Denotational Abstract Interpretation of Logic Programs

K. MARRIOTT
Monash University

H. SØNDERGAARD
The University of Melbourne

N. D. JONES
DIKU

Abstract

Logic programming languages are based on a principle of separation of "logic" and "control." This means that they can be given simple model-theoretic semantics without regard to any particular execution mechanism (or proof procedure, viewing execution as theorem proving). While the separation is desirable from a semantical point of view, it does, however, make sound, efficient implementation of logic programming languages difficult. The lack of "control information" in programs calls for complex dataflow analysis techniques to guide execution. Since dataflow analysis furthermore finds extensive use in error-finding and transformation tools, there is a need for a simple and powerful theory of dataflow analysis of logic programs.

The present paper offers such a theory, based on F. Nielson's extension of P. and R. Cousot's *abstract interpretation*. We present a denotational definition of the semantics of definite logic programs. This definition is of interest in its own right because of its compactness. Stepwise we develop the definition into a generic dataflow analysis which encompasses a large class of dataflow analyses based on the SLD execution model. We exemplify one instance of the definition by developing a provably correct groundness analysis to predict how variables may be bound to ground terms during execution. We also discuss implementation issues and related work.

Categories and Subject Descriptors: D.1.6 [**Programming Languages**]: Logic Programming; D.3.4 [**Programming Languages**]: Processors—*compilers*, *optimization*; F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs—*assertions*, *invariants*, *logics of programs*; F.3.2 [**Logics and Meanings of Programs**]: Semantics of Programming Languages—*denotational semantics*

General Terms: Languages, Theory

Additional Key Words and Phrases: Abstract interpretation, Boolean functions, dataflow analysis, global analysis, groundness analysis.

[0]H. Søndergaard has been supported by The Australian Research Council. The work of N. D. Jones is partially supported by grants from the European Community and the Danish Research Council.

Authors' addresses: Kim Marriott, Dept. of Computer Science, Monash University, Clayton Vic. 3168, Australia. Harald Søndergaard, Dept. of Computer Science, The University of Melbourne, Parkville Vic. 3052, Australia. Neil D. Jones, DIKU, University of Copenhagen, Universitetsparken 1, DK-2100 Copenhagen Ø, Denmark.

1 Introduction

Dataflow analysis is an essential component of many programming tools. The main use of dataflow information is in compilers and other program transformers, where the analysis may guide various improvements of the generated code. Another use is to identify errors in a program, as done by program "debuggers" and type checkers. Stated generally, the purpose of program analysis is to decide whether some *invariant* holds at some *program point*. It may thereby be determined whether some transformation scheme is applicable, and possibly what the exact form of the synthesis should be. The process of investigating such invariance is called *dataflow analysis*.

A fruitful way of viewing dataflow analysis was suggested some 30 years ago, according to which dataflow analysis is "pseudo-evaluation," that is, a process that somehow mimics the normal execution of a program. Naur put this point of view to good use in explaining the type checking component of the Gier Algol compiler, and Sintzoff later provided further examples of its usefulness (we give references later). P. and R. Cousot formalized the idea in their influential theory of *abstract interpretation*.

We later discuss abstract interpretation in more detail, but the following example conveys the basic idea. Rather than using integers as data objects, a dataflow analysis may use *neg*, *zero*, and *plus* to describe negative integers, 0, and positive integers, respectively. Then by reinterpreting operations like multiplication according to the "rules of signs," the dataflow analysis may establish certain properties of a program, such as "whenever control reaches this loop, x is assigned a negative value."

Abstract interpretation prescribes certain relations that should hold between a dataflow analysis and the semantics of the programming language in question. If these relations hold, the dataflow analysis is guaranteed to be correct. To formalize them, however, precise formal definitions of both semantics and dataflow analysis are required. The analysis-as-pseudo-evaluation view is usually reified as a strong similarity between the two definitions, a certain degree of congruence. This naturally leads to viewing dataflow analysis simply as *non-standard semantics*.

Abstract interpretation of *logic programs* has gained considerable currency during the last 10 years. The major impetus has been the quest for dataflow analyses that can improve code generation in Prolog compilers. Logic programming languages are based on a principle of "separation of logic and control," which is desirable from a semantical point of view, but which also causes severe problems for implementation. The lack of "control information" in programs provides a wide scope for compiler optimizations and hence dataflow analysis of these languages. This, and the simple semantics of logic programs, explains the currency that abstract interpretation has gained in logic programming. However, dataflow analysis of logic programs is in some ways more complex than analysis of more traditional languages, since dataflow is bi-directional (owing to unification) and control flow is in terms of backtracking, at least for top-down sequential execution.

Much of the research into abstract interpretation of logic programs has been devoted to designing abstract interpretation "frameworks"' which consist of a generic dataflow algorithm with a few basic

operations as parameters. A particular analysis is obtained by providing these parametric functions. An important property of a framework is that correctness of the resultant analysis is assured as long as the parametric functions correctly approximate the standard interpretation of these parametric functions. Such frameworks facilitate the development of structurally similar analyses and their proofs of correctness, and also allow different analyses to be easily implemented by means of a common "analysis engine."

Frameworks, however, though generic in a certain sense, are implicitly based on a single set of semantic equations which reflect the operational semantics of the language being analyzed and the particular information required. In fact, almost all existing frameworks model the SLD semantics of definite logic programs and collect information about the calls occurring at runtime. A single framework is not suitable for all dataflow applications in logic programming. For example, if the operational semantics is changed, say to a "bottom-up" evaluation or to allow dynamic atom scheduling, or the language is extended, say to allow constraints or negation, then the underlying semantic equations are changed and so a new framework must be designed and proved correct.

Here we give a general abstract interpretation theory in which to compare and design these frameworks and their instances, that is, specific dataflow analyses. The key idea, due to Nielson, is to express the underlying semantic equations of each framework in a common *meta-language*. The main pragmatic advantage is that by a careful choice of the meta-language, properties that are important for proving correctness of dataflow analysis can be established at the level of the meta-language once and for all, rather than establishing them for each framework or analysis. A "universal" meta-language also facilitates a stepwise, derivational approach to the development of dataflow analyses. It is worth noting that these semantic equations can, with the right interpreter, be directly executed, providing a prototype analysis engine which in turn can be instantiated to perform various dataflow analyses.

We illustrate the use of our theory by defining an abstract interpretation framework for definite logic programs which models the standard SLD operational semantics and collects information about a particular query's answers. The definition can be easily extended to collect information about calls. Our semantic definition is considerably cleaner than previous definitions that have been suggested for SLD style semantics. Its simplicity is mainly due to our use of constraints instead of classical substitutions as this avoids traditional problems with renaming and allows us to express unification and composition as simple lattice operations. Finally, we use our abstract interpretation framework to define a simple yet highly precise groundness analysis. This analysis makes use of Boolean functions to trace the interrelation of groundness among variables.

In Section 2 we recapitulate some basic notions. In Section 3 we present the dataflow-analysis-as-approximate-computation view. Section 4 contains an introduction to "language-independent" abstract interpretation. In Section 5 we develop a denotational definition that captures the essence of SLD resolution, as seen from a point of view of many dataflow analyses. This definition is of some interest already because of its avoidance of substitutions and standardizing apart. In Section 6 we turn the semantic definition into a generic definition of a *dataflow semantics*, whose instances define

a wide class of useful dataflow analyses for logic programs. As an example we define a groundness analysis in Section 7. In Section 8 we discuss the implementation of generic dataflow analyzers. In Section 9 we discuss related work, and Section 10 contains a concluding discussion.

Much of the material in this paper was first presented as a tutorial on abstract interpretation given at the North American Conference on Logic Programming in Cleveland, Ohio, 1989. The current exposition is an extensively revised version of a paper presented at the Italian Logic Programming Conference (GULP) in 1990.

Readers are expected to be familiar with the theory of logic programming, and with denotational semantics at the level of the textbooks by Lloyd [36] and Schmidt [56], for example. We have tried to comply with the terminology of these two books. For a general introduction to abstract interpretation see Abramsky and Hankin [1].

2 Preliminaries

In this section we recapitulate some basic notions and facts from domain theory and explain some notation that will be used throughout.

A *preordering* on X is a binary relation that is reflexive and transitive. A *partial ordering* is a preordering that is antisymmetric. A set equipped with a partial ordering is a *poset*. Let $(X, \leq)$ be a poset. A (possibly empty) subset Y of X is a *chain* iff for all $y, y' \in Y, y \leq y' \vee y' \leq y$.

Let $(X, \leq)$ be a poset and let Y be a subset of X. An element $x \in X$ is an *upper bound* for Y iff $y \leq x$ for all $y \in Y$. Dually we may define a *lower bound* for Y. An upper bound x for Y is the *least upper bound* for Y iff, for every upper bound x' for Y, $x \leq x'$, and when it exists, we denote it by $\bigsqcup Y$. Dually, a lower bound x for Y is the *greatest lower bound* for Y iff, for every lower bound x' for Y, $x' \leq x$. When it exists, we denote the greatest lower bound for Y by $\bigsqcap Y$.

A poset for which every subset possesses a least upper bound and a greatest lower bound is a *complete lattice*. In particular, equipped with the subset ordering, the powerset of X, denoted by $\mathcal{P}X$, is a complete lattice. Let X be a complete lattice. We denote $\bigsqcup \emptyset = \bigsqcap X$ by $\bot_X$ and $\bigsqcap \emptyset = \bigsqcup X$ by $\top_X$. The complete lattice X is *Noetherian* iff every ascending chain in X is finite.

Functions are generally used in their Curried form. Our notation for function application uses parentheses sparingly. We use redundant parentheses only when they would seem to help the eye. As usual, function space formation $X \to Z$ associates to the right, and function application to the left. We occasionally use Church's lambda notation for functions, and we use "$\circ$" for composition of functions.

Let $(X, \leq)$ and $(Z, \preceq)$ be posets. A function $F : X \to Z$ is *monotonic* iff $x \leq x' \Rightarrow F\ x \preceq F\ x'$ for all $x, x' \in X$. In what follows, monotonicity of functions is essential, so much so that it is understood throughout this paper that $X \to Z$ denotes the space of *monotonic* functions from X to Z. Furthermore, the function space $X \to Z$ will always be ordered pointwise, that is, if $F, G : X \to Z$ are functions and the ordering on Z is $\preceq$, then the ordering $\sqsubseteq$ on $X \to Z$ is defined

by $F \sqsubseteq G$ iff $\forall\, x \in X \,.\, F\ x \preceq G\ x$.

A function $F : X \to Z$ is *injective* iff $F\ x = F\ x' \Rightarrow x = x'$ for all $x, x' \in X$, and F is *bijective* iff there is a function $F' : Z \to X$ such that $F \circ F'$ and $F' \circ F$ are identity functions.

Let X and Z be complete lattices. A function $F : X \to Z$ is *strict* iff $F\ \bot_X = \bot_Z$. Dually F is *co-strict* iff $F\ \top_X = \top_Z$.

A *fixpoint* for a function $F : X \to X$ is an element $x \in X$ such that $x = F\ x$. If X is a complete lattice, then the set of fixpoints for (the monotonic) $F : X \to X$ is itself a complete lattice. The least element of this lattice is the *least fixpoint* for F, denoted by *lfp* F. Furthermore, defining

$$F \uparrow \alpha = \begin{cases} \bigsqcup\{F \uparrow \alpha' \mid \alpha' < \alpha\} & \text{if } \alpha \text{ is a limit ordinal} \\ F\ (F \uparrow (\alpha - 1)) & \text{if } \alpha \text{ is a successor ordinal,} \end{cases}$$

there is some ordinal α such that $F \uparrow \alpha =$ *lfp* F[1]. The sequence $(F \uparrow 0), (F \uparrow 1), \ldots, (\textit{lfp}\ F)$ is the *(completed) Kleene sequence* for F. If a monotonic function is defined on a *Noetherian* lattice then it has a finite Kleene sequence.

Let X be a complete lattice. A predicate Q is *inclusive* on X iff for all (possibly empty) chains $Y \subseteq X$, $Q\ (\bigsqcup Y)$ holds whenever $(Q\ y)$ holds for every $y \in Y$. Inclusive predicates are admissible in *fixpoint induction*: assume that $F : X \to X$ is monotonic and $Q\ x$ implies $Q\ (F\ x)$ for all $x \in X$. If Q is inclusive then $Q\ (\textit{lfp}\ F)$ holds.

Finally a note about the "semantic brackets" $[\![$ and $]\!]$: We use these for quasi-quotation generally, that is, in this paper they are simply "Quine corners."

3 Approximate computation

Abstract interpretation formalizes dataflow analysis by viewing it as *approximate computation*, in which one manipulates *descriptions* of data rather than the data themselves. In this section we detail this idea. In Section 4 we explain how it can be formalized in the theory of denotational abstract interpretation.

In general the disadvantage of an approximate computation is that the result it yields is not as precise as that of a proper computation. But this is compensated for by two important advantages: First, one approximate computation may yield information about many proper computations at once. Second, approximate computation is usually much faster than the proper computation. In our case, where the concern is with the approximate computation of programs, the difference in speed between proper and approximate computation may be extreme: non-termination versus termination.

The idea of performing program analysis by approximate computation appeared very early in computer science. Naur identified the idea and applied it in work on the Gier Algol compiler in the early sixties [50]. He coined the term *pseudo-evaluation* for what would later be described as

[1] The origin of this assertion is in Kleene's first recursion theorem [33].

> "a process which combines the operators and operands of the source text in the manner in which an actual evaluation would have to do it, but which operates on descriptions of the operands, not on their values" [25].

The same basic idea is found in work by Reynolds [55] and by Sintzoff [57]. Sintzoff used it for proving a number of well-formedness aspects of programs in an imperative language, and for verifying termination properties.

By the mid seventies, efficient dataflow analysis had been studied rather extensively by researchers such as Kam, Kildall, Tarjan, Ullman, and others (for references, see Hecht's book [22]). As a powerful attempt to unify much of that work, a precise framework for discussing approximate computation (of imperative programs) was developed by Patrick and Radhia Cousot [10, 12]. The advantage of such a unifying framework is that it serves as a basis for understanding various dataflow analyses better, including their interrelation, and for discussing their correctness.

The overall idea of P. and R. Cousot was to define a "static" semantics which associates with each program point the set of possible storage states that may obtain at run-time whenever execution reaches that point. A dataflow analysis can then be construed as a finitely computable approximation to the static semantics. The work of P. and R. Cousot has later been extended to declarative languages. Such extensions are not straightforward. For example, there is no clear-cut notion of "program point" in functional or logic programs. Also, dataflow analysis of programs written in a programming language such as Prolog differs somewhat from the analysis of programs written in more conventional programming languages because the dataflow is bi-directional, owing to unification, and the control flow is more complex, owing to backtracking.

Of the applications of abstract interpretation in functional programming we mention work by Jones [26] and by Jones and Muchnick [27] on termination analysis for lambda expressions and, in a Lisp setting, improved storage allocation schemes through reduced reference counting. The main application, though, has been *strictness analysis*, which is concerned with the problem of determining cases where applicative order may be safely used instead of normal order execution. The study of strictness analysis was initiated by Mycroft [49] and the literature on the subject is now quite extensive, see for example Nielson [52].

We can describe approximate computation as evaluating a formula or a program, not over its standard domain, but over a non-standard domain of "descriptions." The standard domain may consist of "states", sets of terms, atomic formulas, substitutions, or whatever, depending on how the semantics is modeled, and the non-standard domain is determined by the kind of program properties that we want to expose. Of course, when performing approximate computations, one must reinterpret all operators so as to apply to descriptions rather than to proper values.

Assume we have a data domain U and operators on U. In the example below, U will be $\mathbb{Z}$, the set of integers. We also assume we have a set X of descriptions. To be precise about the relation between values and descriptions, a *concretization function* $\gamma : X \to \mathcal{P}\, U$ is defined[2]. For every

[2] The terminology, including the use of the symbol 'γ', is due to P. and R. Cousot.

