Technical Report: TR-96-10, May 04, 1996

A hierarchy of constraint systems for data-flow analysis of constraint logic-based languages

Bagnara, Roberto

Dipartimento di Informatica, Università di Pisa
corso Italia 40, 56125 Pisa, Italy

Abstract

Many interesting analyses for constraint logic-based languages are aimed at the detection of emphmonotonic properties, namely of properties which are preserved as the computation progresses. Our basic claim is that most, if not all, of these analyses can be described within a unified notion of constraint domains. We present a class of constraint systems which allows for a smooth integration within an appropriate framework for the definition of non-standard semantics of constraint logic-based languages. Such a framework is also presented and motivated. We then show how such domains can be built, as well as construction techniques which induce a hierarchy of domains. In particular, we propose a general methodology for domain combination with asynchronous interaction (i.e. the interaction is not necessarily synchronized with the domains' operations). Following this methodology, interesting combinations of domains can be expressed with all the the semantic elegance of concurrent constraint programming languages.

ACM–CR Subject Classification:

Keyword and phrases: Data-flow analysis, abstract interpretation, constraint systems, concurrent constraint programming

A hierarchy of constraint systems for data-flow analysis of constraint logic-based languages

Roberto Bagnara

Dipartimento di Informatica, Università di Pisa, Corso Italia 40, 56125 Pisa, Italy

Many interesting analyses for constraint logic-based languages consist in determining the *shape* of the set of solutions of the constraint store at some program points. Our basic claim is that most, if not all, of these analyses can be described within a unified notion of constraint domains. We present a class of constraint systems which allows for a smooth integration within an appropriate framework for the definition of non-standard semantics of constraint logic-based languages. Such a framework is also presented and motivated. We then show how such domains can be built, as well as construction techniques which induce a hierarchy of domains. In particular, we propose a general methodology for domain combination with asynchronous interaction. The interaction among domains is asynchronous in that it is not necessarily synchronized with the domain's operations.

Key words: Constraint Systems, Constraint-based Languages, Data-flow Analysis, Abstract Interpretation.

1 Introduction

Many interesting data-flow analyses for constraint logic-based languages consist in determining the *shape* of the set of solutions of the constraint store at some program points. Examples include definiteness (or groundness), symbolic patterns, types, numerical bounds and relations, symbolic size-relations and so on.

In the case of Prolog, these analyses have been extensively studied (see [15] for a summary of this work). In the case of constraint-based languages, besides the generalization to CLP($\mathcal{H}$) of the ideas and techniques used for Prolog, not much has been done. For languages of the kind of CLP($\mathcal{N}$), where $\mathcal{N}$ is some numerical domain, a data-flow analysis for numerical bounds and relations was first proposed in [5,6]. [4] describes some of the most important applications of such analyses. Subsequently, a technique for integrating (to some extent)

numerical and symbolic patterns in CLP($\mathcal{H}$, $\mathcal{N}$) has been described in [33]. Here, the numerical part is essentially the one proposed in [5].

A key observation is that the shape of the solutions' set can be conveniently described by constraints. Thus, frameworks of constraint-based languages are, in principle, general enough to encompass some of their own data-flow analyses. Intuitively, this is done by replacing the standard constraint domain with one suitable for expressing the desired information. This fundamental aspect was brought to light, for the case of CLP, in [10] and elaborated in [24]. In [24] it is presented a generalized algebraic semantics for constraint logic programs, which is parameterized with respect to an underlying constraint domain. The main advantages of this approach are that: (1) different instances of CLP can be used to define non-standard semantics for constraint logic programs; and (2) several abstract interpretations of CLP programs can be thus formalized inside the CLP paradigm. (The class of abstract interpretations which are captured by the approach of [24] is restricted to *monotonic properties*, that is, properties which are preserved as computations progress.)

In this setting, data-flow analysis is then performed (or at least justified) through abstract interpretation [14,15], i.e. "mimicking" the program run-time behavior by "executing" it, in a finite way, on an approximated (abstract) constraint domain. Following a generalized semantic approach, the concrete and abstract semantics are more easily related, being instances (over two different constraint systems) of the same generalized semantics, which is entirely parametric on a constraint domain. Thus, to ensure correctness, it will be sufficient to exhibit an "abstraction function" α which is a semi-morphism between the constraint domains [7,16].

We move our steps from [24] by providing a more general notion of constraint domain which allows one to adequately describe both the "logical part" of concrete computations (e.g. answer constraints) and as much abstract interpretations (e.g. the shape of those answer constraints) as possible. In particular our notion of constraint system is able to accommodate approximate inference techniques whose importance relies on very practical considerations, such as representing good compromises between precision and computational efficiency. Some of these techniques will be sketched in the examples. The new notion of constraint domain requires the introduction of a new generalized semantics framework which is more liberal than the one of [24].

Moreover, and here comes the main point, we show that our constraint domains admit interesting constructions. The most important one consists in upgrading a domain so that it will be able to represent and manipulate *dependencies* among constraints. This is done by regarding a restricted class of cc agents as constraints. This construction, among other things, opens up the possibility of combining domains in a novel and interesting way. Following this methodology,

the asynchronous interaction between domains can be expressed with all the elegance which derives from the cc framework.

The plan of the paper is as follows: Section 2 introduces some basic notions and notations used throughout the paper. Section 3 explains our generalized semantics for CLP languages. Section 4 introduces *simple constraint systems*: some important building blocks of the hierarchy. Section 5 builds on the previous one presenting *determinate constraint systems*. In Section 6 it is shown how a constraint system is upgraded to incorporate a weak form of disjunction (suitable to monotonic properties) by means of *powerset constraint systems*. Section 7 presents a different kind of upgrade: the one needed in order to have the notion of *dependency* built into the constraint system. This is done considering *ask-and-tell constraint systems*. Section 8 deals with the interesting problem of combining domains. A technique is shown which consists in applying the *ask-and-tell construction* to *product constraint systems*. Finally, Section 9 draws some conclusions and presents some directions for further work.

