}, & \text{if } \kappa = \bot_{\mathsf{ASub}}; \\ \kappa \circ \mathrm{soln}(\kappa, x \mapsto t), & \text{otherwise;} \end{cases}$$

By repeating the abstract computation of Example 30 on the domain ASub, we provide a formal proof that all the classical approaches based on set-sharing are not uniformly more precise than the pair-sharing domain ASub.

Example 41
Consider the substitutions $\sigma, \tau \in RSubst$ and the abstract element $d \in SFL$ as introduced in Example 30.

By Definition 36, we obtain $\kappa = \alpha_{\mathsf{ASub}}(d) = \langle \varnothing, R \rangle$, where

$$R = \{xx_1, xx_2, xy, xz, yy_1, yy_2, yz\},$$

When abstractly evaluating the binding $x \mapsto y$ according to Definition 40, we compute the following:

$$\begin{aligned} \chi_\kappa(x \mapsto y) &= (1, 1), \\ \mathrm{soln}(\kappa, x \mapsto y) &= \bigl\langle \varnothing, \{xy\} \bigr\rangle, \\ \mathrm{amgu}_{\mathsf{ASub}}(\kappa, x \mapsto y) &= \kappa \circ \mathrm{soln}(\kappa, x \mapsto y) = \langle \varnothing, R'' \rangle, \end{aligned}$$

where

$$R'' = R \cup \{x, xy_1, xy_2, x_1y, x_1y_1, x_1y_2, x_1z, x_2y, x_2y_1, x_2y_2, x_2z, y, y_1z, y_2z, z\}.$$

Note that $\{x_1, x_2\} \notin R''$ and $\{y_1, y_2\} \notin R''$, so that these pairs of variables keep their independence. In contrast, as observed in Example 30, the operators in (Bagnara et al. 2000; Bruynooghe et al. 1994a; Hans and Winkler 1992; Langen 1990) will fail to preserve the independence of these pairs.

We now show that the abstract domain *SFL*, when equipped with the operators introduced in Section 3.2, is uniformly more precise than the domain ASub. In particular, the following theorem states that the abstract operator amgu_S of Definition 28 is uniformly more precise than the abstract operator $\mathrm{amgu}_{\mathsf{ASub}}$.

Theorem 42
Let $d \in SFL$ and $\kappa \in \mathsf{ASub}_\perp$ be such that $\alpha_{\mathsf{ASub}}(d) \preceq_{\mathsf{ASub}} \kappa$. Let also $(x \mapsto t) \in Bind$, where $\{x\} \cup \mathrm{vars}(t) \subseteq VI$. Then

$$\alpha_{\mathsf{ASub}}\bigl(\mathrm{amgu}_S(d, x \mapsto t)\bigr) \preceq_{\mathsf{ASub}} \mathrm{amgu}_{\mathsf{ASub}}(\kappa, x \mapsto t).$$

Similar results can be stated for the other abstract operators, such as the abstract existential quantification $\mathrm{aexists}_S$ and the merge-over-all-path operator alub_S. It is worth stressing that, when sequences of bindings come into play, the specification provided in (Codish et al. 1991, Definition 4.7) requires that the *grounding* bindings (i.e., those bindings such that $\chi_\kappa(x \mapsto t) = 0$) are evaluated before the non-grounding ones. Clearly, if we want to lift the result of Theorem 42 so that it also applies to the operator aunify_S, the same evaluation strategy has to be adopted when computing on the domain *SFL*; this improvement is well-known (Langen 1990, pp. 66-67) and already exploited in most implementations of sharing analysis (Bagnara et al. 2000).

5 SFL_2: Eliminating Redundancies

As done in (Bagnara et al. 2002; Zaffanella et al. 2002) for the plain set-sharing domain *SH*, even when considering the richer domain *SFL* it is natural to question whether it contains redundancies with respect to the computation of the observable properties.