$\otimes$	$\bot$	*odd*	*even*	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
odd	$\bot$	*odd*	*even*	$\top$
even	$\bot$	*even*	*even*	*even*
$\top$	$\bot$	$\top$	*even*	$\top$

Table 1: Multiplication of parities

description $x \in X$, $(\gamma\ x)$ is the set of objects which x describes. Thus γ is the semantic function for descriptions.

Example 3.1 Let X be the set $\{\bot, even, odd, \top\}$, ordered by $x \leq x'$ iff $x = \bot \vee x = x' \vee x' = \top$. The denotation of description $x \in X$ is given by $\gamma : X \to \mathcal{P}\,\mathbb{Z}$ by

$$\begin{array}{lcl} \gamma\ \bot & = & \emptyset \\ \gamma\ even & = & \{z \in \mathbb{Z} \mid z \text{ is even}\} \\ \gamma\ odd & = & \{z \in \mathbb{Z} \mid z \text{ is odd}\} \\ \gamma\ \top & = & \mathbb{Z}. \ \blacksquare \end{array}$$

Note that descriptions are ordered according to how large a set of objects they apply to: the more imprecise, the "higher" they sit in the structure. The set $\{2, 4\}$ is approximated by the description *even*, the set $\{2, 3\}$ by $\top$, and multiplication of sets of integers is approximated by the operator $\otimes : X \times X \to X$, given by Table 1. The example, incidentally, illustrates the fact that application of an operator to a description of "everything," that is, $\top$, need not involve loss of information: the operator $\otimes$ is not co-strict since, for example, $\top \otimes even = even$. Also note that the ordering on descriptions is, in a sense, opposite to the ordering used in domain theory: for descriptions, the *top* element corresponds to total lack of information.

< *Figure* 1 >

To see how a computation using the descriptions in Example 3.1 can proceed, consider the flow diagram in Figure 1[3]. Program points are numbered edges. Descriptions can be propagated in the graph by appropriately interpreting the commands according to the "rules of parities." For example, the fact that n is odd at program point 5 is used to conclude that n is even at point 6. Such reasoning can easily be mechanized. Assuming n is $\top$ at point 1, we get the following descriptions of n at other points: at 2 it is $\top$, at 3 it is *even*, at 4 it is $\top$, at 5 it is *odd*, at 6 it is *even*, and at 7 it is *odd*. This information justifies transformation of the program so as to avoid a number of tests; for example, the statement $n := 3n + 1$ can be replaced by $n := (3n + 1)/2$.

[3] Collatz's problem in number theory (also known as the $3n + 1$ problem) amounts to determining whether this program terminates for all $n \in \mathbb{N}$. This problem is still unsolved.

The above example is a simple case of dataflow analysis viewed as approximate computation. In general there are three parameters in designing objects that may serve as descriptions: (1) the program properties that we want to expose, that is, *adequacy* of descriptions, (2) the *precision* that we hope to obtain, and (3) the *efficiency* of the resulting dataflow analysis. It is important to keep in mind that we usually are interested in properties that are undecidable, and so we cannot hope for optimal precision in a strong sense. This is acceptable: a dataflow analysis need not tell the whole truth, although it should of course not contradict truth. In this way, approximate computation becomes to standard computation what numerical analysis is to mathematical analysis: using numerical techniques, problems with no known analytic solution can be "solved" numerically, that is, a solution can be estimated within an interval of error.

It is clear that there is a trade-off between precision and efficiency. The finer-grained descriptions we use, the better dataflow analysis can be performed, but considerations of finite computability and efficiency put a limit on granularity. To obtain termination it is common to use descriptions that form Noetherian lattices. The reason is that if the analysis can be expressed as least fixpoint of a monotonic function on such a lattice then this fixpoint can be computed by means of the function's completed Kleene sequence.

Note that we are not primarily interested in the *results* of computations. For program analysis purposes, our main concern is to extract information about invariance at particular program points, such as "at this point, variable x is always assigned positive values" or "this term becomes ground during execution."

4 A denotational approach

Let us briefly recapitulate the advantages of abstract interpretation. First, it is *semantics-based*, by which we mean to say that it forces dataflow analyses to be defined with direct reference to a formal semantics of the given programming language. While perhaps somewhat restrictive, this discipline is what facilitates the development of *provably correct* dataflow analyses. Second, it is a unifying theory. Often, many seemingly unrelated dataflow analyses can be expressed as variants of a common form. Abstract interpretation tends to emphasize the essential differences as well as what is common in analyses, thus helping taxonomy.

The last point suggests that the design and implementation of a range of dataflow analyses may often be simplified by first designing a *framework* which is, essentially, a generic algorithm that captures the overall computation regime common to a large class of analyses, and then providing the characteristic details of a given analysis in the form of various parametric functions. Indeed, in the area of logic programming, such generic frameworks and various implementations, called *analysis engines*, are now emerging.

However, abstract interpretation can be generalized even further so as to provide a theory of dataflow analysis which is *independent of any particular programming language or operational*

semantics. We have in mind here Nielson's theory[4] of *denotational abstract interpretation* [51, 52, 53].

This section is concerned with explaining and customizing Nielson's theory to better serve our needs. There are two or three revisions that prove useful in the setting of logic programs. These revisions are necessary because Nielson was concerned with deterministic languages but logic programs are non-deterministic. Most importantly, we include a join operator in the meta-language, as join is the natural operation for combining sets of possible outcomes from a non-deterministic choice. Another difference, is that we do not require continuity of functions. We show that Nielson's results still hold in this revised setting, as long as approximation is formalized in terms of a concretization function, rather than in terms of an abstraction function.

4.1 Language-independent abstract interpretation

Assume we are given a language in which one can express the semantics of a wide variety of programming languages. The theory of abstract interpretation may then be developed in the framework of this *meta-language* once and for all. In this way, we need not invent (or reinvent) abstract interpretation for each new kind of programming language or operational semantics—each is just a special instance of the general theory. With a careful choice of meta-language, properties that are important for the correctness of dataflow analyses can be established at the level of the meta-language once and for all. They need not be re-proved for individual analyses or even for individual programming languages. Figure 2 illustrates the point which we push further in Section 4.2.

< *Figure* 2 >

Expressing standard and non-standard semantics in the same meta-language also supports a *derivational* approach to the development of dataflow analyses. The *definition* of a dataflow analysis should be easily derivable from that of the standard semantics. Only in a second stage should the analysis be implemented from its definition. Such a stepwise approach may be preferable to the task of proving some baroque dataflow procedure correct with respect to a semantic definition (or an interpreter).

< *Figure* 3 >

Figure 3 illustrates how the denotational approach allows the separation of concerns. The two upper circles represent formal definitions in the meta-language. The lower circles represent *implementations* of the semantic definitions. The vertical arrows represent the relation "implements" (or "abstracts" if read the other way). The point is that the relation (marked '?' in the figure) between a dataflow procedure and an operational semantics is usually very complicated and the problem of establishing the former's correctness with respect to the latter is hard. In our approach it is broken

[4] Some of the ideas in Nielson's treatment can be traced back to work by Véronique Donzeau-Gouge [19].

up into two orthogonal issues: that of implementation (of a formally defined dataflow analysis) and that of correct *approximation* of one definition by another.

The notion of approximation is made precise in Section 4.2. Later, when we give the formal semantic definitions (the two upper circles in Figure 3) relevant to logic programs, the reader will realize that they are virtually identical—a few "bricks" may differ, but the structure and mortar are identical. This is very useful, since the approximation relation will be shown to have the property that it will automatically hold at the top level if only it holds at the level of the few selected "bricks".

We stress that, to achieve this desirable situation, the exact choice of meta-language is important. It is not the case that any language will do. On the one hand, the meta-language must be sufficiently expressive to be useful, and on the other hand, it must be sufficiently curtailed for the all-important Theorem 4.4 below to hold.

The present treatment is similar to Nielson's in his paper on strictness analysis [52]. There are, however, important differences. We do not formalize abstract interpretation in terms of an "abstraction function" but rather in terms of a "concretization function." In the theory of P. and R. Cousot [10, 12] this difference would be a matter of taste only, since the two functions uniquely determine each other. Here, however, the difference is important: we do not require the existence of an abstraction function, and Nielson does not require the existence of a concretization function. The reason for our choice is that we want our meta-language to include a join operator, something that Nielson does not need, as he is concerned with deterministic programming languages only. In Nielson's framework, the addition of a join operation would invalidate the all-important Theorem 4.4 below, as shown in Example 4.1. In addition we find it simpler to think in terms of concretization functions since they are in a sense "semantic functions" for descriptions.

Like Nielson we use the formalism of denotational semantics. Although this is not the only choice for a meta-language, its usefulness and suitability should be apparent from the following sections: both standard and non-standard semantics are easily presented in the meta-language. By choosing the right level of abstraction, they can be made highly congruent: if the standard semantics employs a certain operator on the standard domain, the non-standard semantics should use a corresponding operator on the non-standard domain.

The meta-language is one of typed lambda expressions, and the language of type expressions is given by

$$\begin{array}{lll} T \in \mathit{Type} & ::= & S \mid L \\ L \in \mathit{Lat} & ::= & D \mid T \to L \end{array}$$

where $S \in \mathit{Stat}$, $D \in \mathit{Dyn}$, *Stat* is a collection of *static* types, and *Dyn* is a collection of *dynamic* types. The difference between the two kinds is that (the interpretation of) a static type remains the same throughout all (standard and non-standard) semantics, whereas a dynamic type may change. We call $\mathit{Stat} \cup \mathit{Dyn}$ the collection of *base* types, and *Lat* is the collection of lattice types. When we give the semantics of these types shortly, it will become clear why S, $T \to S$, $T \to T \to S$, and so on, are excluded from the lattice types.

The syntax of the meta-language is given by

$$
\begin{array}{rcll}
e & ::= & c_i & \text{(base functions)} \\
 & | & x_i & \text{(variables)} \\
 & | & \lambda\ x : T\,.\,e & \text{(function abstraction)} \\
 & | & e\ e' & \text{(function application)} \\
 & | & \text{if } e \text{ then } e' \text{ else } e'' & \text{(conditional)} \\
 & | & \mathit{lfp}\ e & \text{(least fixed point)} \\
 & | & e \sqcup e' & \text{(join)}
\end{array}
$$

We will generally be concerned with expressions that are *closed*, that is, every variable is bound by a lambda.

There is a notion of well-typing for this language, and we explain it shortly. Static types are interpreted as posets (ordered by identity) and dynamic types as complete lattices. A *type interpretation* $\mathbf{I}$ thus assigns a structure $(\mathbf{I}\ T)$ to each base type T. By natural extension the semantics of types is defined as follows:

$$
\begin{array}{lcll}
\mathbf{I}\,[\![S]\!] & = & \mathbf{I}\,S & \text{(a (fixed) poset, ordered by identity)} \\
\mathbf{I}\,[\![D]\!] & = & \mathbf{I}\,D & \text{(some complete lattice)} \\
\mathbf{I}\,[\![T \to L]\!] & = & \mathbf{I}\,[\![T]\!] \to \mathbf{I}\,[\![L]\!] & \text{(ordered pointwise)}
\end{array}
$$

Recall that the "$\to$" on the right-hand side denotes monotonic function space.

By this, $\mathbf{I}\,[\![L]\!]$ is a complete lattice for every $L \in \mathit{Lat}$. This is the reason why dynamic types were required to denote complete lattices. The semantic equations in the following sections define least fixpoints of monotonic functionals over domains of type $T \to L$, and the type discipline thus automatically guarantees well-definedness of the semantics. We do not want to require that domains with static types have excessive structure: many domains which are to remain fixed throughout all (interpretations of) semantic definitions, such as "the set of programs," are best thought of simply as sets.

We now explain the notion of well-typedness. The denotation of an expression e is relative to a type environment τ and a type T such that $\tau \vdash e : T$ (that is, in environment τ, e has type T). The type rules are:

$$\tau \vdash c_i : T \quad \text{iff } T \text{ is the (fixed) type of } c_i \qquad\qquad \tau \vdash x_i : T \quad \text{iff } \tau\ x_i = T$$

$$\frac{\tau\,[T/x] \vdash e : T'}{\tau \vdash (\lambda\ x : T\,.\,e) : T \to T'} \qquad\qquad \frac{\tau \vdash e : T \to T' \qquad \tau \vdash e' : T}{\tau \vdash (e\ e') : T'}$$

$$\frac{\tau \vdash e : \mathit{Bool} \qquad \tau \vdash e' : T \qquad \tau \vdash e'' : T}{\tau \vdash \text{if } e \text{ then } e' \text{ else } e'' : T} \qquad\qquad \frac{\tau \vdash e : L \to L}{\tau \vdash \text{lfp } e : L}$$

$$\frac{\tau \vdash e : L \qquad \tau \vdash e' : L}{\tau \vdash e \sqcup e' : L}$$

Here $\tau\,[T/x]$ is the type environment which is identical to τ, except that x is associated with type T. The type *Bool* is that of truth values, and L denotes a lattice type.

We are now ready to explain the semantics of the meta-language. An *interpretation* $\mathbf{I}$ denotes a type interpretation (by an abuse of notation also called $\mathbf{I}$) together with an assignment of an element of $\mathbf{I}\,[\![T]\!]$ to each base function c of type T. By natural extension this gives the semantics of the meta-language. Let the domain of τ be $\{x_1, \ldots, x_k\}$ and let $\tau\ x_i = T_i$ for $i \in \{1, \ldots, k\}$. Then $\mathbf{I}\,[\![e]\!] : \mathbf{I}\,[\![T_1]\!] \times \ldots \times \mathbf{I}\,[\![T_k]\!] \to \mathbf{I}\,[\![T]\!]$ is defined as follows (we let η abbreviate $(v_1, \ldots, v_k)$):

$$
\begin{array}{lcl}
\mathbf{I}\,[\![c_i]\!]\ \eta & = & \mathbf{I}\ c_i \\
\mathbf{I}\,[\![x_i]\!]\ \eta & = & v_i \\
\mathbf{I}\,[\![\lambda\ x : T\ .\ e]\!]\ \eta\ v & = & \mathbf{I}\,[\![e]\!]\ (v_1, \ldots, v_k, v) \\
\mathbf{I}\,[\![e\ e']\!]\ \eta & = & \mathbf{I}\,[\![e]\!]\ \eta\ (\mathbf{I}\,[\![e']\!]\ \eta) \\
\mathbf{I}\,[\![\text{if } e \text{ then } e' \text{ else } e'']\!]\ \eta & = & \text{if } \mathbf{I}\,[\![e]\!]\ \eta \text{ then } \mathbf{I}\,[\![e']\!]\ \eta \text{ else } \mathbf{I}\,[\![e'']\!]\ \eta \\
\mathbf{I}\,[\![\mathit{lfp}\ e]\!]\ \eta & = & \mathit{lfp}\ (\mathbf{I}\,[\![e]\!]\ \eta) \\
\mathbf{I}\,[\![e \sqcup e']\!]\ \eta & = & (\mathbf{I}\,[\![e]\!]\ \eta) \sqcup (\mathbf{I}\,[\![e']\!]\ \eta).
\end{array}
$$

By varying the interpretation, one may obtain different semantics from the same set of semantic equations. The *standard interpretation* gives the usual input/output behavior of the program while dataflow analyses may be expressed as "non-standard" interpretations. The role of abstract interpretation is to give relationships between the standard and non-standard interpretations which guarantee that the dataflow analysis safely approximates the standard semantics.

4.2 A theory of approximation

To relate standard and non-standard interpretations, one must first explain what the descriptions in the non-standard semantics mean in terms of the standard semantics. This is done by means of "insertions" where an insertion consists of a function which maps descriptions to the largest object that they describe.

Definition. An *insertion* is a triple (X, γ, Y) where X and Y are complete lattices, and the monotonic function $\gamma : X \to Y$ is co-strict. A *concretization family*, $\Gamma = \{\gamma_D\}$, for interpretations $\mathbf{I}'$ and $\mathbf{I}$ is an indexed family of functions such that for each $D \in \mathit{Dyn}$, $((\mathbf{I}'\ D), \gamma_D, (\mathbf{I}\ D))$ is an insertion. ■

The motivation for the definition of insertion is that the domain X of descriptions should "approximate" Y in the sense that the two have compatible structure, so γ should be monotonic. Furthermore, every element in Y should have a corresponding description, so γ should be co-strict.