2 Preliminaries

Throughout the paper we will assume familiarity with the basic notions of lattice theory, semantics of logic programming languages, and abstract interpretation.

Let U be a set. The set of all subsets of U will be denoted by $\wp(U)$. The set of all *finite* subsets of U will be denoted by $\wp_f(U)$. The notation $S \subseteq_f T$ stands for $S \in \wp_f(T)$. For $S \subseteq U$ we will denote the complement $U \setminus S$ by $\overline{S}$, when U is clear from the context. For $S, T \subseteq U$ the notation $S \uplus T$ denotes *disjoint union*, emphasizing the fact that $S \cap T = \varnothing$. By $U^\star$ we will denote the set of all finite sequences of elements drawn from U. The empty sequence is denoted by ε. For $x \in U^\star$, the *length* of x will be denoted by $\# x$, and, for i such that $1 \leq i \leq \# x$, the notation $x[i]$ stands for the i-th element of x. Let $S_1, \ldots, S_n$ be sets. We will denote elements of $S_1 \times \cdots \times S_n$ by $\langle e_1, \ldots, e_n \rangle$. The *projection mappings* $\pi_i \colon S_1 \times \cdots \times S_n \to S_i$ are defined, for $i = 1, \ldots, n$, by $\pi_i(\langle e_1, \ldots, e_n \rangle) \stackrel{\text{def}}{=} e_i$. The *liftings* $\pi_i \colon \wp(S_1 \times \cdots \times S_n) \to \wp(S_i)$ given by $\pi_i(T) \stackrel{\text{def}}{=} \{\, \pi_i(t) \mid t \in T \,\}$ will also be used.

A *partial order* $\preceq$ over a set P is a binary relation which is reflexive, transitive, and antisymmetric. $\preceq$ is a *total order* if, in addition, for each $x, y \in P$, either $x \preceq y$ or $y \preceq x$. A set P equipped with a partial (resp. total) order $\preceq$ is said to be *partially ordered* (resp. *totally ordered*), and sometimes written $\langle P, \preceq \rangle$. Partially ordered sets are also called *posets*. A subset S of a poset $\langle P, \preceq \rangle$ is said to be a *chain* if it is totally ordered wrt $\preceq$. Given $x \in P$, the *downward*

closure of x in $\langle P, \preceq \rangle$ is given by $\{ y \mid y \preceq x \}$ and denoted by $\downarrow x$. Given a poset $\langle P, \preceq \rangle$ and $S \subseteq P$, $y \in P$ is an *upper bound* for S iff $x \preceq y$ for each $x \in S$. An upper bound y for S is the *least upper bound* (or *lub*) of S iff for every upper bound y' it is $y \preceq y'$. The *lub*, when it exists, is unique. In this case we write $y = lub\, S$. *Lower bounds* and *greatest lower bounds* are defined dually. $\langle P, \preceq \rangle$ is said *bounded* if it has a minimum and a maximum element.

A poset $\langle L, \preceq \rangle$ such that, for each $x, y \in L$, both $lub\{x, y\}$ and $glb\{x, y\}$ exist, is called a *lattice*. In this case, *lub* and *glb* are also called, respectively, the *join* and the *meet* operations of the lattice. A poset where only the *glb* operation is well-defined is called a *meet-semilattice*. A *complete lattice* is a lattice $\langle L, \preceq \rangle$ such that every subset of L has both a least upper bound and a greatest lower bound.

An algebra $\langle L, \wedge, \vee \rangle$ is also called a *lattice* if $\wedge$ and $\vee$ are two binary operations over L which are commutative, associative, idempotent, and satisfy the following *absorption laws*, for each $x, y \in L$: $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$. The two definitions of lattices are equivalent. This can be seen by setting up the isomorphism given by: $x \preceq y \stackrel{\text{def}}{\Longleftrightarrow} x \wedge y = x \stackrel{\text{def}}{\Longleftrightarrow} x \vee y = y$, $glb\{x, y\} \stackrel{\text{def}}{=} x \wedge y$, and $lub\{x, y\} \stackrel{\text{def}}{=} x \vee y$.

The notions of meet-semilattice and of bounded lattice are imported into the algebraic definition in the natural way. For instance, a bounded lattice is an algebra $\langle L, \wedge, \vee, \bot, \top \rangle$ such that $\langle L, \wedge, \vee \rangle$ is a lattice and the following two *annihilation* laws are satisfied for each $x \in L$: $x \wedge \bot = \bot$ and $x \vee \top = \top$. A lattice is said *distributive* if it satisfies, for each $x, y, z \in L$, the *distributive laws* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. It is well known that, for lattices, the distributive laws are equivalent.

An algebra $\langle M, \cdot, 1 \rangle$ is a *monoid* iff '$\cdot$' is an associative binary operator over M, and $1 \in M$ satisfies the *identity law*: for each $x \in M$, $x \cdot 1 = 1 \cdot x = x$. The monoid $\langle M, \cdot, 1 \rangle$ is said *commutative* or *idempotent* if '$\cdot$' is so.

The sets of all natural, real, and ordinal numbers will be denoted, respectively, by $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{O}$. The first limit ordinal equipotent with the set of natural numbers is denoted by ω.

3 A case study: CLP

The constraint domains which are the subject of this work are not bound to a particular class of constraint logic-based languages. However, for the sake of clarity and to help the intuition, we will focus on the class of CLP languages [30,32], which is more and more influential and captures several existing, im-

plemented languages. We will present a *generalized approach* to the semantics of CLP programs of which abstract interpretation is an important instance. This is necessary for a full understanding of how the domains of later sections are employed in data-flow analysis of CLP languages.

3.1 CLP: the syntax

Here we give a precise definition of what we will call a CLP(C) program. Notice that here we are concerned with syntax only. In general, C (the language of *atomic constraints*) is a subset of a first order language L (the language of constraints). Let us start by defining L itself.