It is worth stressing that the results presented in (Bagnara et al. 2002) and (Zaffanella et al. 2002) cannot be simply inherited by the new domain. The concept of "redundancy" depends on both the starting domain and the given observables: in the *SFL* domain both of these have changed. First of all, as can be seen by looking at the definition of amgu_S, freeness and linearity positively interact in the computation of sharing information: *a priori* it is an open issue whether or not the "redundant" sharing groups can play a role in such an interaction. Secondly, since freeness and linearity information can be themselves usefully exploited in a number of applications of static analysis (e.g., in the optimized implementation of concrete unification or in occurs-check reduction), these properties have to be included in the observables.

We will now show that the domain *SFL* can be simplified by applying the same notion of redundancy as identified in (Bagnara et al. 2002). Namely, in the definition of *SFL* it is possible to replace the set-sharing component *SH* by *PSD* without affecting the precision on groundness, independence, freeness and linearity. In order to prove such a claim, we now formalize the new observable properties.

Definition 43
(The observables of *SFL*.) The (overloaded) *groundness* and *independence* observables $\rho_{Con}, \rho_{PS} \in \mathrm{uco}(\mathit{SFL})$ are defined, for each $\langle sh, f, l\rangle \in \mathit{SFL}$, by

$$\rho_{Con}\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\mathrm{def}}{=} \bigl\langle \rho_{Con}(sh), \varnothing, \varnothing \bigr\rangle,$$
$$\rho_{PS}\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\mathrm{def}}{=} \bigl\langle \rho_{PS}(sh), \varnothing, \varnothing \bigr\rangle;$$

the *freeness* and *linearity* observables $\rho_F, \rho_L \in \mathrm{uco}(\mathit{SFL})$ are defined, for each $\langle sh, f, l\rangle \in \mathit{SFL}$, by

$$\rho_F\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\mathrm{def}}{=} \langle \mathit{SG}, f, \varnothing\rangle,$$
$$\rho_L\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\mathrm{def}}{=} \langle \mathit{SG}, \varnothing, l\rangle.$$

The overloading of ρ_{PSD} working on the domain *SFL* is the straightforward extension of the corresponding operator on *SH*: in particular, the freeness and linearity components are left untouched.

Definition 44
(Non-redundant *SFL*.) For each $\langle sh, f, l\rangle \in \mathit{SFL}$, the operator $\rho_{PSD} \in \mathrm{uco}(\mathit{SFL})$ is defined by

$$\rho_{PSD}\bigl(\langle sh, f, l\rangle\bigr) \stackrel{\mathrm{def}}{=} \bigl\langle \rho_{PSD}(sh), f, l \bigr\rangle.$$

This operator induces the lattice $\mathit{SFL}_2 \stackrel{\mathrm{def}}{=} \rho_{PSD}(\mathit{SFL})$.

As proved in (Zaffanella et al. 2002), we have that $\rho_{PSD} \sqsubseteq (\rho_{Con} \sqcap \rho_{PS})$; by the above definitions, it is also clear that $\rho_{PSD} \sqsubseteq (\rho_F \sqcap \rho_L)$; thus, ρ_{PSD} is more precise than the reduced product $(\rho_{Con} \sqcap \rho_{PS} \sqcap \rho_F \sqcap \rho_L)$. Informally, this means that the domain SFL_2 is able to *represent* all of our observable properties without precision losses.

The next theorem shows that $\rho_{\scriptscriptstyle PSD}$ is a congruence with respect to the aunify_S, alub_S and $\mathrm{aexists}_S$ operators. This means that the domain SFL_2 is able to *propagate* the information on the observables as precisely as *SFL*, therefore providing a completeness result.

Theorem 45
Let $d_1, d_2 \in \mathit{SFL}$ be such that $\rho_{\scriptscriptstyle PSD}(d_1) = \rho_{\scriptscriptstyle PSD}(d_2)$. Then, for each sequence of bindings $bs \in \mathit{Bind}^*$, for each $d' \in \mathit{SFL}$ and $V \in \wp(\mathit{VI})$,

$$\begin{aligned}
\rho_{\scriptscriptstyle PSD}\bigl(\mathrm{aunify}_S(d_1, bs)\bigr) &= \rho_{\scriptscriptstyle PSD}\bigl(\mathrm{aunify}_S(d_2, bs)\bigr),\\
\rho_{\scriptscriptstyle PSD}\bigl(\mathrm{alub}_S(d_1, d')\bigr) &= \rho_{\scriptscriptstyle PSD}\bigl(\mathrm{alub}_S(d_2, d')\bigr),\\
\rho_{\scriptscriptstyle PSD}\bigl(\mathrm{aexists}_S(d_1, V)\bigr) &= \rho_{\scriptscriptstyle PSD}\bigl(\mathrm{aexists}_S(d_2, V)\bigr).
\end{aligned}$$