In P. and R. Cousot's theory of abstract interpretation, the function γ is required to have an *adjoined*, so-called *abstraction* function $\alpha : Y \to X$.

Definition. Let X and Y be complete lattices. The (monotonic) functions $\gamma : X \to Y$ and $\alpha : Y \to X$ are *adjoined* iff $\forall\, x \in X\ .\ \forall\, y \in Y\ .\ \alpha\ y \leq x \Leftrightarrow y \leq \gamma\ x$. ■

The abstraction function can be thought of as giving the best description of an object. P. and R. Cousot [10] demand that an abstraction function exist. This they do on grounds that otherwise dataflow analyses may not yield the best possible result, given the set of descriptions chosen, see also Søndergaard [59].

Like Bruynooghe and Janssens [4, 5] we do not require the existence of an abstraction function. Note that when it exists, it is uniquely defined by $\alpha\ y = \bigsqcap\{x \mid y \leq \gamma\ x\}$. The following definition allows us to characterize when an abstraction function exists.

Definition. Let X be a lattice and $Y \subseteq X$. We say that Y is *Moore-closed* (in X) iff

$$\forall\ Y' \subseteq Y\ .\ \bigsqcap Y' \in Y.\quad \blacksquare$$

Lemma 4.1 [12]. Let (X, γ, Y) be an insertion. Then γ has an adjoint iff $\{\gamma\ x \mid x \in X\}$ is Moore-closed. $\blacksquare$

Recalling our convention (Example 3.1) of ordering descriptions according to how large a set of objects they apply to, we now define what it means for a description to safely approximate another description.

Definition. Let $\Gamma = \{\gamma_D\}_{D \in Dyn}$ be a concretization family for interpretations $\mathbf{I}'$ and $\mathbf{I}$, and let $S \in \mathit{Stat}$ and $D \in \mathit{Dyn}$ be types. The relation $\mathit{appr}[\Gamma]_T$ is defined by

$$\begin{array}{lcl} u\ \mathit{appr}[\Gamma]_S\ v & \Leftrightarrow & v = u \\ u\ \mathit{appr}[\Gamma]_D\ v & \Leftrightarrow & v \leq \gamma_D\ u \\ u\ \mathit{appr}[\Gamma]_{T \to L}\ v & \Leftrightarrow & \forall\ u', v'\ .\ u'\ \mathit{appr}[\Gamma]_T\ v' \Rightarrow (u\ u')\ \mathit{appr}[\Gamma]_L\ (v\ v'). \end{array} \quad \blacksquare$$

When the concretization family Γ and type T is clear from the context we shall write $\mathit{appr}[\Gamma]_T$ simply as appr.

Lemma 4.2 For all lattice types L and concretization families Γ, $\mathit{appr}[\Gamma]_L$ is inclusive.

Proof: The proof is by structural induction on the types. Let $Z \subseteq (\mathbf{I}\ [\![L]\!]) \times (\mathbf{I}'\ [\![L]\!])$ be a chain such that $x\ \mathit{appr}[\Gamma]_L\ y$ holds for all $(x, y) \in Z$. Clearly $\bigsqcup Z = (\bigsqcup X, \bigsqcup Y)$, where $X = \{x \mid (x, y) \in Z\}$ and $Y = \{y \mid (x, y) \in Z\}$.

Consider the case $L \in \mathit{Dyn}$. By monotonicity of γ_L, $y \leq \gamma_L\ x \leq \gamma_L\ (\bigsqcup\ X)$ for all $(x, y) \in Z$. Thus $\bigsqcup Y \leq \gamma_L\ (\bigsqcup\ X)$ and so appr is inclusive for this case.

The other case is when $L = [\![T \to L']\!]$. Let $(x', y') \in (\mathbf{I}\ [\![T]\!]) \times (\mathbf{I}'\ [\![T]\!])$ be given. Then $W = \{(x\ x', y\ y') \mid (x, y) \in Z\}$ is a chain and $\bigsqcup W = ((\bigsqcup X)\ x', (\bigsqcup Y)\ y')$. Assume $x'\ \mathit{appr}[\Gamma]_T\ y'$ holds. Then $(x\ x')\ \mathit{appr}[\Gamma]_{L'}\ (y\ y')$ holds for all $(x, y) \in Z$, by the definition of appr. Since $\mathit{appr}[\Gamma]_{L'}$ is inclusive, $(x\ x')\ \mathit{appr}[\Gamma]_{L'}\ (y\ y')$ holds for $(x, y) = \bigsqcup Z = (\bigsqcup X, \bigsqcup Y)$. Since x' and y' were arbitrary, $(\bigsqcup X)\ \mathit{appr}[\Gamma]_L\ (\bigsqcup Y)$ holds, so $\mathit{appr}[\Gamma]_L$ is inclusive. $\blacksquare$

Definition. A relation $R \subseteq X \times Y$ is *order-preserving* iff for all $x, x' \in X$ and $y, y' \in Y$, if $x\ R\ y$ and $x \leq x'$ and $y' \leq y$, then $x'\ R\ y'$. R is *additive* iff for all $x \in X$ and $y, y' \in Y$, if $x\ R\ y$ and $x\ R\ y'$, then $x\ R\ y \sqcup y'$. ■

Lemma 4.3 For all lattice types L and concretization families Γ, $appr[\Gamma]_L$ is order-preserving and additive.

Proof: The proof is by straightforward structural induction on the types. ■

These results lead to the following theorem which extends an important result by Nielson [52]. It says that if we are given base functions $c_1, \ldots, c_n$ and $c'_1, \ldots, c'_n$ such that c'_i approximates c_i for every $i \in \{1, \ldots, n\}$, then the closed expression $e[c'_1, \ldots, c'_n]$ approximates $e[c_1, \ldots, c_n]$.

Theorem 4.4 Let Γ be a concretization family for interpretations $\mathbf{I}$ and $\mathbf{I}'$. If $(\mathbf{I}\ c)\ appr\ (\mathbf{I}'\ c)$ holds for every base function c, then, for any closed expression e, $(\mathbf{I}\ e)\ appr\ (\mathbf{I}'\ e)$.

Proof: The proof is by structural induction on the form of e. Most cases are straightforward and we show only two: $e = [\![lfp\ e']\!]$ because fixpoint induction is needed for that case, and $e = [\![e_1 \sqcup e_2]\!]$ since this is a construct which is not in Nielson's language.

Consider the case $e = [\![lfp\ e']\!]$. Note that e' must be a closed expression. Furthermore, the type discipline guarantees that $\mathbf{I}\ [\![e']\!] \in \mathbf{I}\ [\![L]\!] \to \mathbf{I}\ [\![L]\!]$ for some $L \in Lat$, while $\mathbf{I}'\ [\![e']\!] \in \mathbf{I}'\ [\![L]\!] \to \mathbf{I}'\ [\![L]\!]$.

Let $g : ((\mathbf{I}\ [\![L]\!]) \times (\mathbf{I}'\ [\![L]\!])) \to ((\mathbf{I}\ [\![L]\!]) \times (\mathbf{I}'\ [\![L]\!]))$ be defined by $g\ (x, x') = (\mathbf{I}\ [\![e']\!]\ x, \mathbf{I}'\ [\![e']\!]\ x)$ and assume that $x\ appr\ x'$ holds. By the induction hypothesis $(\mathbf{I}\ [\![e']\!]\ x)\ appr\ (\mathbf{I}'\ [\![e']\!]\ x)$. We can interpret this as a statement $Q\ (x, x') \Rightarrow Q\ (g\ (x, x'))$ where Q is inclusive by Lemma 4.2, and so $Q\ (lfp\ g)$ holds, that is, $(lfp\ (\mathbf{I}\ [\![e']\!]))\ appr\ (lfp\ (\mathbf{I}'\ [\![e']\!]))$. Thus $(\mathbf{I}\ [\![lfp\ e']\!])\ appr\ (\mathbf{I}'\ [\![lfp\ e']\!])$, as desired.

Consider the case $e = [\![e_1 \sqcup e_2]\!]$. Note that e_1 and e_2 must be closed. The type discipline guarantees that $(\mathbf{I}\ [\![e_1]\!]), (\mathbf{I}\ [\![e_2]\!]) \in (\mathbf{I}\ [\![L]\!])$ for some lattice type L, while $(\mathbf{I}'\ [\![e_1]\!]), (\mathbf{I}'\ [\![e_2]\!]) \in (\mathbf{I}'\ [\![L]\!])$. Thus $\mathbf{I}\ [\![e_1 \sqcup e_2]\!]$ and $\mathbf{I}'\ [\![e_1 \sqcup e_2]\!]$ are well-defined.

By the induction hypothesis,

$$(\mathbf{I}\ [\![e_1]\!])\ appr[\Gamma]_L\ (\mathbf{I}'\ [\![e_1]\!]) \text{ and } (\mathbf{I}\ [\![e_2]\!])\ appr[\Gamma]_L\ (\mathbf{I}'\ [\![e_2]\!]).$$

From Lemma 4.3, $appr[\Gamma]_L$ is order-preserving, so

$$(\mathbf{I}\ [\![e_1 \sqcup e_2]\!])\ appr[\Gamma]_L\ (\mathbf{I}'\ [\![e_1]\!]) \text{ and } (\mathbf{I}\ [\![e_1 \sqcup e_2]\!])\ appr[\Gamma]_L\ (\mathbf{I}'\ [\![e_2]\!]).$$

Thus, by additivity of $appr[\Gamma]_L$, $(\mathbf{I}\ [\![e_1 \sqcup e_2]\!])\ appr[\Gamma]_L\ (\mathbf{I}'\ [\![e_1 \sqcup e_2]\!])$. ■

It is worth noticing the generality of this result: it immediately allows us to argue inductively the correctness of a whole dataflow analysis (that is, non-standard semantics) once certain primitive

base functions are shown to be in the relation "safely approximates." This applies not only to logic programming languages as discussed in this paper, but to any language whose semantics can be expressed in the meta-language. (In fact the meta-language can be further extended in various natural directions [52].)

Example 4.1 In Nielson's theory of denotational abstract interpretation the approximation relation is defined in terms of an "abstraction function" $\alpha : Y \to X$ which maps a data object $y \in Y$ to its best approximation $x \in X$. Thus x approximates y iff $\alpha\ y \leq x$.

< *Figure* 4 >

In this setting Theorem 4.4 does not hold because of the join operator. To see this consider the lattices in Figure 4. Clearly, $a \sqcup_Y b = \top$ and $a \sqcup_X b = c$. With the abstraction function $\alpha : Y \to X$ defined by $\alpha\ y = y$, we have that a approximates a and b approximates b, but c does not approximate $\top$. ■

Perhaps surprisingly, the relation $appr[\Gamma]_T$ is in general neither reflexive nor transitive. For counterexamples see Nielson's [53] Example 5.1.3 for lack of reflexivity and Marriott's [38] Example 5.1 for lack of transitivity. Reflexivity and transitivity would seem to be essential requirements to *appr* if the relation is to be used as an ordering on analyses. This motivates the following definition.

Definition. A lattice type $T \in Type$ is *first-order* iff it can be generated by the grammar

$$T ::= D \mid D \to T \mid S \to T$$

where $S \in Stat$ and $D \in Dyn$. ■

For example, $(S \to D) \to D$ is not first-order.

The following proposition says that approximation is transitive for first-order types.

Proposition 4.5 Let $\mathbf{I}$, $\mathbf{I}'$ and $\mathbf{I}''$ be interpretations and let e be a closed expression of first-order lattice type. Then $(\mathbf{I}\ e)\ appr[\Gamma']\ (\mathbf{I}'\ e) \wedge (\mathbf{I}'\ e)\ appr[\Gamma'']\ (\mathbf{I}''\ e) \Rightarrow (\mathbf{I}\ e)\ appr[\Gamma'' \circ \Gamma']\ (\mathbf{I}''\ e)$, where $\Gamma'' \circ \Gamma'$ stands for the concretization family $\{\gamma''_D \circ \gamma'_D \mid D \in Dyn, \gamma'_D \in \Gamma', \gamma''_D \in \Gamma''\}$.

Proof: The proof is by induction on types. In the case of D or $S \to T$, it is straightforward. So assume that the assertion holds for types D and T, and we will show it holds for types $D \to T$. Assume that $v\ appr[\Gamma'' \circ \Gamma']_D\ v''$. Then $v\ appr[\Gamma']_D\ v'$ and $v'\ appr[\Gamma'']_D\ v''$ where $v' = \gamma'_D\ v$. Assume that $u\ appr[\Gamma']_{D \to T}\ u'$ and $u'\ appr[\Gamma'']_{D \to T}\ u''$. Then $(u\ v)\ appr[\Gamma']_T\ (u'\ v')$ and $(u'\ v')\ appr[\Gamma'']_T\ (u''\ v'')$. By the induction hypothesis, $(u\ v)\ appr[\Gamma'' \circ \Gamma']_T\ (u''\ v'')$. It follows that $u\ appr[\Gamma'' \circ \Gamma']_{D \to T}\ u''$. ■

This result is useful because it allows the stepwise development and proof of approximations. At first sight, the restriction to first-order types looks serious, since the proposition does not seem to offer any help if we are working with continuation-based denotational definitions. However, one has to remember that the proposition will only be applied to the semantic functions *for a program as a whole* and the restriction therefore has little impact.

Approximation is also reflexive for first-order types, as there is a natural "identity" approximation.

Definition. Let **I** be an interpretation. The *identity* concretization family for **I** is the concretization family $\Gamma_{Id} = \{\gamma_D\}$ where, for each $D \in Dyn$, $\gamma_D\ x = x$. ■

Proposition 4.6 Let **I** be an interpretation with identity concretization family Γ_{Id} and let e be a closed expression of first-order lattice type. Then $(\mathbf{I}\ e)\ appr[\Gamma_{Id}]\ (\mathbf{I}\ e)$.

Proof: We actually prove that for all first-order lattice types, L, $u\ appr[\Gamma_{Id}]_L\ v$ iff $v \leq u$. The proof is by induction on types.

The base case when $L \in Dyn$ follows from the definition of Γ_{Id}. Consider the case when L is $D \to L'$. Now $u\ appr[\Gamma_{Id}]_{D \to L'}\ v$ iff for all u' and v', $u'\ appr[\Gamma_{Id}]_D\ v' \Rightarrow (u\ u')\ appr[\Gamma_{Id}]_{L'}\ (v\ v')$. By the induction hypothesis, $u\ appr[\Gamma_{Id}]_{D \to L'}\ v$ iff for all u' and v', $v' \leq u' \Rightarrow (v\ v') \leq (u\ u')$, which by monotonicity of u and v, holds iff $v \leq u$. The case when L is $S \to L'$ is similar. ■

In this section we have introduced a general theory of abstract interpretation which is based on a simple meta-language and formalized in terms of concretization functions. The theory carefully separates the two concerns: approximation and implementation. The meta-language is a variant of the typed lambda-calculus and has been carefully chosen so that correctness of approximation lifts from basic expressions to all expressions in the language (Theorem 4.4). This facilitates proofs of correctness.

In general, approximation in this theory is not transitive or reflexive, but we have given a simple condition which ensures that approximation is transitive and reflexive (Proposition 4.5 and Proposition 4.6). This allows us to develop dataflow analyses in a stepwise, derivational manner. In the remainder of the paper we illustrate an application of the theory.

5 SLD resolution: A constraint logic programming view

Interpreters and compilers for logic programming languages are usually based on SLD resolution. Therefore it is reasonable to base the abstract interpretation of such languages on some formalization of SLD resolution. We demonstrate the utility of the language-independent theory of abstract interpretation developed in the last section by using it to give a generic analysis framework for logic programs which captures the SLD semantics.