Definition 1 (Language of constraints.) *Let V and Λ be two disjoint denumerable sets of variable symbols. Let also fix two particular isomorphisms between Λ and $\mathbb{N}$, and between V and $\mathbb{N}$. Let $Vars \stackrel{\text{def}}{=} V \uplus \Lambda$. Let Ω and Π_C be two finite sets of operation and predicate symbols, respectively, each symbol being characterized with its* arity. *Let also $Vars$, Ω and Π_C be mutually disjoint. $\mathsf{L} = \mathsf{L}(Vars, \Omega, \Pi_C, \dots)$ is a* language of constraints *iff it is any first order language with equality built (by means of standard constructions, possibly with connectives and quantifiers) over the given sets of symbols.*

The extra-set of variables Λ allows us to simplify the following treatment. We will stipulate that the *heads* of clauses can only contain variable's symbols drawn from Λ.

Now, a CLP language can impose restrictions on the form of constraints that may actually appear in programs. However these restrictions must not destroy too much of the language's expressivity.

Definition 2 (Atomic constraint.) *Given a language of constraints L, let C be any subset of L such that:*

(i) *C is closed under variable renaming;*
(ii) *C contains all the formulas of the form $X = t$, where $X \in Vars$ and t is a term built over Ω and $Vars$.*

Then C is a language of atomic constraints.

Before introducing the full syntax of CLP programs a few remarks about notation are in order. We will denote program variables by means of capital letters (X, Y, ...). Tuples of distinct variable will be denoted by $\bar{X}$, $\bar{Y}$, and so forth. Tuples are always assumed to be of the right cardinality, e.g., if p is a predicate symbol of arity n and we write $p(\bar{X})$, then $\bar{X}$ is an n-tuple. Special

tuples denoted by $\vec{\Lambda}$, denoting initial finite segments of Λ, will also be used [1]. In the above hypotheses, by writing $p(\vec{\Lambda})$ we understand that $\vec{\Lambda}$ denotes the n-tuple consisting of the first n variable's symbols in Λ. We will also abuse the notation by confusing a tuple with the set of its components.

We can now introduce the notion of CLP(C) program. Notice that, not to exclude in advance any real CLP language, we carefully avoid making any compromising assumption.

Definition 3 (CLP program.) *Let C be a language of atomic constraints with distinguished variable symbols in Λ. Let Π_P be a finite set of predicate symbols, disjoint from the symbols used in C. We will denote by A_P the set of atoms over Π_P, that is*

$$\mathsf{A}_P \stackrel{\text{def}}{=} \left\{ q(\bar{X}) \;\middle|\; q \in \Pi_P, \bar{X} \in \mathit{Vars}^\star \right\}.$$

A CLP(C) *program P over Π_P is a finite sequence of* rules *(or* clauses*) of the form*

$$p(\vec{\Lambda}) :- \langle b_1, \ldots, b_k \rangle,$$

with $p \in \Pi_P$ and $k \geq 0$, where, for $1 \leq i \leq k$, either b_i is a constraint $b_i \in \mathsf{C}$ with $\mathit{vars}(b_i) \cap \Lambda \subseteq \vec{\Lambda}$, or $b_i \in \mathsf{A}_P$. $p(\vec{\Lambda})$ is called the head *of the rule, whereas $\langle b_1, \ldots, b_k \rangle$ is the* body.

The syntax of any CLP language can be defined in such a way, by augmenting the first order language on which it is based with the set of distinguished variable symbols Λ and transforming each program along the lines of Definition 3 by means of standard techniques. This transformation is always possible by virtue of Definition 2. This *normalization* of programs has the property that predicate's symbols are always applied to tuples of distinct variables. Further, all the heads of the rules defining a program predicate p/n have the same variables in the same positions. Observe that the body B of a clause $p(\vec{\Lambda}) :- B$ is a sequence, that is an element of $(\mathsf{C} \cup \mathsf{A}_P)^\star$. As programs themselves are sequences, the semantic constructions will be free to take into account the selection and search rules used in real languages. So far for the syntax, we now examine the (possibly non-standard) semantics of CLP languages.

3.2 Non-standard semantics for CLP

Here we start from very basic facts. We recognize the existence of four different activities in the execution, and thus in the analysis, of constraint logic programs:

[1] Recall that we have fixed a total ordering on Λ.

(i) different execution paths are explored;
(ii) along any path, constraints are accumulated in the so called *constraint store*;
(iii) the constraint store is recursively subdivided into parts. The activity of imposing restrictions in the way different parts can interact is usually called *hiding*.
(iv) Pieces of information (parameters) are passed between program rules.

For different (non-standard) semantics, and at different levels of abstraction the degree of correlation among these activities may vary considerably. For instance, while in a "standard" semantic execution paths are explored depending on the satisfiability of the accumulated constraints, in the case of "non-standard" semantic constructions these activities can be somewhat unrelated. Perhaps because the satisfiability check does not make sense in the non-standard interpretation (think about groundness analysis), or because it can be safely moved outside the construction process.

The way we define domains of interpretation for CLP languages is clearly highly dependent on the application we have in mind. Here we give a general description of what are the characteristics of a quite wide class of domains which covers many non-standard semantics for CLP. Then we will obtain our specific class of domains by imposing restrictions on the general scheme. This is important for a full understanding of the hypotheses which are behind our approach.

Suppose we are interested in some properties of programs' *terminating* computations. To this minimal requirement corresponds the following class of interpretation domains.