Finally, by providing the minimality result, we show that the domain SFL_2 is indeed the generalized quotient (Cortesi et al. 1998; Giacobazzi et al. 1998) of *SFL* with respect to the reduced product $(\rho_{\scriptscriptstyle Con} \sqcap \rho_{\scriptscriptstyle PS} \sqcap \rho_{\scriptscriptstyle F} \sqcap \rho_{\scriptscriptstyle L})$.

Theorem 46
For each $i \in \{1, 2\}$, let $d_i = \langle sh_i, f_i, l_i \rangle \in \mathit{SFL}$ be such that $\rho_{\scriptscriptstyle PSD}(d_1) \neq \rho_{\scriptscriptstyle PSD}(d_2)$. Then there exist a sequence of bindings $bs \in \mathit{Bind}^*$ and an observable property $\rho \in \{\rho_{\scriptscriptstyle Con}, \rho_{\scriptscriptstyle PS}, \rho_{\scriptscriptstyle F}, \rho_{\scriptscriptstyle L}\}$ such that

$$\rho\bigl(\mathrm{aunify}_S(d_1, bs)\bigr) \neq \rho\bigl(\mathrm{aunify}_S(d_2, bs)\bigr).$$

As far as the implementation is concerned, the results proved in (Bagnara et al. 2002) for the domain *PSD* can also be applied to SFL_2. In particular, in the definition of amgu_S every occurrence of the star-union operator can be safely replaced by the self-bin-union operator. As a consequence, it is possible to provide an implementation where the time complexity of the amgu_S operator is bounded by a polynomial in the number of sharing groups of the set-sharing component.

The following result provides another optimization that can be applied when both terms x and t are definitely linear, but none of them is definitely free (i.e., when we compute sh'' by the second case stated in Definition 28).

Theorem 47
Let $sh \in \mathit{SH}$ and $(x \mapsto t) \in \mathit{Bind}$, where $\{x\} \cup \mathrm{vars}(t) \subseteq \mathit{VI}$. Let $sh_- \stackrel{\mathrm{def}}{=} \overline{\mathrm{rel}}\bigl(\{x\} \cup \mathrm{vars}(t), sh\bigr)$, $sh_x \stackrel{\mathrm{def}}{=} \mathrm{rel}\bigl(\{x\}, sh\bigr)$, $sh_t \stackrel{\mathrm{def}}{=} \mathrm{rel}\bigl(\mathrm{vars}(t), sh\bigr)$, $sh_{xt} \stackrel{\mathrm{def}}{=} sh_x \cap sh_t$, $sh_W \stackrel{\mathrm{def}}{=} \mathrm{rel}(W, sh)$, where $W = \mathrm{vars}(t) \setminus \{x\}$, and

$$sh^{\diamond} \stackrel{\mathrm{def}}{=} \mathrm{bin}\bigl(sh_x \cup \mathrm{bin}(sh_x, sh_{xt}^{\star}), sh_t \cup \mathrm{bin}(sh_t, sh_{xt}^{\star})\bigr).$$

Then it holds

$$\rho_{\scriptscriptstyle PSD}\bigl(\mathrm{cyclic}_x^t(sh_- \cup sh^{\diamond})\bigr) = \begin{cases} \rho_{\scriptscriptstyle PSD}\bigl(sh_- \cup \mathrm{bin}(sh_x, sh_t)\bigr), & \text{if } x \notin \mathrm{vars}(t);\\ \rho_{\scriptscriptstyle PSD}\bigl(sh_- \cup \mathrm{bin}(sh_x^2, sh_W)\bigr), & \text{otherwise.}\end{cases}$$

Therefore, even when terms x and t possibly share (i.e., when $sh_{xt} \neq \varnothing$), by using SFL_2 we can avoid the expensive computation of at least one of the two inner binary unions in the expression for $sh^{\diamond}$.