In this paper we will only be concerned with definite programs [36]. A *definite program*, or *program*, is a finite set of clauses. A *clause* is of the form $H \leftarrow B$ where H, the *head*, is an *atom* and B, the *body*, is a finite sequence of atoms. We let *Var* denote the (countably infinite) set of variables, *Term* the set of terms, *Pred* the set of predicate symbols, *Atom* the set of atoms, *Clause* the set of clauses, and *Prog* the set of (definite) programs.

We assume that we are given a function $vars : (Prog \cup Atom \cup Term) \rightarrow \mathcal{P}\, Var$, such that $(vars\ S)$ is the set of variables that occur in the syntactic object S. A syntactic object S is *ground* iff it is constructed without variables, that is, $vars\ S = \emptyset$.

A *substitution* is an almost-identity mapping $\theta \in Sub \subseteq Var \rightarrow Term$. Substitutions are not distinguished from their natural extensions to other syntactic categories. Our notation for substitutions is fairly standard. For instance $\{x \mapsto a\}$ denotes the substitution θ such that $(\theta\ x) = a$ and $(\theta\ V) = V$ for all variables $V \neq x$. The *restriction* of a substitution θ to a set of variables W, written $\theta|_W$, is the substitution θ' defined by $\theta'\ V$ is $\theta\ V$ if $V \in W$, otherwise it is V. The *domain* of a substitution θ, written $dom\ \theta$, is the set of variables $\{V \in Var \mid \theta\ V \neq V\}$.

A *unifier* of $A, H \in Atom$ is a substitution θ such that $(\theta\ A) = (\theta\ H)$. If such a unifier exists, then A and H are *unifiable*. A unifier θ of A and H is an (idempotent) *most general unifier* of A and H iff $\theta' = \theta' \circ \theta$ for every unifier θ' of A and H. Two atoms A and H have a most general unifier whenever they are unifiable. The auxiliary function $mgu : Atom \rightarrow Atom \rightarrow \mathcal{P}\, Sub$ is defined as follows. If A and H are unifiable, then $(mgu\ A\ H)$ yields a singleton set consisting of a most general unifier of A and H. Otherwise $(mgu\ A\ H) = \emptyset$.

Let $G = \leftarrow A_1, \ldots, A_n$ be a *query* with *selected atom* A_i and let $C = H \leftarrow A'_1, \ldots, A'_k$ be a clause. If A_i and H are unifiable, then

$$\theta\, [\![A_1, \ldots, A_{i-1}, A'_1, \ldots, A'_k, A_{i+1}, \ldots, A_n]\!]$$

is a *resolvent* of G and C with unifier θ, where $\{\theta\} = mgu\ A_i\ H$.

Let P be a definite program and let G be a query. An *SLD derivation* of $P \cup \{G\}$ consists of

- a maximal sequence $G_0, G_1, \ldots$ of queries with $G_0 = G$,
- a sequence $C_0, C_1, \ldots$ of fresh variants of clauses from P (that is, the variables in C_i are consistently replaced by variables not in $C_0, \ldots, C_{i-1}$, or G),
- a sequence $\theta_0, \theta_1, \ldots$ of substitutions,

such that for all i, G_{i+1} is a resolvent of G_i and C_i with unifier θ_i. An SLD derivation may be finite or infinite. Assume it is finite, with final elements G_{n+1}, C_n, and θ_n. Then if G_{n+1} is empty, the derivation is *successful*, otherwise it is *finitely failed*. If it is successful, the *computed answer* is $\theta_n \circ \ldots \circ \theta_0$, restricted to the set of variables occurring in G.

We will, in fact, not need substitutions and unification as defined above until Section 7. Perhaps surprisingly, they play no role in the formal semantics we are about to present. Inspired by constraint

logic languages, we let the role of substitutions be played by term equations. There are several reasons for this, but most importantly:

1. It is simpler to think of term equations ordered by logical consequence than substitutions ordered by some complicated "instantiation" ordering. It also provides a pleasing uniformity in the present context, since, in Section 7, we will "approximate" term equations by propositional formulas (or Boolean functions), again ordered by logical implication.

2. It does away with the awkward directionality of substitutions. Semantically, the distinction between $\{x \mapsto y\}$ and $\{y \mapsto x\}$ is unnecessary and hampers full abstraction.

3. Substitutions do not form a complete lattice and it is common to restrict attention to *idempotent* substitutions. That approach seems unnatural, in particular since the class of idempotent substitutions is not closed under composition, witness $\{x \mapsto f(y)\} \circ \{y \mapsto x\}$.

The other characteristic of our definition is that unification is not only performed when a clause is entered, but also when it is exited. This is to enforce a regime in which "only local variables matter." It reflects the fact that a compiler, optimizing code for a given clause, will mainly need dataflow information expressed in terms of variables local to the clause.

Finally our definition assumes the standard (left-to-right) computation rule.

5.1 Existentially quantified term equations

We now describe the most important semantic domain involved in the definitions to come.

Definition. An *ex-equation* is a possibly existentially quantified conjunction of basic equations $T_1 = T_2$. The conjunction may be empty, in which case we denote it by *true*. We call the set of ex-equations *Eqn*. ■

We consider ex-equations in the context of an alphabet given by some program/query. The semantics of a basic ex-equation is given by the term algebra over that alphabet. Ordering the elements by logical consequence, and considering equivalence classes in the usual way, we obtain a partially ordered set with *true* as the greatest element and *false*, the equivalence class of unsatisfiable elements, as the smallest.

Example 5.1 The ex-equation $\exists\, y\, .\, x = f(y)$ corresponds to the substitution $\{x \mapsto f(y)\}$, and so does the ex-equation $x = f(y)$. The difference between the two is that the latter specifies a relation between two program variables, x and y, whereas the former merely states that x is constrained to take certain forms. Said differently, the *name* y is significant in the latter, but not in the former. We thus have two different kinds of placeholders in terms. ■

We can extend the definition of a "unifier" to ex-equations in a natural way. This provides the link between our semantic definition and the more usual definition using substitutions.

Definition. A *unifier* of ex-equation e is a substitution θ such that $\models (\theta\ e)$. We let *unif* e denote the set of unifiers of e. ■

Thus, θ is a unifier of the atoms A and H iff it is a unifier of the ex-equation $A = H$. Note that application of a substitution to an ex-equation requires that the existentially quantified variables be renamed away from the variables in the substitution, so as to avoid name clashes.

Example 5.2 The ex-equation $\exists\, y\ .\ x = f(y)$ has unifiers $\{x \mapsto f(z)\}$, $\{x \mapsto f(a)\}$, and so on. Unifiers for $x = f(y)$ include $\{x \mapsto f(y)\}$, $\{x \mapsto f(a), y \mapsto a\}$, and $\{x \mapsto f(z), y \mapsto z\}$, but not $\{x \mapsto f(z)\}$ or $\{x \mapsto f(a)\}$. The ex-equation *false* has no unifier. ■

5.2 The base semantics

We now make use of ex-equations to give semantic definition which is suitable as a basis for abstract interpretation and which captures SLD resolution. The definition makes use of the auxiliary functions, *comb*, which corresponds to composition, and *unify*, which corresponds to computing the most general unifier[5].

We shall need a particular kind of variable renaming: A *name toggle* is an involution: a bijection $\rho \in Ren \subset Var \to Var$ which satisfies $\rho = \rho^{-1}$. We do not distinguish a name toggle from its natural extension to atoms and clauses. The function $ren : \mathcal{P}\ Var \to \mathcal{P}\ Var \to Ren$ generates name toggles: $(ren\ U\ W)$ is some name toggle, such that for all V in W, $ren\ U\ W\ V \notin U$. Note that this is renaming of variables in W "away from" U.

Definition. The function $comb : \mathcal{P}\ Eqn \to \mathcal{P}\ Eqn \to \mathcal{P}\ Eqn$ is defined by

$$comb\ E\ E' = \{e \wedge e' \mid e \in E \wedge e' \in E'\}.$$

The function $restrict : \mathcal{P}\ Var \to \mathcal{P}\ Eqn \to \mathcal{P}\ Eqn$ is defined by

$$restrict\ U\ E = \{\exists\, \overline{U}\ .\ e \mid e \in E\}$$

where $\overline{U}$ denotes $(vars\ E) \setminus U$. The function $unify : Atom \to Atom \to \mathcal{P}\ Eqn \to \mathcal{P}\ Eqn$ is defined by

$$unify\ H\ A\ E = restrict\ (vars\ H)\ (comb\ \{H\ = \rho\ A\}\ (\rho\ E))$$

where $\rho = ren\ (vars\ H)\ ((vars\ A) \cup (vars\ E))$. ■

[5] "Corresponds" should be taken in a loose sense: *comb*, unlike composition, is commutative, and *unify* is non-commutative. The commutativity of *comb* restores the intuition of SLD resolution as constraint manipulation, an intuition which is lost with substitutions and their composition. If e and e' are constraints, then "composing" them simply means forming their conjunction. The reason why *unify* is non-commutative will become clear shortly.

Notice that the *calling* atom A is renamed away from the clause head H. The auxiliary functions are defined to operate on *sets* E of conjunctions, rather than single conjunctions, because in the next section it proves useful to have the broader definitions.

Example 5.3 Let e be $\exists\, u\,.\,(y = u \wedge z = f(u))$ and let e' be $y = a$. Then $comb\ \{e\}\ \{e'\}$ is $\{y = a \wedge z = f(a)\}$.

Let $A_1 = p(a, x)$, $A_2 = p(y, z)$, and let e be $\exists\, u\,.\,(y = u \wedge z = f(u))$. Then we have that $(unify\ A_1\ A_2\ \{e\}) = \{x = f(a)\}$. Notice that this ex-equation does not constrain y or z, only variables in A_1 may be constrained. On the other hand we have that $(unify\ A_2\ A_1\ \{e\}) = \{y = a\}$, in which both x and z are unconstrained: With name toggle $\{y \mapsto y', z \mapsto z', y' \mapsto y, z' \mapsto z\}$ we get

$$\begin{array}{lcl} unify\ A_2\ A_1\ \{e\} & = & \{\exists\, y', z'\,.\,(y = a \wedge z = x \wedge \exists\, u\,.\,(y' = u \wedge z' = f(u)))\} \\ & = & \{y = a\}. \end{array}$$

Notice also that $(unify\ A_1\ A_1\ \{e\}) = \{true\}$, while $(unify\ A_2\ A_2\ \{e\}) = \{e\}$.

Let $A_3 = p(f(y), z)$. Then $(unify\ A_3\ A_2\ \{true\}) = \{true\}$. There is no "occur check problem" since variables in A_2 are renamed.

Finally let $A_4 = p(x, x)$. Then $(unify\ A_4\ A_2\ \{e\}) = \emptyset$, corresponding to failure of unification. ■

To summarize: $unify\ H\ A\ \{e\}$ is the result of conjoining $H = A$ with e, then restricting the result to variables in H. As a first step of unification, variables in A and e are consistently renamed so as to avoid collisions with variables in H. Unification can be done with respect to a set E, and $unify\ H\ A\ E$ is then $\{unify\ H\ A\ \{e\} \mid e \in E\}$. Notice how the restriction to variables in H means that *unify* is not symmetric with respect to H and A.

The following definition captures the essence of an SLD refutation-based interpreter using a standard computation rule and a parallel search rule. The domain $Atom$ is ordered by identity, Den is ordered pointwise.

Definition. The *base semantics* has semantic domain

$$Den \quad = \quad Atom \to \mathcal{P}\ Eqn \to \mathcal{P}\ Eqn$$

and semantic functions

$$\begin{array}{lcl} \mathbf{P_{bas}} & : & Prog \to Den \\ \mathbf{C_{bas}} & : & Clause \to Den \to Den \\ \mathbf{B_{bas}} & : & Body \to Den \to (\mathcal{P}\ Eqn) \to (\mathcal{P}\ Eqn). \end{array}$$

It is defined as follows[6].

$$
\begin{array}{lcl}
\mathbf{P_{bas}}\ [\![P]\!] & = & \mathit{lfp}\ (\bigsqcup_{C \in P}(\mathbf{C_{bas}}\ [\![C]\!])) \\
\mathbf{C_{bas}}\ [\![H \leftarrow B]\!]\ d\ A\ E & = & \bigcup_{e \in E} \mathit{comb}\ \{e\}\ (\mathit{unify}\ A\ H\ (\mathbf{B_{bas}}\ [\![B]\!]\ d\ (\mathit{unify}\ H\ A\ \{e\}))) \\
\mathbf{B_{bas}}\ [\![\mathit{nil}]\!]\ d\ E & = & E \\
\mathbf{B_{bas}}\ [\![A : B]\!]\ d\ E & = & \mathbf{B_{bas}}\ [\![B]\!]\ d\ (d\ A\ E). \quad \blacksquare
\end{array}
$$

The statements we are interested in generating from a dataflow analysis are of the form "whenever execution reaches this point, so and so holds." In saying so, we do not actually say that execution does reach the point. In particular, "whenever the computation terminates, so and so holds" concludes nothing about termination. As non-termination is not distinguished from finite failure, we can assume a *parallel* search rule, rather than the customary depth-first rule, thereby simplifying the semantic equations. Owing to the use of a parallel search rule, the execution of a program naturally yields a *set* of answers, as opposed to a sequence.

Example 5.4 Consider the following list concatenation program P:

$$
\begin{array}{l}
\mathit{append}(\mathit{nil}, y, y). \\
\mathit{append}(u : x, y, u : z) \leftarrow \mathit{append}(x, y, z).
\end{array}
$$

and let $A = \mathit{append}(x, y, a : \mathit{nil})$. Execution of P yields two instantiations of the variables in A. We have that $\mathbf{B_{bas}}\ [\![P]\!]\ A\ \{\mathit{true}\} = \{x = \mathit{nil} \wedge y = a : \mathit{nil}, x = a : \mathit{nil} \wedge y = \mathit{nil}\}$. $\blacksquare$

A note about semantical modeling and dataflow analysis may be appropriate at this point. We have defined $\mathbf{B_{bas}}$ such that given a program P and a query A it returns the set of computed answer constraints. That is, $\mathbf{B_{bas}}$ selects what is considered the relevant information from the SLD tree for $P \cup \{\leftarrow A\}$, namely for each success leaf, the conjunction of the constraints that decorate the path from the success leaf to the root. Other information is "forgotten." For example, $(\mathbf{B_{bas}}\ [\![P]\!]\ A)$ contains no information about the length of derivations, the constraints that decorate paths leading to failure nodes, or how variables outside A become constrained during execution.

This is quite in accordance with the common understanding of SLD semantics as the *result* of applying SLD resolution. However, dataflow analysis aims at extracting information about a program's *execution*, that is, about some of the very details that our "SLD semantics" forgets. For example, a dataflow analysis that aims at determining which calls may appear at runtime cannot afford to disregard those paths in the SLD tree that lead to failure. For this reason we need a notion of "extended semantics," in which the calls to a clause (restricted to the local variables in the clause) are collected. It is straightforward to modify the base semantics so that it collects this information. To limit the number of semantic definitions, however, we shall not do this and

[6] Strictly speaking, the singleton set constructor $\{\cdot\}$ as used in the definition is not part of our meta-language, and it is commonly avoided in denotational definitions as it is not monotonic. Its use here causes no problems: the semantic functions are well-defined. Subsequent definitions will avoid using $\{\cdot\}$ so as to be able to utilize Theorem 4.4. Finally, $\bigsqcup_{C \in P}$ is just an abbreviation for the the repeated use of the meta-language's $\sqcup$.

will ignore this issue for the remainder of this paper. Readers should keep in mind, however, that ultimately the touchstone for the correctness of a dataflow analysis returning information about calls to a clause is its soundness with respect to this extended semantics.

At this stage we have given a very simple denotational definition of logic programs which captures the SLD operational semantics. Its simplicity is due to the use of existentially quantified term equations, rather than substitutions, and a parallel, rather than sequential, search rule.

6 Dataflow analysis of logic programs

The semantic definitions given in the previous section have been designed to capture the essence of SLD resolution. In this section we develop a generic dataflow analysis framework from these definitions by factoring out certain operations.