Definition 4 (Ordered domain.) *An* ordered domain of interpretation *for a CLP language is a structure:*

$$\bar{\mathcal{D}} \stackrel{\text{def}}{=} \left\langle \mathcal{D}, \sqsubseteq, \preceq, \otimes, \oplus, \bot, \mathbf{1}, \{\bar{\exists}_{\vec{\Lambda}}\}_{\vec{\Lambda}\in\Lambda^\star}, \{d_{\bar{X}\bar{Y}}\}_{\bar{X},\bar{Y}\in \mathit{Vars}^\star} \right\rangle,$$

where $\mathcal{D}$ is a set of (not better specified) properties, $\sqsubseteq \subseteq \mathcal{D}\times\mathcal{D}$ and $\preceq \subseteq \mathcal{D}\times\mathcal{D}$ are relations over $\mathcal{D}$, $\otimes\colon \mathcal{D}\times\mathcal{D}\to\mathcal{D}$ and $\oplus\colon \mathcal{D}\times\mathcal{D}\to\mathcal{D}$ are binary operators, $\{\bar{\exists}_{\vec{\Lambda}}\}_{\vec{\Lambda}\in\Lambda^\star}$ is a family of unary operators, $\bot$, $\mathbf{1}$, and $\{d_{\bar{X}\bar{Y}}\}_{\bar{X},\bar{Y}\in \mathit{Vars}^\star}$ are distinguished elements of $\mathcal{D}$. Furthermore

O_1. $\langle \mathcal{D}, \oplus, \bot\rangle$ *is a monoid;*
O_2. $\langle \mathcal{D}, \otimes, \mathbf{1}\rangle$ *is a monoid;*
O_3. $\bot$ *is an* annihilator *for $\otimes$, i.e. for each $D\in\mathcal{D}$, $\bot\otimes D = D\otimes\bot = \bot$;*
O_4. $\langle \mathcal{D}, \sqsubseteq\rangle$ *is a partial order with minimum element $\bot$;*
O_5. $\langle \mathcal{D}, \preceq\rangle$ *is a partial order with maximum element $\mathbf{1}$.*

The $\oplus$ operator models the merging of information coming from different execution paths. The monoidal structure ensures that the composition process is "insensitive to grouping" and that the empty path (which intuitively corresponds to $\bot$) is ignored. Not requiring more than the monoidal structure means that we have not lost already the ability of taking into account the order on which paths are tried.

The $\otimes$ operator models the constraint accumulation process. Similar considerations apply here as in the case of $\oplus$, with the monoidal unit $\mathbf{1}$ standing, intuitively, for the empty constraint store, i.e. the one containing no information at all.

The $\bar{\exists}_{\vec{\Lambda}}$ operators represent the *hiding* process: any variable $X \notin \vec{\Lambda}$ appearing in the scope of $\bar{\exists}_{\vec{\Lambda}}$ is isolated (hidden) from other occurrences of X outside the scope. The "complement sign" which appears on top of $\bar{\exists}_{\vec{\Lambda}}$ signifies that we formalize hiding in a dual way with respect to traditional approaches [45,24]. Notice that the exact interpretation of the $\bar{\exists}_{\vec{\Lambda}}$ operators is, by now, relatively free. They might stand for projection onto the "variables of interest" $\vec{\Lambda}$ (this will be our case), or renaming to fresh variables (e.g. to model what happens in meta-interpreters: any variable not in $\vec{\Lambda}$ which appears in the scope is given a fresh name), or for very low-level operations (e.g. creation and disposal of environment-frames in machine-level traces: one slot for each "local variable", that is, each X in scope which is not in $\vec{\Lambda}$).

Similar considerations apply also to the distinguished elements representing parameter passing. In our present application $d_{\bar{X}\bar{Y}}$ will represent, roughly speaking, the fact that the tuples of variables $\bar{X}$ and $\bar{Y}$ are tightly correlated with respect to the properties of interest. When dealing with WAM traces, they could represent, for instance, the multiple assignment of the registers $\bar{X}$ to the *argument registers* $\bar{Y}$ [1].

Thus far we have given a mathematical dress to the ingredients which, in our intuition, constitute the computations of CLP programs. We now put ourselves in an abstract interpretation setting.

The non-standard semantics we are interested in will, in general, be captured by some *property transformer* $\Phi_P \colon \mathcal{D} \to \mathcal{D}$, where P is the program at hand. The purpose of the Φ_P operator, at an intuitive level, is that of exploring the (partial) computation paths of P. It will be designed in such a way so that iterated applications of Φ_P to the "null path" $\bot$ corresponds to the iterative re-construction of *all* the computation paths of P. This exploration process is usually monotonic, in that the "knowledge" about the possible paths increases between successive iterates. This relationship between successive iterates is captured (in a program independent way) by the relation $\sqsubseteq$, which is referred to as the *computational order* of the interpretation domain. When this is the

case, Φ_P is conceived so that any of its post-fixpoints (with respect to $\sqsubseteq$) is a property taking into account all the the computational possibilities of P and possibly more.

The relation $\preceq$, instead, specifies the relative precision of program properties. $D_1 \preceq D_2$ means that "D_1 is more precise than D_2". In other words, every set of computations which enjoys property D_1 enjoys also property D_2. In the framework of abstract interpretation, $\preceq$ is referred to as the *approximation ordering* of the domain. Notice that the distinction between approximation ordering and computational ordering is important: one has to do with the precision of properties, the other holds between successive iterates of the property transformers. In principle, they could be totally unrelated [16]. (It might be observed that it is not sensible to talk about a computational ordering of the domain without the explicit reference to a particular class of properties' transformers. However, since the domain of interpretation and the transformers are usually chosen at the same time, we found it more convenient to present the computational ordering as part of the domain.)

The objective of the game is now to derive, for any program P, a property which holds for all its computation paths. Generally speaking this will given, depending on the feasibility of the goal and on various other considerations, by either the least fixpoint or a post-fixpoint (wrt $\sqsubseteq$) of Φ_P or by some approximations (wrt $\preceq$) of them. Observe that the choice of a fixpoint presentation for the non-standard semantics is not restrictive in any way [18].