6 Experimental Evaluation

Example 30 shows that an analysis based on the new abstract unification operator can be strictly more precise than one based on the classical proposal. However, that example is artificial and leaves open the question as to whether or not such a phenomenon actually happens during the analysis of real programs and, if so, how often. This was the motivation for the experimental evaluation we describe in this section. We consider the abstract domain $Pos \times SFL_2$ (Bagnara et al. 2001), where the non-redundant version SFL_2 of the domain SFL is further combined, as described in (Bagnara et al. 2001, Section 4), with the definite groundness information computed by Pos and compare the results using the (classical) abstract unification operator of (Bagnara et al. 2001, Definition 4) with the (new) operator amgu_S given in Definition 28. Taking this as a starting point, we experimentally evaluate eight variants of the analysis arising from all possible combinations of the following options:

1. the analysis can be goal independent or goal dependent;
2. the set-sharing component may or may not have widening enabled (Zaffanella et al. 1999);
3. the abstract domain may or may not be upgraded with structural information using the Pattern($\cdot$) operator (see (Bagnara et al. 2000) and (Bagnara et al. 2001, Section 5)).

The experiments have been conducted using the China analyzer (Bagnara 1997) on a GNU/Linux PC system. China is a data-flow analyzer for (constraint) logic programs performing bottom-up analysis and deriving information on both call-patterns and success-patterns by means of program transformations and optimized fixpoint computation techniques. An abstract description is computed for the call- and success-patterns for each predicate defined in the program. The benchmark suite, which is composed of 372 logic programs of various sizes and complexity, can be considered representative.

The precision results for the goal independent comparisons are summarized in Table 1. For each benchmark, precision is measured by counting the number of independent pairs as well as the numbers of definitely ground, free and linear variables detected. For each variant of the analysis, these numbers are then compared by computing the relative precision improvements and expressing them using percentages. The benchmark suite is then partitioned into several precision equivalence classes and the cardinalities of these classes are shown in Table 1. For example, when considering a goal independent analysis without structural information and without widenings, the value 5 found at the intersection of the row labeled '$0 < p \leq 2$' with the column labeled 'I' should be read: "for five benchmarks there has been a (positive) increase in the number of independent pairs of variables which is less than or equal to two percent." Note that we only report on independence and linearity (in the columns labeled 'I' and 'L', respectively), because no differences have been observed for groundness and freeness. The precision class labeled 'unknown' identifies those benchmarks for which the analyses timed-out (the time-out threshold was

Goal Independent	Without Widening				With Widening			
	w/o SI		with SI		w/o SI		with SI	
Prec. class	I	L	I	L	I	L	I	L
$5 < p \leq 10$	—	2	—	2	—	2	—	2
$2 < p \leq 5$	—	—	—	—	—	—	—	1
$0 < p \leq 2$	5	5	9	6	6	6	12	8
same precision	357	355	337	338	366	364	360	361
unknown	10	10	26	26	—	—	—	—

Table 1. *Classical* $Pos \times SFL_2$ *versus enhanced one: precision.*

fixed at 600 seconds). Hence, for goal independent analyses, a precision improvement affects from 1.6% to 3% of the benchmarks, depending on the considered variant.

When considering the goal dependent analyses, we obtain a single, small improvement, so that no comparison tables are included here: the improvement, affecting linearity information, can be observed when the abstract domain includes structural information.

With respect to differences in the efficiency, the introduction of the new abstract unification operator has no significant effect on the computation time: small differences (usually improvements) are observed on as many as 6% of the benchmarks for the goal independent analysis without structural information and without widenings; other combinations register even less differences.

We note that it is not surprising that the precision and efficiency improvements occur very rarely since the abstract unification operators behave the same except under very specific conditions: the two terms being unified must not only be definitely linear, but also possibly non-free and share a variable.