First we introduce some imprecision in the semantics. So far, for all ex-equations generated by a clause, track was kept of the particular ex-equation the clause was called with, so that the meet (conjunction) of generated equations and corresponding call equations could be computed. We now abandon this approach in order to get closer to a dataflow semantics. The point is that, in a dataflow semantics, a "description" x will replace E, the set of "current" ex-equations, and since descriptions will generally be atomic (in the sense of non-decomposable), it makes little sense to refer to *elements* of x. As a first step we thus replace "$\bigcup_{e \in E} \ldots e \ldots$" in the definition of the base semantics by "$\ldots E \ldots$."

Definition. The *lax semantics* has semantic functions

$$\begin{array}{lcl} \mathbf{P_{lax}} & : & \mathit{Prog} \to \mathit{Den} \\ \mathbf{C_{lax}} & : & \mathit{Clause} \to \mathit{Den} \to \mathit{Den} \\ \mathbf{B_{lax}} & : & \mathit{Body} \to \mathit{Den} \to (\mathcal{P}\ \mathit{Eqn}) \to (\mathcal{P}\ \mathit{Eqn}). \end{array}$$

It is defined as follows.

$$\begin{array}{lcl} \mathbf{P_{lax}}\ [\![P]\!] & = & \mathit{lfp}\ (\bigsqcup_{C \in P}(\mathbf{C_{lax}}\ [\![C]\!])) \\ \mathbf{C_{lax}}\ [\![H \leftarrow B]\!]\ d\ A\ E & = & \mathit{comb}\ E\ (\mathit{unify}\ A\ H\ (\mathbf{B_{lax}}\ [\![B]\!]\ d\ (\mathit{unify}\ H\ A\ E))) \\ \mathbf{B_{lax}}\ [\![\mathit{nil}]\!]\ d\ E & = & E \\ \mathbf{B_{lax}}\ [\![A : B]\!]\ d\ E & = & \mathbf{B_{lax}}\ [\![B]\!]\ d\ (d\ A\ E). \quad \blacksquare \end{array}$$

This semantics is only an approximation to $\mathbf{P_{bas}}$, as the following example shows. However, the lack of precision introduced with $\mathbf{P_{lax}}$ is acceptable for the purpose of dataflow analysis: it has no impact on applications of abstract interpretation to programs.

Example 6.1 Consider the program P:

$q(x,y,z) \leftarrow p(x,y), r(x,y,z).$
$p(a,v).$
$p(u,a).$
$r(u,v,v).$

and the query $A = \leftarrow q(x,y,z)$. We have that

$$\mathbf{P_{bas}}\ [\![P]\!]\ A\ \{true\} = \{false, x = a \wedge y = z, y = a \wedge z = a\}.$$

However,

$$\mathbf{P_{lax}}\ [\![P]\!]\ A\ \{true\} = \{false, x = a \wedge y = z, y = a \wedge z = a, x = a \wedge y = a \wedge z = a\}. \quad \blacksquare$$

Proposition 6.1 $\mathbf{P_{lax}}$ *appr* $\mathbf{P_{bas}}$.

Proof: It is not hard to show that $\mathbf{C_{lax}}$ *appr* $\mathbf{C_{bas}}$. The assertion follows by Theorem 4.4. $\blacksquare$

To extract runtime properties of pure Prolog programs one can develop a variety of non-standard interpretations of the preceding semantics. To clarify the presentation, we extract from the lax semantics a *dataflow* semantics which contains exactly those features that are common to all the non-standard interpretations that we want. It leaves the interpretation of one domain X and two base functions, c and u unspecified. These missing details of the dataflow semantics are to be filled in by interpretations. In the standard (lax) interpretation of this semantics, $\mathbf{I_{lax}}$, X is $\mathcal{P}\,Eqn$, c is *comb* and u is *unify*. In a non-standard interpretation, X is assigned whatever set of "descriptions" we choose for approximating sets of ex-equations. So X should be a complete lattice which corresponds to $\mathcal{P}\,Eqn$ in the standard semantics in a way laid down by some insertion $(X, \gamma, (\mathcal{P}\,Eqn))$. The interpretation of c and u should approximate *comb* and *unify* respectively. *Prog*, *Clause*, and *Atom* are static and have the obvious fixed interpretation. They are ordered by identity. As usual, *Den* is ordered pointwise.

Definition. The *dataflow semantics* has domain

$$Den \quad = \quad Atom \to X \to X,$$

semantic functions

$\mathbf{P}$: $Prog \to Den$
$\mathbf{C}$: $Clause \to Den \to Den$
$\mathbf{B}$: $Body \to Den \to X \to X,$

and base functions

$$
\begin{array}{lcl}
c & : & X \to X \to X \\
u & : & \mathit{Atom} \to \mathit{Atom} \to X \to X.
\end{array}
$$

It is defined as follows.

$$
\begin{array}{lcl}
\mathbf{P}\ [\![P]\!] & = & \mathit{lfp}\ (\bigsqcup_{C \in P}(\mathbf{C}\ [\![C]\!])) \\
\mathbf{C}\ [\![H \leftarrow B]\!]\ d\ A\ x & = & c\ x\ (u\ A\ H\ (\mathbf{B}\ [\![B]\!]\ d\ (u\ H\ A\ x))) \\
\mathbf{B}\ [\![\mathit{nil}]\!]\ d\ x & = & x \\
\mathbf{B}\ [\![A : B]\!]\ d\ x & = & \mathbf{B}\ [\![B]\!]\ d\ (d\ A\ x). \quad \blacksquare
\end{array}
$$

An interpretation $\mathbf{I_x}$ for the dataflow semantics is determined by the triple $((\mathbf{I_x}\ X), (\mathbf{I_x}\ c), (\mathbf{I_x}\ u))$. We use the convention that the semantic function $\mathbf{P}$ as determined by an interpretation $\mathbf{I_x}$ is denoted by $\mathbf{P_x}$. For example the standard interpretation $\mathbf{I_{lax}}$ is $((\mathcal{P}\ \mathit{Eqn}), \mathit{comb}, \mathit{unify})$ and the corresponding semantics is denoted by $\mathbf{P_{lax}}$.

Since $\mathbf{C}\ [\![C]\!]$ is monotonic for every clause C and every interpretation, we have the following proposition.

Proposition 6.2 For every interpretation $\mathbf{I_x}$, $\mathbf{P_x}$ is well-defined. ■

Definition. Let $\mathbf{I} = (X, c, u)$ and $\mathbf{I'} = (X', c', u')$ be interpretations. Then $\mathbf{I'}$ is *sound* with respect to $\mathbf{I}$ iff for some insertion (X', γ, X), $c'\ \mathit{appr}\ c$ and $u'\ \mathit{appr}\ u$. ■

The next result follows immediately from Theorem 4.4.

Corollary 6.3 If interpretation $\mathbf{I_x}$ is sound with respect to $\mathbf{I_y}$, then $\mathbf{P_x}\ \mathit{appr}\ \mathbf{P_y}$. ■

By Proposition 4.5 and Proposition 6.1 we therefore have the following theorem.

Theorem 6.4 If interpretation $\mathbf{I_x}$ is sound with respect to $\mathbf{I_{lax}}$, then $\mathbf{P_x}\ \mathit{appr}\ \mathbf{P_{bas}}$. ■

Developing a dataflow analysis in this framework is therefore a matter of choosing the description domain so that it captures the information required from the analysis and then defining suitable functions to approximate *comb* and *unify*. Before giving example dataflow analyses we identify two classes of description domain and indicate how *comb* can be approximated for these classes. This is useful because the descriptions used in most dataflow analyses belong to one of the two classes or are an orthogonal mixture of such descriptions. Thus finding generic ways to approximate *comb* for these classes will help to give some insight into the design of practical dataflow analyses. We note that once a suitable approximation for *comb* has been found, then, by the definition of *unify*, it may be used as the basis for developing an approximation to *unify*.

Definition. An insertion $(X, \gamma, (\mathcal{P}\ \mathit{Eqn}))$ is *downwards closed* iff for all $x \in X$ and $e, e' \in \mathit{Eqn}$, $(e \in \gamma\ x \wedge e' \models e)$ implies $e' \in \gamma\ x$. An insertion $(X, \gamma, (\mathcal{P}\ \mathit{Eqn}))$ is *upwards closed* iff for all $x \in X$ and $e, e' \in \mathit{Eqn}$, $(e \in (\gamma\ x) \setminus \{\mathit{false}\} \wedge e \models e')$ implies $e' \in \gamma\ x$. ■

Examples of downwards closed insertions are those typically used in groundness analysis, type analysis, definite aliasing and definite sharing analysis. Examples of upwards closed insertions are those typically used in possible sharing (independence) analysis, possible aliasing analysis, and freeness analyses. Many complex analyses, such as for the determination of mode statements or the detection of and-parallelism, can be expressed as a combination of simpler analyses based on insertions that are downwards or upwards closed.

A notion of "substitution closure," which is similar to, but more restrictive than downwards closure, is identified by Debray [15] as being the basis for an important class of dataflow analyses. Substitution closure is motivated by considerations of efficiency of dataflow analyses, and effectively limits the precision of analyses by barring the propagation of "aliasing" or "sharing" information in analyses.

Proposition 6.5 Let $(X, \gamma, (\mathcal{P}\, Eqn))$ be a downwards closed insertion and let $comb' : X \to X \to X$ be given. Then $comb'$ *appr* $comb$ iff

$$\forall\, x, x' \in X\, .\, (\gamma\ x) \cap (\gamma\ x') \subseteq \gamma\ (comb'\ x\ x').$$

Proof: We have that

$$\begin{array}{ll} & comb' \ appr \ comb \\ \Leftrightarrow & \forall\, x, x' \in X\, .\, \forall\, E, E' \subseteq Eqn\, .\, E \subseteq (\gamma\ x) \wedge E' \subseteq (\gamma\ x') \Rightarrow (comb\ E\ E') \subseteq \gamma\ (comb'\ x\ x') \\ \Leftrightarrow & \forall\, x, x' \in X\, .\, \forall\, e \in (\gamma\ x)\, .\, \forall\, e' \in (\gamma\ x')\, .\, (e \sqcap e') \in \gamma\ (comb'\ x\ x') \\ \Leftrightarrow & \forall\, x, x' \in X\, .\, (\gamma\ x) \cap (\gamma\ x') \subseteq \gamma\ (comb'\ x\ x'). \quad \blacksquare \end{array}$$

Definition. An insertion $(X, \gamma, (\mathcal{P}\, Eqn))$ is *Moore-closed* iff $\{\gamma\ x \,|\, x \in X\}$ is Moore-closed in $\mathcal{P}\, Eqn$. ■

Corollary 6.6 Let $(X, \gamma, (\mathcal{P}\, Eqn))$ be a downwards closed, Moore-closed insertion. Let $\sqcap_X$ be the meet operator on X. Then $\sqcap_X$ *appr* $comb$ (and in fact is the best approximation). ■

Let us sum up the results of this section. To define a dataflow analysis one needs to lay down a complete (for termination preferably Noetherian) lattice X of "descriptions." These descriptions should be designed so as to convey the desired kind of dataflow information. The information contents of a description should be specified by a function γ in such a way that $(X, \gamma, (\mathcal{P}\, Eqn))$ is an "insertion." One should also define a function $c : X \to X \to X$ which correctly emulates conjunction of ex-equations (or composition of substitutions) and a function $u : Atom \to Atom \to X \to X$ which correctly emulates unification of atoms in the presence of an ex-equation (or current substitution). That is, one must provide an "interpretation" (X, c, u) which is "sound." The result is a definition of a dataflow analysis which is automatically correct.

As an example, we give in the following section a sound interpretation which specifies a very precise, non-trivial "groundness" analysis.

7 Groundness analysis using Boolean functions

In this section we give an example dataflow analysis for groundness propagation. This analysis is based on the scheme given in the previous section. Certain Boolean functions are used as descriptions. Since the analysis is intimately dependent on the nature of variables in a logic programming language, let us briefly consider the role of variables.

A variable in a logic programming language is very different from a variable in an imperative or functional programming language. It is sometimes referred to as a "logical variable" and characterized as "constrain-only." This is because, as we have seen, execution of a logic program proceeds by steps that continually narrow the set of possible values that a variable may take.

This characteristic of the execution of logic programs makes dataflow analyses harder in some ways, but it also opens up new views of some analysis problems. For example it suggests the possibility of propagating conditional invariants of the form "*From this point on*, if x has (ever gets) property p, then y has (will have) property r." Example 7.7 will make it clearer what we mean by this "projecting into the future," but first we need to explain how dependency information can be represented. A statement such as "x is ground" may be represented by a propositional variable x. Groundness (or other) dependencies may then be represented by Boolean functions, such as that denoted by $y \rightarrow x$.

Since groundness and other interesting properties are not decidable, a dataflow analysis which operates in finite time can only give approximate information, in general. The statements that it produces will carry a modality, as in "x is inevitably ground" or "x is possibly ground." For this reason, only the *positive* Boolean functions are useful. If we associate the meaning "x is inevitably ground" with the formula x, then $\neg x$ would mean "x may not always be ground" and this conveys no information at all, that is, exactly the information conveyed by the function *true*.

Definition. A *Boolean function* is a function $F : Bool^n \rightarrow Bool$. We call the set of all n-ary Boolean functions $Bfun_n$ and let it be ordered by logical consequence ($\models$). The function F is *positive* iff $F(true, \ldots, true) = true$. We denote the set of positive Boolean functions of n variables by Pos_n. ■

For simplicity we will assume that we have some fixed number n of variables and leave out subscripts and the phrase "of n variables." The set of propositional variables $\{x_1, \ldots, x_n\}$ will be referred to as $Pvar$. We shall also use propositional formulas as representations of Boolean functions without worrying about the distinction. Thus we may speak of a formula as if it were a function and in any case denote it by F. As a reminder of the fact that a propositional formula is only one of a class which all represent a given Boolean function, we put square brackets around propositional formulas and think of the result as the class of equivalent formulas. By a slight abuse of notation we sometimes apply logical connectives to these classes of equivalent formulas. We sometimes refer to the formulas as *groundness dependency formulas*.

It is well known that *Bfun* is a Boolean lattice and in fact *Pos* forms a Boolean sublattice of

Bfun. In terms of propositional formulas, meet and join are given by conjunction and disjunction, respectively. In the context of a finite set *Pvar* of propositional variables, the complementation operation on *Pos* is given by $\dot{\neg} F = F \leftrightarrow \bigwedge Pvar$, see [9]. (Here and in the following we use the notation $\bigwedge\{\phi_1, \ldots, \phi_n\}$ for the formula $\phi_1 \wedge \ldots \wedge \phi_n$, and similarly for $\bigvee$.)

Logicians have of course studied *Pos* under several different names. However, the history of dependency clauses for dataflow analysis is rather short. Dart used a class of dependency formulas in his work in the area of deductive databases [13, 14]. Dart's class is strictly less expressive than *Pos*, which was suggested by Marriott and Søndergaard [41] (under the less suggestive name '*Prop*') and further studied by Cortesi *et al.* [9].

One can imagine many types of properties of dataflow information for which dependency formulas is a useful formalism. Here we are concerned with groundness. As an example, if the constraint $x = f(y, z)$ is generated during query evaluation, the relationship $x \leftrightarrow (y \wedge z)$ is deduced. Informally the formula says that if x is (becomes) ground then so is (does) both of y and z, and *vice versa*. Example 7.7 shows how this kind of information may be useful.

Syntactically *Pos* has several interesting characterizations. For example (and surprisingly) it consists of exactly those Boolean functions that can be represented by propositional formulas using only the connectives $\rightarrow$ and $\leftrightarrow$.

Example 7.1 The Boolean function $[\neg x]$ is not in *Pos*. The function $[x \rightarrow y]$ is in *Pos*. In terms of $\wedge$ and $\leftrightarrow$ we could write it as $[x \leftrightarrow (x \wedge y)]$. ■

< *Figure* 5 >

It is convenient to include the (non-positive) Boolean function *false* as an approximation to the empty set of ex-equations. So from here on we deal with the the domain $Pos_\perp = Pos \cup \{false\}$, ordered by logical consequence. Figure 5 shows $Pos_\perp$ in the dyadic case. The idea with using $Pos_\perp$ is that an ex-equation e is described by $\phi \in Pos_\perp$ exactly in case that, for every unifier θ of e, the truth assignment corresponding to the variables ground by θ satisfies ϕ.