A treatment of abstract interpretation for CLP languages in these very general terms is well outside the scope of this paper. Thus we start imposing restrictions on the notion of interpretation domain given in Definition 4 so to obtain a specialized version which is suitable for our purposes. This makes clear what is the class of properties which are captured by the hierarchy of domains that will be presented later.

First of all, we are neither interested in the order in which computations are taken, nor in their multiplicities [2]. This amounts to

O_1'. $\langle \mathcal{D}, \oplus, \bot \rangle$ is a *commutative* and *idempotent* monoid.

Since we are interested in characterizing only the (possibly) successful computations, we disregard (finitely) failed computation paths. We thus postulate the existence in $\mathcal{D}$ of a property characterizing failed computations, the fact that extending a failed computation yields a failed computation, and the fact that such computations have to be ignored. More formally,

[2] We refer the reader to [37] for an understanding of why and how the ordering can be taken into account in the interpretation domain.

O_{s_1}. $\mathbf{0} \in \mathcal{D}$,
O_{s_2}. $\mathbf{0}$ is an *annihilator* for $\otimes$,
O_{s_3}. $\mathbf{0}$ is a *unit* for $\oplus$.

Then, we focus on *monotonic* properties, that is, those which are preserved as computation progresses. Since computations progress by *adding* constraints, this means

O_m. for each $D_1, D_2 \in \mathcal{D}$ we have both $D_1 \otimes D_2 \preceq D_1$ and $D_1 \otimes D_2 \preceq D_2$.

Further, we restrict out interest to *logical* properties. This means that $\otimes$ is interpreted as logical conjunction. Since, by the previous discussion, $\preceq$ is always interpreted as logical implication, we must have

O_2'. $\langle \mathcal{D}, \otimes, \mathbf{1} \rangle$ is a *commutative* and *idempotent* monoid.
O_l. for each $D_1, D_2 \in \mathcal{D}$, if $D_1 \preceq D_2$ then $D_1 \preceq D_1 \otimes D_2$.

Finally, since $D_1 \oplus D_2$ must hold for all the paths characterized by D_1 and all the ones characterized by D_2, we must have

O_p. for each $D_1, D_2 \in \mathcal{D}$ we have both $D_1 \preceq D_1 \oplus D_2$ and $D_2 \preceq D_1 \oplus D_2$.

These assumptions bring us to interpretation domains which are much simpler than those of Definition 4. By O_m and O_l we have that $D_1 \preceq D_2$ holds if and only if $D_1 \otimes D_2 = D_1$. Since $\bot$ and $\mathbf{0}$ are both minimal elements with respect to the ordering $\preceq$ they must coincide. Also, by O_p and the previous discussion, the computational ordering $\sqsubseteq$ must be included in $\preceq$. In fact, in the interpretation domains we will present later, they coincide.

Now the question is: how do we represent the properties of interest? A simple, but far reaching answer was first given in [10]: we can represent properties by means of constraints. This opens up the possibility of computing non-standard semantics of CLP, and, in particular, abstract interpretations, *within* the CLP framework. In this setting the result of the abstract interpretation of a CLP program P is obtained by "executing" (in a finite way) another CLP program P', strongly related to P, over a non-standard domain. Intuitively, this is done by replacing the standard constraint domain with one suitable for expressing the desired information. This possibility led to the idea of a generalized semantics for CLP programs, proposed in [24]. A generalized semantics is parameterized over the (possibly non-standard) constraint system which constitute the domain of the computation. The main advantages of this approach are that:

(i) different instances of CLP can be used to define non-standard semantics for constraint logic programs;
(ii) the semantics of these instances are all captured within a unified algebraic framework; and, in particular,

(iii) many relevant abstract interpretations of CLP programs can be thus formalized inside the CLP paradigm.

The next section is devoted to the class of ordered domains outlined above.

3.3 Constraint systems

Since we aim at a pervasive treatment, we would like to avoid talking too much about what a constraint is. However, for the formal treatment we have in mind, we cannot overlook some basic facts on the relationship between constraints and program variables. The purpose of constraints is, roughly speaking, to restrict the range of values variables can take. For our present objectives the following definition suffices.

Definition 5 (Constraint.) *The class of* constraints *is inductively defined as follows:*

(i) a well-formed formula of any first-order language $\mathcal{L}$ with variables' symbols in Vars is a constraint;
(ii) any set of constraints is a constraint;
(iii) any (meta-level) predicate p/n applied to n constraints is a constraint;
(iv) nothing is a constraint if not by virtue of (i), (ii), and (iii).

Now, on the relationship between constraints and variables, we can reason inductively as follows.

Definition 6 (Variables, free variables, and renaming.) *With reference to* Definition 5*, if c is a constraint by virtue of (i) then the notions of* variables of c *and of* free variables of c *are assumed as primitive. These sets of variables are denoted, respectively, by $vars(c)$ and $FV(c)$. An invertible and idempotent mapping from and to variable's symbols which is the identity almost everywhere is called* renaming*. We will use the notation $[\bar{Y}/\bar{X}]$ for renamings, where $\bar{Y}$ and $\bar{X}$ are disjoint tuples of distinct variables. The renaming $[Y/X]$ has no effect on c if $X \notin FV(C)$, whereas variables' capture is avoided by consistent renaming of bound variables. Besides that, the constraint $c[\bar{Y}/\bar{X}]$ is assumed as defined.*

If C is a constraint because of (ii) then $vars(C) \stackrel{\text{def}}{=} \bigcup_{c \in C} vars(c)$ and[3]

$$FV(C) \stackrel{\text{def}}{=} \left\{ X \in Vars \;\middle|\; \exists c \in C \,.\, \exists Y \in Vars \,.\, c[Y/X] \notin C \right\}. \qquad (1)$$

[3] This definition of FV is an adaptation of the one of *dependent variables* in [43, Definition 2.3].

With these definitions the notion of renaming for C is extended as expected. The application of a renaming to C is defined element-wise.