7 Related Work

Sharing information has been shown to be important for finite-tree analysis (Bagnara et al. 2001; Bagnara et al. 2001). This aims at identifying those program variables that, at a particular program point, cannot be bound to an infinite rational tree (in other words, they are necessarily bound to acyclic terms). This novel analysis is irrelevant for those logic languages computing over a domain of finite trees, while having several applications for those (constraint) logic languages that are explicitly designed to compute over a domain including rational trees, such as Prolog II and its successors (Colmerauer 1982; Colmerauer 1990), SICStus Prolog (Swedish Institute of Computer Science, Programming Systems Group 1995), and Oz (Smolka and Treinen 1994). The analysis specified in (Bagnara et al. 2001) is based on a parametric abstract domain $H \times P$, where the H component (the Herbrand component) is a set of variables that are known to be bound to finite terms, while the parametric component P can be any domain capturing aliasing, groundness, freeness and linearity information that is useful to compute finite-tree information. An obvious choice for such a parameter is the domain combination

SFL. It is worth noting that, in (Bagnara et al. 2001), the correctness of the finite-tree analysis is proved by *assuming* the correctness of the underlying analysis on the parameter P. Thus, thanks to the results shown in this paper, the proof for the domain $H \times \mathit{SFL}$ can now be considered complete.

Codish et al. (Codish et al. 2000) describe an algebraic approach to the sharing analysis of logic programs that is based on *set logic programs*. A set logic program is a logic program in which the terms are sets of variables and standard unification is replaced by a suitable unification for sets, called *ACI1-unification* (unification in the presence of an associative, commutative, and idempotent equality theory with a unit element). The authors show that the domain of *set-substitutions*, with a few modifications, can be used as an abstract domain for sharing analysis. They also provide an isomorphism between this domain and the set-sharing domain *SH* of Jacobs and Langen. The approach using set logic programs is also generalized to include linearity information, by suitably annotating the set-substitutions, and the authors formally state the optimality of the corresponding abstract unification operator $\mathit{lin}\text{-}\mathit{mgu}_{\mathit{ACI1}}$ (Lemma A.10 in the Appendix of (Codish et al. 2000)). However, this operator is very similar to the classical combinations of set-sharing with linearity (Bruynooghe et al. 1994a; Hans and Winkler 1992; Langen 1990): in particular, the precision improvements arising from this enhancement are only exploited when the two terms being unified are definitely independent. As we have seen in this paper, such a choice results in a sub-optimal abstract unification operator, so that the optimality result cannot hold. By looking at the proof of Lemma A.10 in (Codish et al. 2000), it can be seen that the case when the two terms possibly share a variable is dealt with by referring to an example:[5] this one is supposed to show that all the possible sharing groups can be generated. However, even our improved operator correctly characterizes the given example, so that the proof is wrong. It should be stressed that the amgu_S operator presented in this paper, though remarkably precise, is not meant to subsume all of the proposals for an improved sharing analysis that appeared in the recent literature (for a thorough experimental evaluation of many of these proposals, the reader is referred to (Bagnara et al. 2000; Zaffanella 2001)). In particular, it is not difficult to show that our operator is not the optimal approximation of concrete unification.

In a very recent paper (Howe and King 2003), J. Howe and A. King consider the domain *SFL* and propose three optimizations to improve both the precision and the efficiency of the (classical) abstract unification operator. The first optimization is based on the same observation we have made in this paper, namely that the independence check between the two terms being unified is not necessary for ensuring the correctness of the analysis. However, the proposed enhancement does not fully exploit this observation, so that the resulting operator is strictly less precise than our amgu_S operator (even when the operator cyclic_x^t does not come into play). In fact, the first optimization of (Howe and King 2003) is not uniformly more precise than the classical proposals. The following example illustrates this point.

[5] The proof refers to Example 8, which however has nothing to do with the possibility that the two terms share; we believe that Example 2 was intended.

Example 48

Let $VI = \{x, y, z_1, z_2, z_3\}$, $(x \mapsto y) \in \mathit{Bind}$ and $d \stackrel{\mathrm{def}}{=} \langle sh, \varnothing, VI\rangle$, where $sh = \{xz_1, xz_2, xz_3, yz_1, yz_2, yz_3\}$.