Definition. For a substitution θ, let *grounds* θ be the truth assignment which maps a variable to true if θ grounds the variable and to false otherwise. That is, $grounds : Sub \rightarrow Var \rightarrow Bool$ is defined by

$$grounds\ \theta\ V \Leftrightarrow vars\ (\theta\ V) = \emptyset.$$

The concretization function $\gamma : Pos_\perp \rightarrow (\mathcal{P}\ Eqn)$ is defined by

$$\gamma\ \phi = \{e \in Eqn \mid \forall\, \theta \in unif\ e\ .\ (grounds\ \theta) \models \phi\}.$$ ■

This concretization function maps $\phi \in Pos_\perp$ to the set of ex-equations e which have the property that, no matter how they further become constrained to some e', the groundness formula corresponding to e' satisfies ϕ.

Example 7.2 The Boolean function $[x \leftrightarrow y]$ describes both of the ex-equations $x = a \wedge y = b$ and $\exists\, u' \,.\, (x = u' \wedge y = u' \wedge u = u')$, but not the ex-equation $x = a$. However, $[x \leftrightarrow y]$ is not the *best* description for $x = a \wedge y = b$. For this ex-equation, the best description is $[x \wedge y]$ which in turn has $[x \leftrightarrow y]$ as a logical consequence. That is, $[x \leftrightarrow y]$ is a less precise approximation than $[x \wedge y]$.

As a further example, let $\phi = [x \wedge (y \leftrightarrow z)]$. Then $(x = a \wedge y = f(z))$ is approximated by ϕ but $(x = a \wedge y = f(a))$ is not. ■

Lemma 7.1 The triple $(Pos_\perp, \gamma, (\mathcal{P}\, Eqn))$ is a downwards closed, Moore-closed insertion.

Proof: Clearly γ is monotonic and co-strict, and $(Pos_\perp, \gamma, (\mathcal{P}\, Eqn))$ is downwards closed. Let $\Phi \subseteq Pos_\perp$. Then $\bigwedge\, \Phi \in Pos_\perp$ and $\gamma\ (\bigwedge\, \Phi) = \bigcap_{\phi \in \Phi} (\gamma\ \phi)$, so $(Pos_\perp, \gamma, (\mathcal{P}\, Eqn))$ is Moore-closed. ■

It follows from Corollary 6.6 that *comb* is best approximated by conjunction.

Definition. The function $comb_{gro} : Pos_\perp \to Pos_\perp \to Pos_\perp$ is defined by $comb_{gro}\ \phi\ \phi' = \phi \wedge \phi'$. ■

Lemma 7.2 $comb_{gro}$ *appr* $comb$. ■

The function *unify* is somewhat more complex to approximate. Its definition makes use of $restrict_{gro}$, a projection function on propositional formulas and mgu_{gro}, the analogue of *mgu* for propositional formulas. The motivation for approximating *unify* in this way comes directly from its definition.

Because $Pos_\perp$ is downwards closed we can approximate existential quantification of equations by existential quantification on Boolean functions.

Definition. The function $restrict_{gro} : (\mathcal{P}\ Var) \to Pos_\perp \to Pos_\perp$ is defined by

$$restrict_{gro}\ U\ \phi = \exists\, \overline{U}\ .\ \phi. \quad ■$$

This is well defined because positive Boolean functions are closed under existential quantification. In particular, $\exists\, X\ .\ \phi = \{X \mapsto true\}\ \phi \vee \{X \mapsto false\}\ \phi$ (which also explains *why* $Pos_\perp$ is closed under existential quantification).

Example 7.3 We have

$$\begin{aligned} restrict_{gro}\ \{x, y, z\}\ [x \wedge (y \leftrightarrow v) \wedge (z \leftrightarrow v)] &= [x \wedge y \wedge z] \vee [x \wedge \neg y \wedge \neg z] \\ &= [x \wedge (y \leftrightarrow z)]. \quad ■ \end{aligned}$$

Lemma 7.3 $restrict_{gro}$ *appr* $restrict$.

Proof: By the definition of *restrict*, we must show that if $e \in \gamma\ \phi$ then $(\exists\, \overline{U}\,.\, e) \in \gamma\ (restrict_{gro}\ U\ \phi)$. This holds since

$$\begin{array}{lcl} e \in \gamma\ \phi & \Rightarrow & \forall\, \theta \in unif\ e\,.\,(grounds\ \theta) \models \phi \\ & \Rightarrow & \forall\, \theta \in unif\ e\,.\,(grounds\ \theta|_U) \models \exists\, \overline{U}\,.\,\phi \\ & \Rightarrow & \forall\, \theta \in unif\ (\exists\, \overline{U}\,.\, e)\,.\,(grounds\ \theta|_U) \models \exists\, \overline{U}\,.\,\phi \\ & \Rightarrow & \forall\, \theta \in unif\ (\exists\, \overline{U}\,.\, e)\,.\,(grounds\ \theta) \models \exists\, \overline{U}\,.\,\phi \\ & \Rightarrow & (\exists\, \overline{U}\,.\, e) \in \gamma\ (restrict_{gro}\ U\ \phi). \quad \blacksquare \end{array}$$

Definition. The function $mgu_{gro} : Atom \to Atom \to Pos_\perp$ is defined by

$$\begin{array}{lcl} mgu_{gro}\ A\ H & = & \text{if } (mgu\ A\ H) = \emptyset \text{ then } false \text{ else let } \{\mu\} = (mgu\ A\ H) \text{ in} \\ & & [\bigwedge \{\, V \leftrightarrow (\bigwedge \{\, V' \mid V' \in (vars\ (\mu\ V))\})\} \mid V \in dom\ \mu\}]. \quad \blacksquare \end{array}$$

Example 7.4 Let $A = p(x, y)$ and $H = p(a, f(u, v))$. Then $mgu_{gro}\ A\ H = [x \wedge (y \leftrightarrow (u \wedge v))]$. ■

Lemma 7.4 $(mgu_{gro}\ A\ H)\ appr\ \{A = H\}$.

Proof: The case when A and H are not unifiable is immediate. Otherwise consider some $V \in dom\ \mu$ where μ is a most general unifier of A and H. Let $T = \mu\ V$. Now, $\theta \in unif\ [\![A = H]\!]$ implies that $\theta\ V = \theta\ T$. Thus $vars\ (\theta\ V) = \emptyset$ iff for all $V' \in (vars\ T), vars\ (\theta\ V') = \emptyset$. Thus, $[V \leftrightarrow (\bigwedge \{\, V' \mid V' \in (vars\ (\mu\ V))\})]$ approximates μ. The result follows from the fact that $Pos_\perp$ is Moore-closed. ■

Definition. The function $unify_{gro} : Atom \to Atom \to Pos_\perp \to Pos_\perp$ is defined by

$$\begin{array}{lcl} unify_{gro}\ H\ A\ \phi & = & \text{let } \rho = ren\ (vars\ H)\ ((vars\ A) \cup (vars\ \phi)) \text{ in} \\ & & restrict_{gro}\ (vars\ H)\ ((\rho\ \phi) \wedge (mgu_{gro}\ H\ (\rho\ A))). \quad \blacksquare \end{array}$$

Lemma 7.5 $unify_{gro}\ appr\ unify$.

Proof: This follows from the definition of *unify*, Theorem 4.4 and Lemmas 7.2–7.4. ■

Example 7.5 Let $A = append(x, y, z)$, $H = append(nil, y, y)$, and $H' = append(u : x, y, u : z)$. Then

$$\begin{array}{lcl} unify_{gro}\ H\ A\ [true] & = & [true] \\ unify_{gro}\ A\ H\ [true] & = & [x \wedge (y \leftrightarrow z)] \\ unify_{gro}\ H'\ A\ [true] & = & [true] \\ unify_{gro}\ A\ H'\ [false] & = & [false] \\ unify_{gro}\ A\ H'\ [x \wedge (y \leftrightarrow z)] & = & [(x \wedge y) \leftrightarrow z]. \end{array}$$

To see how the last result comes about, consider the most general unifier of A and H' (after application of a name toggle): $\{x \mapsto u^\# : x^\#, y \mapsto y^\#, z \mapsto u^\# : z^\#\}$. We have that

$$mgu_{gro}\ A\ H' = [(x \leftrightarrow (u^\# \wedge x^\#)) \wedge (y \leftrightarrow y^\#) \wedge (z \leftrightarrow (u^\# \wedge z^\#))].$$

Conjoining the formula $[x \wedge (y \leftrightarrow z)]$ (after name toggling), we get

$$[(x \leftrightarrow (u^\# \wedge x^\#)) \wedge (y \leftrightarrow y^\#) \wedge (z \leftrightarrow (u^\# \wedge z^\#)) \wedge x^\# \wedge (y^\# \leftrightarrow z^\#)].$$

We need to restrict this to the set $\{x, y, z\}$. "Projecting away" $x^\#$ yields

$$[(x \leftrightarrow u^\#) \wedge (y \leftrightarrow y^\#) \wedge (z \leftrightarrow (u^\# \wedge z^\#)) \wedge (y^\# \leftrightarrow z^\#)].$$

Projecting $y^\#$ away yields $[(x \leftrightarrow u^\#) \wedge (y \leftrightarrow z^\#) \wedge (z \leftrightarrow (u^\# \wedge z^\#))]$ and projecting $u^\#$ away then yields $[(y \leftrightarrow z^\#) \wedge (z \leftrightarrow (x \wedge z^\#))]$. Finally, projecting $z^\#$ away yields $[z \leftrightarrow (x \wedge y)]$. ■

Definition. The *groundness analysis* $\mathbf{P_{gro}}$ is given by instantiating the dataflow semantics with the interpretation $(Pos_\perp, comb_{gro}, unify_{gro})$. ■

Theorem 7.6 $\mathbf{P_{gro}}$ *appr* $\mathbf{P_{bas}}$.

Proof: This follows immediately from Lemma 7.1, Lemma 7.2, Lemma 7.5, and Theorem 6.4. ■

Example 7.6 Let P be the *append* program

$$append(nil, y, y).$$
$$append(u : x, y, u : z) \leftarrow append(x, y, z).$$

Consider the query $A = \leftarrow append(x, y, z)$. To compute $\mathbf{P_{gro}}\ [\![P]\!]\ A\ [true]$, the analysis proceeds as follows. Let $d_P = \bigsqcup_{C \in P}(\mathbf{C_{gro}}\ [\![C]\!])$. We then have

$$\begin{array}{lcll} (d_P \uparrow 0)\ A\ [true] & = & [false] & \\ (d_P \uparrow 1)\ A\ [true] & = & [x \wedge (y \leftrightarrow z)] \vee [false] & = [x \wedge (y \leftrightarrow z)] \\ (d_P \uparrow 2)\ A\ [true] & = & [x \wedge (y \leftrightarrow z)] \vee [(x \wedge y) \leftrightarrow z] & = [(x \wedge y) \leftrightarrow z] \end{array}$$

and $(d_P \uparrow 3) = (d_P \uparrow 2) = lfp\ d_P$. Thus $\mathbf{P_{gro}}\ [\![P]\!]\ A\ [true] = [(x \wedge y) \leftrightarrow z]$. Similarly one can show that $\mathbf{P_{gro}}\ [\![P]\!]\ A\ [z] = [x \wedge y \wedge z]$. In the "extended" version of $\mathbf{P_{gro}}$, we find that, provided this holds in the initial call, all calls to *append* will have a third argument which is inevitably ground. ■

Example 7.7 Consider the following (naive) program R to reverse lists:

$$rev(nil, nil).$$
$$rev(x : y, z) \leftarrow append(u, x : nil, z), @rev(y, u).$$

Consider the query $A' = rev(x, y)$ and assume that we are interested in queries of that form with x being ground. A first approximation, $[x \wedge y]$, is obtained by considering the fact $rev(nil, nil)$:

$$\begin{aligned}(d_R \uparrow 0)\ A'\ [x] &= [false] \\ (d_R \uparrow 1)\ A'\ [x] &= [x \wedge y].\end{aligned}$$

That is, so far it looks as if the query will result only in answers with x and y ground, but this may well be revised in a subsequent approximation step.

In processing the recursive clause, we use the approximation already obtained for *append*. In terms of the variables in R, the approximation is $[(u \wedge x) \leftrightarrow z]$. Conjoining this with the "current constraint" $[x \wedge y]$, we arrive (after simplification) at the formula

$$\phi : [x \wedge y \wedge (z \leftrightarrow u)]$$

as the approximation which holds at the program point marked @. It expresses that x and y will be ground and that z is (or will become) ground iff u is (will). This relation between z and u is what we had in mind when saying that invariants may be "projected into the future."

We now see the value of this: The (current) formula for the last atom in the clause is $[y \wedge u]$ (from $d_R \uparrow 1$), and conjoining this with ϕ we get, after simplification, $[x \wedge y \wedge z \wedge u]$. In terms of the variables in the query this translates (after restriction) to $x \wedge y$, that is,

$$(d_R \uparrow 2)\ A'\ [x] = [x \wedge y].$$

We conclude that $[x \wedge y]$ is a fixpoint, that is, y will indeed become ground in every answer, assuming that x was. This information in turn can be translated into information about calls. It says that if *rev* is queried with a ground first argument, all the generated calls to *rev* will have a ground first argument. ■

The details of implementing the groundness analysis are beyond the scope of this paper. The important choice is how to represent Boolean functions in a way that supports their efficient manipulation. Le Charlier and Van Hentenryck [35] use ordered binary-decision diagrams [7] for the purpose and report very good results, both as regards precision and efficiency of the analysis. Marriott and Søndergaard [42] show that a groundness analysis using *Pos* has the property that queries need only be analyzed in their most general form—analysis of instances can be done simply by conjoining elements in *Pos*, speeding up the analysis (this is related to Jacobs and Langen's "condensing" [24]). Codish and Demoen [8] report good results with their implementation of *Pos* which is based on an "abstract compilation" approach, that is, on the generation of a constraint program whose execution in turn corresponds to the dataflow analysis.

8 Implementation issues

The denotational equations given in this paper can be considered *definitions* of logic program semantics ($\mathbf{P}_{\mathbf{bas}}$) and of dataflow analyses (the instances of $\mathbf{P}$), presented in the same formal language. What is being defined is orthogonal to the ways in which it may be computed, and the equations in themselves contain little commitment as to how one could implement the dataflow analyses. Indeed, one of the purposes of this paper is to show how the orthogonal issues of approximation and implementation can (and should) be kept separate, as depicted in Figure 3.

Read naively, the equations specify a highly redundant way of computing certain mathematical objects. On the other hand, the denotational definitions can be given a "call-by-need" reading which guarantees that the same partial result is not repeatedly recomputed and only computed at all if it is needed for the final result. Such readings are independent of *what* is being defined, and a reader is free to choose whichever is desired. In fact, with such a call-by-need reading the definition of $\mathbf{P}$ is, modulo syntactic rewriting, a working implementation of a generic dataflow analyzer written in a functional programming language [20]. In programming languages which do not support a call-by-need semantics, implementation is somewhat harder.

The direct implementation obtained from "running the definition" is interpretive and not very efficient. Hermenegildo *et al.* [23] suggest that analysis can be sped up by specializing an abstract interpreter to a given source program, thus in effect performing "abstract compilation." The same idea is implicit in earlier work on abstract interpretation. For example, Mycroft [49] performs strictness analysis by generating functional programs that compute Boolean values which in turn provide the desired strictness information.

In the remainder of this section we sketch a traditional interpretive implementation[7]. This is instructive because it shows the close relationship between our semantic definition and other generic analyzers (written in C or Prolog) based on the AND/OR tree framework of Bruynooghe *et al.* [3, 6].