If $\mu(C_1, \ldots, C_n)$ is a constraint by virtue of (iii) then the above notions are extended as they would be in any first-order language.

In the sequel we will apply renamings carefully so that, when we write $C[\bar{Y}/\bar{X}]$, it is ensured that $FV(C) \cap \bar{Y} = \varnothing$. We will emphasize this fact by saying that $[\bar{Y}/\bar{X}]$ is a renaming *for* C.

All the members of our hierarchy of domains will turn out to be *constraint systems* in the precise sense stated by the following definition.

Definition 7 (Constraint system.) *Any algebra $\bar{\mathcal{D}}$ of the form*

$$\left\langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{\Lambda}}\}_{\vec{\Lambda} \in \Lambda^\star}, \{d_{\bar{X}\bar{Y}}\}_{\bar{X},\bar{Y} \in Vars^\star} \right\rangle$$

is a constraint system *if and only if it satisfies the following conditions:*

G_0. *$\mathcal{D}$ is a set of constraints;*
G_1. *$\langle \mathcal{D}, \otimes, \mathbf{1} \rangle$ is a commutative and idempotent monoid;*
G_2. *$\langle \mathcal{D}, \oplus, \mathbf{0} \rangle$ is a commutative and idempotent monoid;*
G_3. *$\mathbf{0}$ is an* annihilator *for $\otimes$, i.e., for each $C \in \mathcal{D}$, $C \otimes \mathbf{0} = \mathbf{0}$;*
G_4. *$\otimes$* absorbs *$\oplus$, i.e., for each $C_1, C_2 \in \mathcal{D}$, $C_1 \otimes (C_1 \oplus C_2) = C_1$;*
G_5. *for each $\vec{\Lambda} \in \Lambda^\star$ and $C \in \mathcal{D}$, it is $FV\left(\bar{\exists}_{\vec{\Lambda}} C\right) \subseteq \vec{\Lambda}$.*

A constraint system induces the relation $\vdash \subseteq \mathcal{D} \times \mathcal{D}$ given, for each $C_1, C_2 \in \mathcal{D}$, by

$$C_1 \vdash C_2 \quad \stackrel{\text{def}}{\iff} \quad C_1 \otimes C_2 = C_1. \tag{2}$$

The relation $\vdash$ is referred to as the approximation ordering *of the constraint system. The notation $C_1 \Vdash C_2$ stands for $C_1 \vdash C_2 \wedge C_1 \neq C_2$.*

In the sequel we will feel free to drop the quantifiers from the notation of the families of projection operators and diagonal elements.

Condition G_4 can be restated as

$$C_1 \vdash C_1 \oplus C_2 \quad \text{and} \quad C_2 \vdash C_1 \oplus C_2.$$

In this form it clearly stands for the correctness of the merge operation, characterizing it as a (not necessarily least) upper bound operator with respect to the approximation ordering.

Hypothesis 8 *Indeed, constraint systems must satisfy some other (very technical) conditions related to how they deal with variables. For instance, they do*

not invent new free variables: $FV(C_1 \otimes C_2) \subseteq FV(C_1) \cup FV(C_2)$*, and similarly for the merge operator. The operators are also* generic *in that they are insensible to variable names. This implies that, if* $[\bar{Y}/\bar{X}]$ *is a renaming for both* C_1 *and* C_2*, then*

$$(C_1 \otimes C_2)[\bar{Y}/\bar{X}] = C_1[\bar{Y}/\bar{X}] \otimes C_2[\bar{Y}/\bar{X}].$$

In particular, if we have also $C_1 \vdash C_2$*, then* $C_1[\bar{Y}/\bar{X}] \vdash C_2[\bar{Y}/\bar{X}]$*. In the sequel we will take all these overwhelmingly reasonable requirements for granted.*

Constraint systems enjoy several properties.

Proposition 9 (Properties of c.s.) *Any constraint system satisfies the following properties, for each* $C, C_1, C_2 \in \mathcal{D}$*:*

(i) $\langle \mathcal{D}, \vdash, \otimes, \mathbf{0}, \mathbf{1} \rangle$ *is a bounded meet-semilattice;*
(ii) $C \oplus \mathbf{1} = \mathbf{1}$*;*
(iii) $C_1 \vdash C_1 \oplus (C_1 \otimes C_2)$*;*
(iv) $C_1 \oplus C_2 = C_2 \quad \Longrightarrow \quad C_1 \vdash C_2$*.*

PROOF.

(i) First of all, axiom G_1 implies that $\vdash$ is a partial order. Reflexivity, transitivity, and antisymmetry of $\vdash$ come, respectively, from idempotence, associativity, and commutativity of $\otimes$. The ordering definition (2) ensures that $\otimes$ is the greatest lower bound operator with respect to $\vdash$. G_3 and G_1 imply that $\mathbf{0}$ and $\mathbf{1}$ are the minimum and maximum elements wrt $\vdash$.
(ii) Notice that, for each $C \in \mathcal{D}$, $\mathbf{1} \otimes (\mathbf{1} \oplus C) = \mathbf{1}$ is an instance of G_4, which, by G_1 becomes $\mathbf{1} \oplus C = \mathbf{1}$.
(iii) By G_4 we have $C_1 \otimes \Big(C_1 \oplus (C_1 \otimes C_2)\Big) = C_1$, whence the thesis.
(iv) Suppose $C_1 \oplus C_2 = C_2$. Then G_4 implies $C_1 \otimes C_2 = C_1 \otimes (C_1 \oplus C_2) = C_1$, thus $C_1 \vdash C_2$. $\square$

Observe that $\langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1} \rangle$, in general, is not a lattice. Both $\otimes$ and $\oplus$ are associative, commutative, and idempotent, but, as stated above, while one of the absorption laws holds (axiom G_4 of Definition 7), only one direction of the dual law is generally valid (property (iii) of Proposition 9). In particular, $\oplus$ might be not component-wise monotone with respect to $\vdash$: for each $C_1, C_2 \in \mathcal{D}$, from the obvious relations $C_1 \otimes C_2 \vdash C_2$ and $C_2 \vdash C_2$ we would get $(C_1 \otimes C_2) \oplus C_2 \vdash C_2$. Observe also that $\oplus$ does not distribute, in general, over $\otimes$, as this would imply the equivalence of the two absorption laws.