Since x and y are linear and independent, amgu_S as well as all the classical abstract unification operators will compute $d_1 = \big\langle sh_1, \varnothing, \{x, y\}\big\rangle$, where

$$sh_1 \stackrel{\mathrm{def}}{=} \mathrm{bin}(sh_x, sh_y) = \{xyz_1, xyz_1z_2, xyz_1z_3, xyz_2, xyz_2z_3, xyz_3\}.$$

In contrast, a computation based on (Howe and King 2003, Definition 3.2), results in the less precise abstract element $d_2 = \big\langle sh_2, \varnothing, \{x, y\}\big\rangle$, where

$$sh_2 \stackrel{\mathrm{def}}{=} \mathrm{bin}(sh_x^\star, sh_y) \cap \mathrm{bin}(sh_x, sh_y^\star) = sh_1 \cup \{xyz_1z_2z_3\}.$$

The second optimization shown in (Howe and King 2003) is based on the enhanced combination of set-sharing and freeness information, which was originally proposed in (Filé 1994). In particular, the authors propose a slightly different precision enhancement, less powerful as far as precision is concerned, which however seems to be amenable for an efficient implementation. The third optimization in (Howe and King 2003) exploits the combination of the domain *SFL* with the groundness domain *Pos*.

8 Conclusion

In this paper we have introduced the abstract domain *SFL*, combining the set-sharing domain *SH* with freeness and linearity information. While the carrier of *SFL* can be considered standard, we have provided the specification of a new abstract unification operator, showing examples where this operator achieves more precision than the classical proposals. The main contributions of this paper are the following:

- we have defined a precise abstraction function, mapping arbitrary substitutions in rational solved form into their *most precise* approximation on *SFL*;
- using this abstraction function, we have provided the mandatory proof of *correctness* for the new abstract unification operator, *for both finite-tree and rational-tree languages*;
- we have formally shown that the domain *SFL* is *uniformly* more precise than the domain ASub; we have also provided an example showing that all the classical approaches to the combinations of set-sharing with freeness and linearity fail to satisfy this property;
- we have shown that, in the definition of *SFL*, we can replace the set-sharing domain *SH* by its non-redundant version *PSD*. As a consequence, it is possible to implement an algorithm for abstract unification running in *polynomial time* and still obtain the same precision on all the considered observables, that is groundness, independence, freeness and linearity.

Acknowledgment

We recognize the hard work required to review technical papers such as this one and would like to express our real gratitude to the Journal referees for their critical reading and constructive suggestions for preparing this improved version.

References

Bagnara, R. 1997. Data-flow analysis for constraint logic-based languages. Ph.D. thesis, Dipartimento di Informatica, Università di Pisa, Pisa, Italy. Printed as Report TD-1/97.

Bagnara, R., Gori, R., Hill, P. M., and Zaffanella, E. 2001. Finite-tree analysis for constraint logic-based languages. In *Static Analysis: 8th International Symposium, SAS 2001*, P. Cousot, Ed. Lecture Notes in Computer Science, vol. 2126. Springer-Verlag, Berlin, Paris, France, 165–184.

Bagnara, R., Hill, P. M., and Zaffanella, E. 1997. Set-sharing is redundant for pair-sharing. In *Static Analysis: Proceedings of the 4th International Symposium*, P. Van Hentenryck, Ed. Lecture Notes in Computer Science, vol. 1302. Springer-Verlag, Berlin, Paris, France, 53–67.

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

Bagnara, R., Hill, P. M., and Zaffanella, E. 2002. Set-sharing is redundant for pair-sharing. *Theoretical Computer Science 277,* 1-2, 3–46.

Bagnara, R., Zaffanella, E., Gori, R., and Hill, P. M. 2001. Boolean functions for finite-tree dependencies. In *Proceedings of the 8th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR 2001)*, R. Nieuwenhuis and A. Voronkov, Eds. Lecture Notes in Artificial Intelligence, vol. 2250. Springer-Verlag, Berlin, Havana, Cuba, 579–594.

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

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

Bruynooghe, M. and Codish, M. 1993. Freeness, sharing, linearity and correctness — All at once. In *Static Analysis, Proceedings of the Third International Workshop*, P. Cousot, M. Falaschi, G. Filé, and A. Rauzy, Eds. Lecture Notes in Computer Science, vol. 724. Springer-Verlag, Berlin, Padova, Italy, 153–164. An extended version is available as Technical Report CW 179, Department of Computer Science, K.U. Leuven, September 1993.