To avoid redundant computations, the result of invoking atom A in the context of description x should be recorded. Such memoing can be implemented using function graphs. The function graph for a function f is the set of pairs $\{(x,f(x)) \mid x \in dom\ f\}$ where $dom\ f$ denotes the domain for f. The computation of a function graph is best done in a demand-driven fashion: we only compute as much of it as is necessary in order to answer a given query. This corresponds to the "minimal function graph" semantics used by Jones and Mycroft [29].

However, matters are complicated by the fact that we are performing a fixpoint computation. Recall that we want to compute a partial function $d : Atom \to X \to X$. Thus for each atom A in the program or query, we must keep a function graph mapping each "input" description x to the corresponding "output" description $x' = d\ A\ x$. However, as the function definition is recursive,

[7] Since it is really the collecting semantics which must be approximated, a dataflow analysis is seen as a fixpoint computation over a domain of *annotations* of a given program. An annotation is a mapping from the set of program points to the lattice of descriptions used, and the computation continues as long as a new description is found to obtain at some program point.

we must compute the result by means of the function's Kleene sequence. This means that the (partial) function graph that we compute does not simply correspond to a function that becomes more and more defined; the result corresponding to input x may well be revised several times as we go. An example is given by the computation of $d\ A\ x$ in Example 7.6 where $A = \mathit{append}(x, y, z)$ and $x = \mathit{true}$: at one stage the value is assumed to be $[x \wedge (y \leftrightarrow z)]$, but later this is revised to $[(x \wedge y) \leftrightarrow z]$.

This means that the function graph cannot be used (as might have been hoped) to simply look up values $d\ A\ x$. Rather, we must organize the computation such that a request for $d\ A\ x$ is always taken as a request to *recompute* this value, and only if that computation leads to a recursive request for $d\ A\ x$ will the current value be used, that is, a simple look-up is performed.

Another, less important, way to improve efficiency, is to only compute the function graph "modulo variable renaming." The reason we can do this is that the meaning of a program is independent of variable names in the following sense:

Proposition 8.1 Let ρ be a name toggle. Then $\rho\,(\mathbf{P}_{\mathbf{bas}}\,[\![P]\!]\ A\ E) = \mathbf{P}_{\mathbf{bas}}\,[\![P]\!]\,(\rho\ A)\,(\rho\ E)$. ■

Thus in an implementation we do not want to distinguish, for example, the calls $(p(x, f(y, x)), \{x \mapsto y\})$ and $(p(u, f(v, u)), \{u \mapsto v\})$. The simplest solution is to annotate variables with numbers as they are met, starting from 1, and to refer to them through these numbers. For example, the two calls above are both referred to as $(p(1, f(2, 1)), \{1 \mapsto 2\})$.

Other avenues are open for improving the efficiency of a generic dataflow analyzer:

- A certain amount of partial evaluation can be performed to speed up the fixpoint computation. For example, a given body atom will be unifiable with a fixed set of clause heads, and the relevant clauses should not be looked up repeatedly. Rather, each atom should be annotated with the clauses it may successfully call, and the corresponding most general unifiers.

- Le Charlier, Musumbu and Van Hentenryck [34] suggest maintaining a (dynamic) dependency graph for the following reason: Updating an entry in the function graph will not necessarily mean that every other entry has to be recomputed, and it is in fact possible to keep track of which other entries will be affected. If a functional programming language is used, the graph need not even be explicit—proper use of continuations can achieve the same effect with less effort on the implementor's part, though possibly less efficiently [20]. More specifically, rather than yielding a result description x' only, $d\ A\ x$ should return a pair (x', k), where k is a continuation. The idea is that k is invoked whenever x' is revised, automatically causing entries that depend on $d\ A\ x$ to be recomputed.

- The monotonicity of the mapping $d\ A$ can be utilized in the following way: Whenever the value of $d\ A\ x$ gets updated to x', we know that the values of $d\ A\ x''$ for $x \sqsubseteq x''$ must be at least x', and we can therefore update each such entry to $x' \sqcup y$, where y is its current value. Similarly, when it is discovered that a new entry $d\ A\ x$ is needed (that is, its value is not $\bot$),

we may look up all the values of $d\ A\ x'$ for $x' \sqsubseteq x$ and use their least upper bound as the initial value for $d\ A\ x$. To make these kinds of consequential update fast, Le Charlier, Musumbu and Van Hentenryck arrange input descriptions as a Hasse graph, that is, a structure which directly reflects the partial ordering of the descriptions.

9 Related work

An indication of the usefulness and wide applicability of abstract interpretation for logic programming is the amount of work published on the topic in recent years. A recent special issue of *Journal of Logic Programming* (1992) has been devoted to the topic and we refer readers to the extensive bibliography of P. and R. Cousot [11].

In particular obtaining information about calls to clauses by approximating the SLD semantics (as studied in this paper) seems useful, as many kinds of code improvement that can be performed automatically by a compiler depend on information about calls that may take place at run time, and other kinds of program transformation make use of that information as well.

A number of papers in the area have been concerned with generic frameworks for abstract interpretation of logic programs. By this is usually meant a general setting that allows one to express a number of dataflow analyses in a uniform way, just as we have done in the present paper through our "dataflow semantics." Almost all of these frameworks approximate the SLD semantics. We now compare our semantic definitions to other denotational SLD-based definitions,and our framework to other generic analysis frameworks.

Early work on SLD-based semantic definitions for logic programs was done by Jones and Mycroft [28] who addressed both operational and denotational semantics. Debray and Mishra [17] gave a thorough exposition of a denotational definition, including a proof of its correctness with respect to SLD. Both Jones and Mycroft and Debray and Mishra assume a left-to-right computation rule and a depth-first search of SLD trees (as in Prolog), and both definitions capture non-termination (unlike ours). Both use *sequences* of substitutions as denotations, rather than sets, which give the definitions a rather different flavor. The definition used by Jones and Søndergaard [30] achieves certain simplifications by assuming a parallel search rule and consequently manipulates *sets* of substitutions. The use of substitutions forces it to employ an elaborate renaming technique which complicates semantic definitions somewhat. Winsborough [61, 62] and Jacobs and Langen [24] have suggested denotational definitions along similar lines. Marriott and Søndergaard [43] have given a uniform presentation of both "bottom-up" (that is, T_P-style [2]) and "top-down" (SLD-based) definitions by expressing both in terms of operations on lattices of substitutions, as far as this is possible. In particular they showed that operations such as unification and composition of substitutions can be adequately dissolved into lattice operations to simplify definitions, an idea which has formed the point of departure for the definitions presented here.

Abstract interpretation of logic programs was first mentioned by Mellish [46] who suggested it as

a way to formalize mode analysis[8]. An occur check analysis which was formalized as a non-standard semantics was given by Søndergaard [58]. Some of the techniques used in the present paper can be traced back to that work. This is the case with the principle of performing unification both on call and return so as to facilitate that only local variables need be manipulated at any stage (this was referred to as a principle of "locality"). The work also established the principle of binding information to *variables* in a program throughout computations, rather than to argument positions as is more usual in other frameworks [3, 37, 47].

Other things being equal, this improves precision. For example, consider a mode analysis of the program

$$\leftarrow p(f(x)).$$
$$p(f(u)).$$

using the two modes "free" (unbound or bound to a variable) and "any." The "argument position" methods will funnel mode information about the variables x and u through the argument position of p and assign x the mode "any," while clearly x could be more precisely deemed "free." To counteract such behavior, an "argument position" method must use more fine-grained descriptions and pay the price of more expensive "abstract operations."

A framework for the abstract interpretation of logic programs was first given by Mellish [47]. Mellish's semantics is an operational parallel to our "lax" semantics with the imprecision that this implies: success patterns are not associated with their corresponding call patterns, so success information is propagated back, not only to the atom that actually called the clause, but to all atoms that unify with the clause's head. The application that had Mellish's interest in particular was mode analysis. Debray [16] subsequently investigated this application in more detail and pointed to a problem in Mellish's application (the so-called aliasing problem, which may manifest itself as either a soundness or a completeness problem, depending on the particular dataflow analysis).

A framework for the abstract interpretation of logic programs based on a denotational definition of SLD was given by Jones and Søndergaard [30]. This was the first denotational approach to abstract interpretation of logic programs, and the first paper in the area to apply the idea of a generic dataflow algorithm with a few basic operations being parameters. The framework allowed even the base (or standard) semantics to be expressed as an instance of the dataflow semantics. This has the advantage of providing a very clean cut between a semantic definition which is *precise* (unlike our lax and dataflow semantics) and interpretations in which *all* introduced imprecision resides. In the present paper we have abandoned this approach only to simplify our presentation. Jones and Søndergaard used operations "call" and "return" which in the present approach have been replaced by "unify" and "comb." We find this conceptually cleaner.

Kanamori and Kawamura [32] suggested a framework based on OLDT resolution [60], which essentially is SLD resolution extended with memoing, so as to avoid redundant computation. Bruynooghe *et al.* [3, 6] suggested an AND/OR tree-based framework which expresses the ideas

[8] The origin of this suggestion can be attributed to Alan Mycroft.

behind the Jones-Søndergaard scheme at a lower level of abstraction. Efficient implementations of dataflow analysis engines based on the AND/OR tree framework are described in [34].

The framework used by Winsborough [61, 62] is rather close to ours. In particular, one semantic definition (Winsborough's "total function graph semantics" [62]) is almost identical to our base semantics, the difference being that, where we employ ex-equations, it works with substitutions which are "canonized" to bar variants of a substitution from introducing redundancy (Mellish [47] used the same idea).

Debray [15] has studied a framework for dataflow analysis with the point of departure that analyses must be *efficient*. He identifies a property of description domains ("substitution closure") and gives a complexity analysis to support the claim that the corresponding class of dataflow analyses can be implemented efficiently. Our groundness analysis falls outside Debray's class, as does any dataflow analysis that attempts to maintain information about possible aliasing (see also below).

In other studies of logic program analysis [43], we have found it useful to distinguish between "bottom-up" and "top-down" analysis. This distinction is not clear-cut, but we think of a top-down semantics as one that allows for extraction of information about the SLD tree that corresponds to the execution of a program given some query. Bottom-up analysis is not based on such a semantics to begin with, but on a T_P-style semantics [2], and therefore it cannot provide information about calls that will take place at runtime. Bottom-up analysis suffices for several applications, though. It is not only the conceptually simplest of the two, it also allows for efficient derivation of *query-independent* information about a program.

It has been suggested that top-down analysis can be done by first applying the so-called magic set transformation to the source program/query pair, and then computing call patterns in a bottom-up fashion from the transformed program. See for example [18, 54] and the closely related Alexander template approach [31].

For instance, assume that we are given the *append* program from before:

$$append(nil, y, y).$$
$$append(u : x, y, u : z) \leftarrow append(x, y, z).$$

and the query $\leftarrow append(x, y, z)$. The program/query combination is transformed to the following:

$$append(nil, y, y) \leftarrow call\_append(nil, y, y).$$
$$append(u : x, y, u : z) \leftarrow call\_append(u : x, y, u : z), append(x, y, z).$$
$$call\_append(x, y, z) \leftarrow call\_append(u : x, y, u : z).$$
$$call\_append(x, y, z).$$

A bottom-up evaluation of the transformed program will reflect what happens in a top-down evaluation of the original program. In our example, the unit clause '$call\_append(x, y, z)$' expresses the fact that *append* will be called with arguments (x, y, z). The first clause in the transformed program says that if an instance of $append(nil, y, y)$ is called then it will succeed, and so on.

In general, each clause $H \leftarrow A_1, \ldots, A_n$ $(n \geq 0)$ in P gives rise to $n+1$ clauses, namely

$$H \leftarrow call\_H, A_1, \ldots, A_n.$$

and for $i \in \{1, \ldots, n\}$:

$$call\_A_i \leftarrow call\_H, A_1, \ldots, A_{i-1}.$$

A query $\leftarrow A_1, \ldots, A_m$ is replaced by m clauses $(i \in \{1, \ldots, m\})$:

$$call\_A_i \leftarrow A_1, \ldots, A_{i-1}.$$

Applying bottom-up abstract interpretation to the transformed program will then yield call pattern information about the original program. However, whether this approach is better than what we have suggested in this paper is not clear as the magic set transformation is not free and the resulting program is typically much larger than the original.

10 Conclusion

One contribution of this paper is a new framework for the abstract interpretation of definite logic programs based on SLD resolution. It captures the essence of a major class of dataflow analyses used in many different logic programming tools, in particular compilers. It is based on *simple* semantic definitions for logic programs and dataflow analyses. The simplicity is partly due to the use of sets of existentially quantified equations rather than sequences of substitutions. There is a high degree of congruence between the standard semantics and the dataflow analyses, emphasizing their close relationship.

We have demonstrated the usefulness of our framework by developing a non-trivial groundness analysis and proving its correctness. The groundness analysis uses positive Boolean functions to capture groundness dependencies among variables in a program. This results in a simple and clean, yet highly precise, dataflow analysis.

However, we feel that the most important contribution of our paper is a theory of "language-independent abstract interpretation," which is suitable for logic programming style languages and other non-deterministic programming languages. Our theory is a modification of the denotational approach developed by F. Nielson in the context of deterministic programming languages. The key idea is to formalize abstract interpretation in terms of a powerful meta-language such as that of denotational semantics. This allows for generality at different levels. First, it allows for comfortable reasoning at exactly the level of abstraction called for by any particular class of applications, or dataflow analyses. Second, the proof of correctness of a particular dataflow analysis becomes simpler, since parts of it can be conducted at the level of the meta-language once and for all. Finally, most of the theory is independent of any particular programming language, since it is expressed in terms of the meta-language only.

Our theory facilitates development of analyses in other related programming language paradigms. It has been applied successfully to develop a generic framework for the analysis of logic programs where the semantics is based on a fixpoint characterization of the least model [40], rather than the SLD based semantics considered here. Our theory has also been used to formalize dataflow analysis for: constraint logic programming languages [39, 45]; logic programming languages that allow the use of "safe" negation [44]; and even concurrent constraint programming languages [21]. Other related languages in which our theory should be useful include logic programming languages with delay mechanisms ("freeze," "wait," "when," *etc.*), as well as deductive databases.

Acknowledgements

We would like to thank Will Winsborough for his insightful comments. Very thorough referees have reviewed a previous version of this paper, and we thank them for their constructive critique.

References

[1] Abramsky, S., and Hankin, C., editors. *Abstract Interpretation of Declarative Languages.* Ellis Horwood, 1987.

[2] Apt, K., and van Emden, M. Contributions to the theory of logic programming. *Journal of the ACM* **29**: 841–862, 1982.

[3] Bruynooghe, M. A framework for the abstract interpretation of logic programs. Report CW 62, Dept. of Computer Science, University of Leuven, Belgium, 1987.

[4] Bruynooghe, M. A practical framework for the abstract interpretation of logic programs. *Journal of Logic Programming* **10** (2): 91–124, 1991.

[5] Bruynooghe, M., and Janssens, M. Deriving descriptions of possible values of program variables by means of abstract interpretation. *Journal of Logic Programming* **13** (2&3): 205–258, 1992.

[6] Bruynooghe, M. et al. Abstract interpretation: towards the global optimization of Prolog programs. In *Proc. Fourth Int. Symp. Logic Programming*, pages 192–204. San Francisco, California, 1987.

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

[8] Codish, M. Private communication, May 1993.

[9] Cortesi, A., Filé, G., and Winsborough, W. *Prop* revisited: Propositional formula as abstract domain for groundness analysis. In *Proc. Sixth Ann. IEEE Symp. Logic in Computer Science*, pages 322–327. Amsterdam, The Netherlands, 1991.

[10] Cousot, P., and Cousot, R. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. Fourth Ann. ACM Symp. Principles of Programming Languages*, pages 238–252. Los Angeles, California, 1977.

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

[12] Cousot, P., and Cousot, R. Systematic design of program analysis frameworks. In *Proc. Sixth Ann. ACM Symp. Principles of Programming Languages*, pages 269–282. San Antonio, Texas, 1979.