So far for generic constraint systems, we consider now some strengthenings of Definition 7.

Definition 10 (Closed c.s.) *A constraint system is said* closed *if*

G_c. *for each family* $\{C_i \in \mathcal{D}\}_{i\in\mathbb{N}}$, $\bigoplus_{i\in\mathbb{N}} C_i \stackrel{\text{def}}{=} C_1 \oplus C_2 \oplus \cdots$ *exists and is unique in* $\mathcal{D}$*; moreover, associativity, commutativity, and idempotence of* $\oplus$ *apply to denumerable as well as to finite families of operands.*

So, the operation of merging together the information coming from all the computation paths always makes sense in a closed constraint system. Notice however that property G_c is only necessary when the semantic construction requires it. This will never happen when considering "abstract semantic constructions" formalizing data-flow analyses (which are finite in nature). In these cases the idea of merging infinitely many pieces of information is a nonsense in itself. Closedness will instead be a must for the constraint systems intended to capture "concrete" program semantics.

Another optional property of constraint systems that we will mention is distributivity.

Definition 11 (Distributive c.s.) *Consider the following conditions:*

G_d. $\langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}\rangle$ *is a distributive lattice;*
G_D. *for each* $C \in \mathcal{D}$ *and each family* $\{C_i \in \mathcal{D}\}_{i\in\mathbb{N}}$ *such that* $\bigoplus_{i\in\mathbb{N}} C_i$ *exists,* $C \otimes (\bigoplus_{i\in\mathbb{N}} C_i) = \bigoplus_{i\in\mathbb{N}} (C \otimes C_i)$.

A constraint system is said distributive *if it satisfies* G_d*. If it satisfies the stronger condition* G_D *then it is said* completely distributive.

Distributivity is useful for proving the equivalence of different abstract semantics constructions used for data-flow analysis. Complete distributivity is required for proving that a concrete semantics corresponds to the operational model of the language [24]. Observe that closed and completely distributive constraint systems are instances of the *closed semi-rings* used in [24].

Definition 12 (Noetherian c.s.) *A constraint system is said* Noetherian *if is satisfy the* ascending chain condition*:*

G_N. *in* $\mathcal{D}$ *every strictly ascending chain,* $C_0 \Vdash C_1 \Vdash C_2 \Vdash \cdots$*, is finite.*

For the abstract semantics constructions we will make use of another class of operators over constraints. These operators were introduced in [13] and called *widenings*.

Definition 13 (Widening.) [13] *Given a constraint system* $\bar{\mathcal{D}}$*, a binary operator* $\nabla\colon \mathcal{D} \to \mathcal{D}$ *is called a* widening for $\bar{\mathcal{D}}$ *if*

W_1. *for each* $C_1, C_2 \in \mathcal{D}$ *we have* $C_1 \vdash C_1 \nabla C_2$ *and* $C_2 \vdash C_1 \nabla C_2$*;*

W_2. *for each increasing chain* $C_0 \vdash C_1 \vdash C_2 \vdash \cdots$, *the sequence given by* $C'_0 \stackrel{\text{def}}{=} C_0$ *and, for* $n \geq 1$, $C'_n \stackrel{\text{def}}{=} C'_{n-1} \nabla C_n$, *is stationary after some* $k \in \mathbb{N}$.

Widenings allow to define *convergence acceleration methods* which ensure termination of the "abstract interpreter". However, even when termination is granted anyway (e.g., when the constraint system is Noetherian), these methods are often crucial for achieving *rapid* termination, that is, for obtaining usable data-flow analyzers. More sophisticated methods for convergence acceleration exist which employ also *narrowing* operators, and more complex widenings than the ones defined above (see [17,16]).

3.4 Generalized semantics

In a generalized semantics setting, the first thing to do is to provide atomic constraints with an interpretation on the chosen constraint system. Suppose that we are interested in deriving information about just two kind of program points: clause's entries and clause's successful exits. In a data-flow analysis setting (where this is often the case) that is to say that we want to derive *call-patterns* and *success-patterns*. In other words, for each clause we want to derive properties of the constraint store which are valid

- whenever the clause is invoked (call-patterns);
- whenever a computation starting with the invocation of the clause terminates with success (success-patterns).

Observe that call-patterns depend on the ordering of atoms in the body of clauses and on the selection rule employed. By means of program transformations similar to the *magic* one [9,21] we can obtain the call-patterns of the original program (with respect to the selection rule employed) as success-patterns of the transformed one. These transformations, in fact, besides modifying the clauses of the original program, introduce new clauses that characterize the conditions under which the original clauses are invoked. In the transformed program the ordering of atoms in the clause's bodies is no longer important. Notice that the technique proposed in [21], while restricted to logic programs [4], is more sophisticated than usual transformation approaches, and allows not to loose the connection between call and success patterns. For these reasons we will consider only one kind of program points: clause's exits. Furthermore, in our domains the operation capturing constraint composition is associative, commutative, and idempotent. This means that we can assume without preju-

[4] Actually, we have developed a technique, still based on program transformation, which is general enough to accommodate the entire CLP framework [48].

dice that all the clauses are of the form

$$p(\vec{\Lambda}) :- \{c_1, \ldots, c_n\} \,\square\, \{b_1, \ldots, b_k\},$$

where $\{c_1, \ldots, c_n\}$ is a set of atomic constraints, and $\{b_1, \ldots, b_k\}$ is a set of atoms. All the other restrictions imposed by Definition 3 must continue to hold. We now must associate a meaning to the finite sets of atomic constraints which occurs in clauses.