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

Bruynooghe, M., Codish, M., and Mulkers, A. 1994b. A composite domain for freeness, sharing, and compoundness analysis of logic programs. Technical Report CW 196, Department of Computer Science, K.U. Leuven, Belgium. July.

Bruynooghe, M., Codish, M., and Mulkers, A. 1995. Abstracting unification: A key step in the design of logic program analyses. In *Computer Science Today: Recent Trends and Developments*, J. van Leeuwen, Ed. Lecture Notes in Computer Science, vol. 1000. Springer-Verlag, Berlin, 406–425.

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

Codish, M., Dams, D., Filé, G., and Bruynooghe, M. 1993. Freeness analysis for logic programs — and correctness? In *Logic Programming: Proceedings of the Tenth International Conference on Logic Programming*, D. S. Warren, Ed. MIT Press Series in Logic Programming. The MIT Press, Budapest, Hungary, 116–131. An extended version is available as Technical Report CW 161, Department of Computer Science, K.U. Leuven, December 1992.

Codish, M., Dams, D., Filé, G., and Bruynooghe, M. 1996. On the design of a correct freeness analysis for logic programs. *Journal of Logic Programming 28,* 3, 181–206.

Codish, M., Dams, D., and Yardeni, E. 1991. Derivation and safety of an abstract unification algorithm for groundness and aliasing analysis. See Furukawa (1991), 79–93.

Codish, M., Lagoon, V., and Bueno, F. 2000. An algebraic approach to sharing analysis of logic programs. *Journal of Logic Programming 42,* 2, 111–149.

Codish, M., Mulkers, A., Bruynooghe, M., Garcìa de la Banda, M., and Hermenegildo, M. 1993. Improving abstract interpretations by combining domains. In *Proceedings of the ACM SIGPLAN Symposium on Partial Evaluation and Semantics-Based Program Manipulation.* ACM Press, Copenhagen, Denmark, 194–205. Also available as Technical Report CW 162, Department of Computer Science, K.U. Leuven, December 1992.

Codish, M., Mulkers, A., Bruynooghe, M., Garcìa de la Banda, M., and Hermenegildo, M. 1995. Improving abstract interpretations by combining domains. *ACM Transactions on Programming Languages and Systems 17,* 1 (Jan.), 28–44.

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

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

Colmerauer, A. 1990. An introduction to Prolog-III. *Communications of the ACM 33,* 7, 69–90.

Cortesi, A. and Filé, G. 1999. Sharing is optimal. *Journal of Logic Programming 38,* 3, 371–386.

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

Cousot, P. and Cousot, R. 1977. 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.* ACM Press, New York, 238–252.

Cousot, P. and Cousot, R. 1979. Systematic design of program analysis frameworks. In *Proceedings of the Sixth Annual ACM Symposium on Principles of Programming Languages.* ACM Press, New York, 269–282.

FILÉ, G. 1994. Share $\times$ Free: Simple and correct. Tech. Rep. 15, Dipartimento di Matematica, Università di Padova. Dec.

FURUKAWA, K., Ed. 1991. *Logic Programming: Proceedings of the Eighth International Conference on Logic Programming*. MIT Press Series in Logic Programming. The MIT Press, Paris, France.

GIACOBAZZI, R., RANZATO, F., AND SCOZZARI, F. 1998. Complete abstract interpretations made constructive. In *Proceedings of 23rd International Symposium on Mathematical Foundations of Computer Science (MFCS'98)*, J. Gruska and J. Zlatuska, Eds. Lecture Notes in Computer Science, vol. 1450. Springer-Verlag, Berlin, 366–377.

HANS, W. AND WINKLER, S. 1992. Aliasing and groundness analysis of logic programs through abstract interpretation and its safety. Tech. Rep. 92–27, Technical University of Aachen (RWTH Aachen).

HILL, P. M., BAGNARA, R., AND ZAFFANELLA, E. 1998. The correctness of set-sharing. In *Static Analysis: Proceedings of the 5th International Symposium*, G. Levi, Ed. Lecture Notes in Computer Science, vol. 1503. Springer-Verlag, Berlin, Pisa, Italy, 99–114.