[13] Dart, P. *Dependency Analysis and Query Interfaces for Deductive Databases.* PhD thesis, The University of Melbourne, Australia, 1988.

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

[15] Debray, S. K. Efficient dataflow analysis of logic programs. In *Proc. Fifteenth Ann. ACM Symp. Principles of Programming Languages*, pages 260–273. San Diego, California, 1988.

[16] Debray, S. K. *Global Optimization of Logic Programs.* PhD Thesis, State University of New York at Stony Brook, New York, 1986.

[17] Debray, S. K., and Mishra, P. Denotational and operational semantics for Prolog. *Journal of Logic Programming* **5** (1): 61–91, 1988.

[18] Debray, S. K., and Ramakrishnan, R. Canonical computation of logic programs. Draft, 1991.

[19] Donzeau-Gouge, V. Utilisation de la sémantique dénotationelle pour l'étude d'interprétations non-standard. Research Report 273, IRIA, Le Chesnay, France, 1978.

[20] Errington, D. L., and Søndergaard, H. Absinth: A generic dataflow analyser for logic programs. Technical Report 92/19, Dept. of Computer Science, University of Melbourne, Australia, 1992.

[21] Falaschi, M. et al. Compositional analysis for concurrent constraint programming. To appear in *Proc. IEEE Symp. Logic in Computer Science.* Montreal, Canada, 1993.

[22] Hecht, M. *Flow Analysis of Computer Programs.* North-Holland, 1977.

[23] Hermenegildo, M., Warren, R., and Debray, S. K. Global flow analysis as a practical compilation tool. *Journal of Logic Programming* **13** (4): 349–366, 1992.

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

[25] Jensen, J. Generation of machine code in Algol compilers. *BIT* **5**: 235–245, 1965.

[26] Jones, N. D. Flow analysis of lambda expressions. In S. Even and O. Kariv, editors, *Proc. Eighth Int. Coll. Automata, Languages and Programming* (Lecture Notes in Computer Science 115), pages 114–128. Springer-Verlag, 1981.

[27] Jones, N. D., and Muchnick, S. S. Flow analysis and optimization of Lisp-like structures. In S. S. Muchnick and N. D. Jones, editors, *Program Flow Analysis*, pages 102–131. Prentice-Hall, 1981.

[28] Jones, N. D., and Mycroft, A. A stepwise development of operational and denotational semantics for Prolog. In *Proc. 1984 Int. Symp. Logic Programming*, pages 289–298. Atlantic City, New Jersey, 1984.

[29] Jones, N. D., and Mycroft, A. Dataflow analysis of applicative programs using minimal function graphs. In *Proc. Thirteenth Ann. ACM Symp. Principles of Programming Languages*, pages 296–306. St. Petersburg, Florida, 1986.

[30] Jones, N. D., and Søndergaard, H. A semantics-based framework for the abstract interpretation of Prolog. In Abramsky and Hankin [1], pages 123–142.

[31] Kanamori, T. Abstract interpretation based on Alexander templates. *Journal of Logic Programming* **15** (1&2): 31–54, 1993.

[32] Kanamori, T., and Kawamura, T. Abstract interpretation based on OLDT resolution. *Journal of Logic Programming* **15** (1&2): 1–30, 1993.

[33] Kleene, S. C. *Introduction to Metamathematics*. North-Holland, 1971. Originally published by Van Nostrand, 1952.

[34] Le Charlier, B., Musumbu, K., and Van Hentenryck, P. A generic abstract interpretation algorithm and its complexity analysis. In K. Furukawa, editor, *Logic Programming: Proc. Eighth Int. Conf.*, pages 64–78. MIT Press, 1990.

[35] Le Charlier, B., and Van Hentenryck, P. Groundness analysis for Prolog. To appear in *Proc. Third ACM Symp. Partial Evaluation and Semantics-Based Program Manipulation.* Copenhagen, Denmark, 1993.

[36] Lloyd, J. W. *Foundations of Logic Programming*. Springer-Verlag, second edition 1987.

[37] Mannila, H., and Ukkonen, E. Flow analysis of Prolog programs. In *Proc. Fourth Symp. Logic Programming*, pages 205–214. San Francisco, California, 1987.

[38] Marriott, K. Frameworks for abstract interpretation. *Acta Informatica* **30** (2): 103–129, 1993.

[39] Marriott, K., and Søndergaard, H. Analysis of constraint logic programs. In S. Debray and M. Hermenegildo, *Logic Programming: Proc. North American Conf. 1990*, pages 531–547. MIT Press, 1990.

[40] Marriott, K., and Søndergaard, H. Bottom-up dataflow analysis of normal logic programs. *Journal of Logic Programming* **13** (2&3): 181–204, 1992.

[41] Marriott, K., and Søndergaard, H. Notes for a tutorial on abstract interpretation of logic programs. Presented to North American Conf. Logic Programming, Cleveland, Ohio, 1989.

[42] Marriott, K., and Søndergaard, H. Precise and efficient groundness analysis. Technical Report 93/7, Dept. of Computer Science, The University of Melbourne, 1993.

[43] Marriott, K., and Søndergaard, H. Semantics-based dataflow analysis of logic programs. In G. X. Ritter, editor, *Information Processing 89*, pages 601–606. North-Holland, 1989.

[44] Marriott, K., Søndergaard, H., and Dart, P. A characterization of non-floundering logic programs. In S. Debray and M. Hermenegildo, editors, *Logic Programming: Proc. North American Conf. 1990*, pages 661–680. MIT Press, 1990.

[45] Marriott, K., and Stuckey, P. The 3 R's of optimizing constraint logic programs: Refinement, removal and reordering. *Proc. Twentieth ACM Symp. Principles of Programming Languages*, pages 334–344. Charleston, South Carolina, 1993.

[46] Mellish, C. S. The automatic generation of mode declarations for Prolog programs. DAI Research Paper No. 163, University of Edinburgh, Scotland, 1981.

[47] Mellish, C. S. Abstract interpretation of Prolog programs. In Abramsky and Hankin [1], pages 181–198.

[48] Mellish, C. S. Some global optimizations for a Prolog compiler. *Journal of Logic Programming* **2** (1): 43–66, 1985.

[49] Mycroft, A. *Abstract Interpretation and Optimising Transformations for Applicative Programs*. PhD Thesis, University of Edinburgh, Scotland, 1981.

[50] Naur, P. The design of the Gier Algol compiler, part II. *BIT* **3**: 145–166, 1963.

[51] Nielson, F. A denotational framework for data flow analysis. *Acta Informatica* **18**: 265–287, 1982.

[52] Nielson, F. Strictness analysis and denotational abstract interpretation. *Information and Computation* **76** (1): 29–92, 1988.

[53] Nielson, F. Two-level semantics and abstract interpretation. *Theoretical Computer Science* **69**: 117–242, 1989.

[54] Nilsson, U. Abstract interpretation: A kind of magic. In J. Małuszyński and M. Wirsing, editors, *Programming Language Implementation and Logic Programming* (Lecture Notes in Computer Science 528), pages 299-309. Springer-Verlag, 1991.

[55] Reynolds, J. C. Automatic computation of data set definitions. In A. Morrell, editor, *Information Processing 68*, pages 456–461. North-Holland, 1969.

[56] Schmidt, D. *Denotational Semantics: A Methodology for Language Development.* Allyn and Bacon, 1986.

[57] Sintzoff, M. Calculating properties of programs by valuation on specific models. *SIGPLAN Notices* **7** (1): 203–207, 1972. Proc. ACM Conf. Proving Assertions about Programs.

[58] Søndergaard, H. An application of abstract interpretation of logic programs: Occur check reduction. In B. Robinet and R. Wilhelm, editors, *Proc. ESOP 86* (Lecture Notes in Computer Science 213), pages 327–338. Springer-Verlag, 1986.

[59] Søndergaard, H. *Semantics-Based Analysis and Transformation of Logic Programs.* PhD Thesis, University of Copenhagen, Denmark, 1989.

[60] Tamaki, H., and Sato, T. OLD resolution with tabulation. In E. Shapiro, editor, *Proc. Third Int. Conf. Logic Programming* (Lecture Notes in Computer Science 240), pages 84–98. Springer-Verlag 1986.

[61] Winsborough, W. Automatic, transparent parallelization of logic programs at compile time. PhD Thesis, University of Wisconsin-Madison, Wisconsin, 1988.

[62] Winsborough, W. Source-level transforms for multiple specialization of Horn clauses (extended abstract). Technical report 88-15, Dept. of Computer Science, University of Chicago, Illinois, 1988.

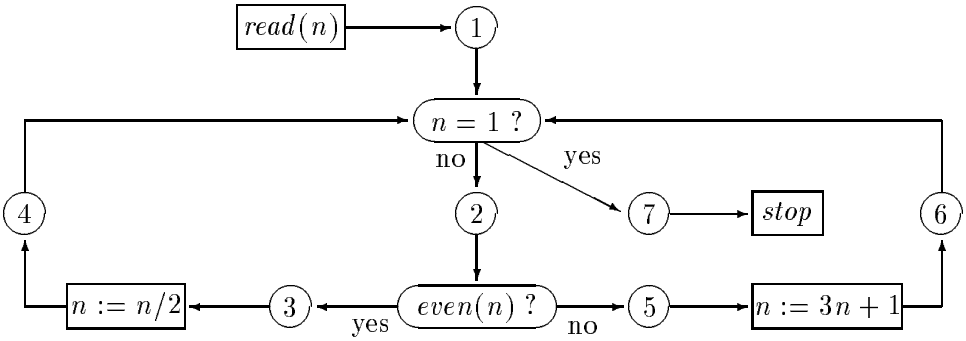

Figure 1: A flow diagram

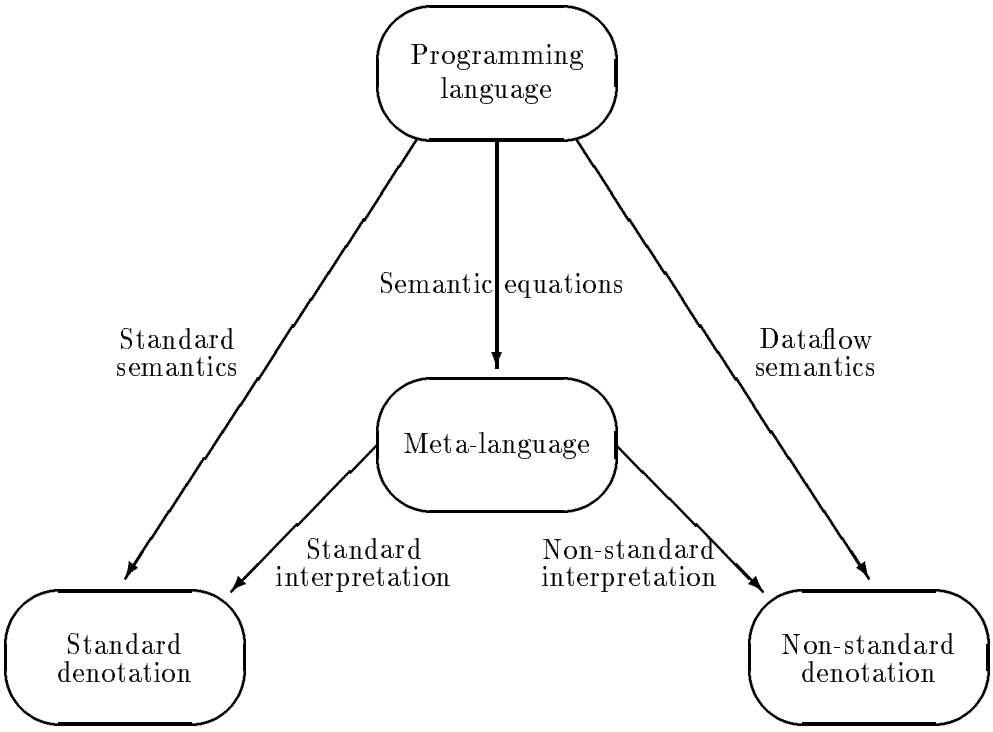

Figure 2: The role of the meta-language (after Nielson)

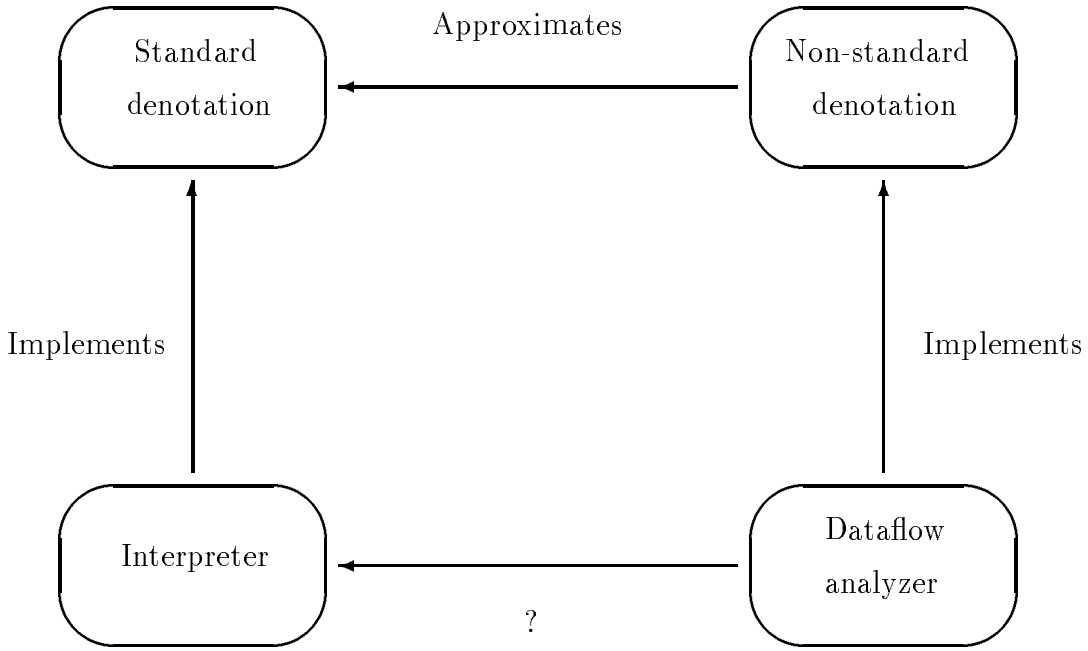

Figure 3: Separating two orthogonal aspects of the dataflow analyzer

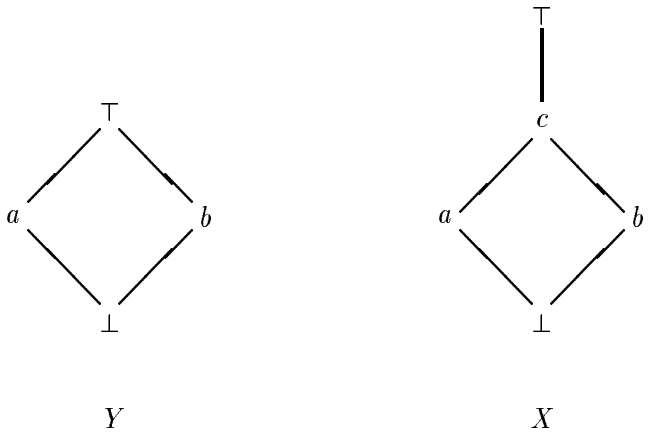

Figure 4: Example lattices

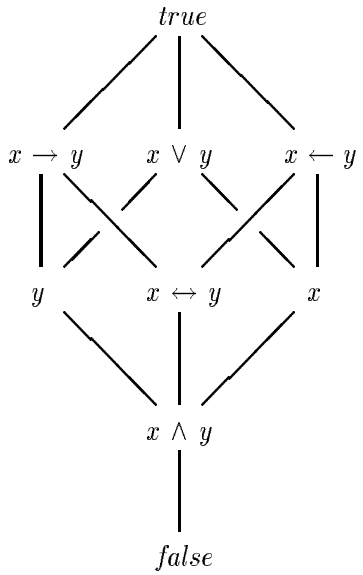

Figure 5: The $Pos_{\perp}$ functions of two variables