HILL, P. M., BAGNARA, R., AND ZAFFANELLA, E. 2002. Soundness, idempotence and commutativity of set-sharing. *Theory and Practice of Logic Programming 2,* 2, 155–201.

HILL, P. M., BAGNARA, R., AND ZAFFANELLA, E. 2003. On the analysis of set-sharing, freeness and linearity for finite and rational tree languages. Tech. Rep. 2003.08, School of Computing, University of Leeds. Available at `http://www.comp.leeds.ac.uk/research/pubs/reports.shtml`.

HOWE, J. M. AND KING, A. 2003. Three optimisations for sharing. *Theory and Practice of Logic Programming 3,* 2, 243–257.

INTRIGILA, B. AND ZILLI, M. V. 1996. A remark on infinite matching vs infinite unification. *Journal of Symbolic Computation 21,* 3, 2289–2292.

JACOBS, D. AND LANGEN, A. 1989. Accurate and efficient approximation of variable aliasing in logic programs. In *Logic Programming: Proceedings of the North American Conference*, E. L. Lusk and R. A. Overbeek, Eds. MIT Press Series in Logic Programming. The MIT Press, Cleveland, Ohio, USA, 154–165.

JAFFAR, J., LASSEZ, J.-L., AND MAHER, M. J. 1987. Prolog-II as an instance of the logic programming scheme. In *Formal Descriptions of Programming Concepts III*, M. Wirsing, Ed. North-Holland, Amsterdam, 275–299.

KEISU, T. 1994. Tree constraints. Ph.D. thesis, The Royal Institute of Technology, Stockholm, Sweden. Also available in the SICS Dissertation Series: SICS/D–16–SE.

KING, A. 1994. A synergistic analysis for sharing and groundness which traces linearity. In *Proceedings of the Fifth European Symposium on Programming*, D. Sannella, Ed. Lecture Notes in Computer Science, vol. 788. Springer-Verlag, Berlin, Edinburgh, UK, 363–378.

KING, A. 2000. Pair-sharing over rational trees. *Journal of Logic Programming 46,* 1–2, 139–155.

KING, A. AND SOPER, P. 1994. Depth-k sharing and freeness. In *Logic Programming: Proceedings of the Eleventh International Conference on Logic Programming*, P. Van Hentenryck, Ed. MIT Press Series in Logic Programming. The MIT Press, Santa Margherita Ligure, Italy, 553–568.

LANGEN, A. 1990. Advanced techniques for approximating variable aliasing in logic programs. Ph.D. thesis, Computer Science Department, University of Southern California. Printed as Report TR 91-05.

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

Muthukumar, K. and Hermenegildo, M. 1991. Combined determination of sharing and freeness of program variables through abstract interpretation. See Furukawa (1991), 49–63. An extended version appeared in (Muthukumar and Hermenegildo 1992).

Muthukumar, K. and Hermenegildo, M. 1992. Compile-time derivation of variable dependency using abstract interpretation. *Journal of Logic Programming 13,* 2&3, 315–347.

Smolka, G. and Treinen, R. 1994. Records for logic programming. *Journal of Logic Programming 18,* 3, 229–258.

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

Swedish Institute of Computer Science, Programming Systems Group 1995. *SICStus Prolog User's Manual*, release 3 #0 ed. Swedish Institute of Computer Science, Programming Systems Group.

Zaffanella, E. 2001. Correctness, precision and efficiency in the sharing analysis of real logic languages. Ph.D. thesis, School of Computing, University of Leeds, Leeds, U.K. Available at `http://www.cs.unipr.it/~zaffanella/`.

Zaffanella, E., Bagnara, R., and Hill, P. M. 1999. Widening Sharing. In *Principles and Practice of Declarative Programming*, G. Nadathur, Ed. Lecture Notes in Computer Science, vol. 1702. Springer-Verlag, Berlin, Paris, France, 414–431.

Zaffanella, E., Hill, P. M., and Bagnara, R. 1999. Decomposing non-redundant sharing by complementation. In *Static Analysis: Proceedings of the 6th International Symposium*, A. Cortesi and G. Filé, Eds. Lecture Notes in Computer Science, vol. 1694. Springer-Verlag, Berlin, Venice, Italy, 69–84.

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