Definition 14 (Constraint interpretation.) *Given a language* C *of atomic constraints and a domain of interpretation* $\bar{\mathcal{D}}$*, a* constraint interpretation of C in $\bar{\mathcal{D}}$ *is a computable function* $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}} : \wp_f(\mathsf{C}) \to \mathcal{D}$.

Then usually one considers, instead of the *syntactic* program P, its *semantic* version over the domain $\bar{\mathcal{D}}$, obtained by interpreting the atomic constraints of clauses through $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}}$. Recall that, for $r = 1, \ldots, \#P$, we denote by $P[r]$ the r-th clause of P.

Definition 15 (Generalized program.) *When* $\bar{\mathcal{D}}$ *is a constraint system, a* $\mathrm{CLP}(\bar{\mathcal{D}})$ program *is a sequence of Horn-like formulas of the form*

$$p(\vec{\Lambda}) :- C \,\square\, \{b_1, \ldots, b_k\},$$

where $C \in \bar{\mathcal{D}}$ *is finitely representable. Given a* $\mathrm{CLP}(\mathsf{C})$ *program* P *and a constraint interpretation* $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}}$*, the* $\mathrm{CLP}(\bar{\mathcal{D}})$ *program* $[\![P]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}}$ *is given, for each* $r = 1, \ldots, \#P$*, by*

$$[\![P]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}}[r] \equiv p(\vec{\Lambda}) :- [\![C]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}} \,\square\, B \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad P[r] \equiv p(\vec{\Lambda}) :- C \,\square\, B. \tag{3}$$

An interpretation for a program P over a constraint system $\bar{\mathcal{D}}$ is a function from its program points (one for each clause) to $\mathcal{D}$. Notice that we deviate from standard approaches in that our interpretations associate a meaning to *each distinct program rule*, not to each distinct program predicate [4].

Definition 16 (Interpretation.) *Let* $\bar{\mathcal{D}}$ *be a constraint system, and* P *a* $\mathrm{CLP}(\bar{\mathcal{D}})$ *program. An* interpretation for P over $\bar{\mathcal{D}}$ *is any element of*

$$\mathcal{I}_P^{\bar{\mathcal{D}}} \stackrel{\text{def}}{=} \{1, \ldots, \#P\} \to \mathcal{D}.$$

All the operations and relations over $\bar{\mathcal{D}}$ *are extended point-wise to* $\mathcal{I}_P^{\bar{\mathcal{D}}}$*. In particular* $\mathcal{I}_P^{\bar{\mathcal{D}}}$ *is partially ordered by the lifting of* $\vdash$*, i.e., for each* $I_1, I_2 \in \mathcal{I}_P^{\bar{\mathcal{D}}}$*,*

$$I_1 \vdash I_2 \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \forall r \in \{1, \ldots, \#P\} : I_1(r) \vdash I_2(r).$$

Interpretations will be represented by means of function graphs.

It is straightforward to show that all the interesting properties of constraint systems lift smoothly to interpretations.

We are left with the choice of the semantics construction, that is, of the "interpretation transformer". For the purpose of this work we choose a bottom-up construction expressed by a flavor of the usual *immediate consequence operator* T_P, taking an interpretation and returning a new interpretation. More specifically, this transformer takes the information arising from a set of finite computation paths and gives back the information relative to those computation paths induced by the program starting from the input ones.

Recall that our set of program variables is $\mathit{Vars} = \Lambda \uplus V$, where Λ and V are totally ordered. For $\vec{\Lambda} \in \Lambda^\star$ and $W \subseteq_f \mathit{Vars}$, we denote by $\bar{Y} \ll_{\vec{\Lambda}} W$ the fact that, with respect to the ordering of V, $\bar{Y}$ is a tuple of distinct consecutive variables in V such that $\#\bar{Y} = \#\vec{\Lambda}$ and the first element of $\bar{Y}$ immediately follows the greatest variable in W.

Definition 17 (Interpretation transformer.) *Let P be a* CLP($\bar{\mathcal{D}}$) *program, where $\bar{\mathcal{D}}$ is a constraint system. The operator induced by P over $\mathcal{I}_P^{\bar{\mathcal{D}}}$, $T_P^{\bar{\mathcal{D}}} \colon \mathcal{I}_P^{\bar{\mathcal{D}}} \to \mathcal{I}_P^{\bar{\mathcal{D}}}$, is*

$$T_P^{\bar{\mathcal{D}}}(I) \stackrel{\text{def}}{=} \left\{ \left(r, T_P^{\bar{\mathcal{D}}}(r, I)\right) \;\middle|\; 1 \leq r \leq \#P \right\}, \tag{4}$$

where $T_P^{\bar{\mathcal{D}}} \colon \{1, \ldots, \#P\} \times \mathcal{I}_P^{\bar{\mathcal{D}}} \to \mathcal{D}$ is given by

$$T_P^{\bar{\mathcal{D}}}(r, I) \stackrel{\text{def}}{=} \bigoplus \left\{ \bar{\exists}_{\vec{\Lambda}} \tilde{C} \;\middle|\; \begin{array}{l} P[r] \equiv p(\vec{\Lambda}) \mathrel{:-} C \mathbin{\square} \left\{p_1(\bar{X}_1), \ldots, p_n(\bar{X}_n)\right\} \\ \textit{and, for each } i = 1, \ldots, n\textit{:} \\ \qquad P[r_i] \equiv p_i(\vec{\Lambda}_i) \mathrel{:-} C_i \mathbin{\square} B_{r_i} \\ \qquad \bar{Y}_i \ll_{\vec{\Lambda}_i} FV\left(P[r]\right) \cup \bar{Y}_1 \cup \cdots \cup \bar{Y}_{i-1} \\ \qquad \tilde{C}_i = I(r_i)[\bar{Y}_i / \vec{\Lambda}_i] \\ \qquad C_i' = d_{\bar{X}_i \bar{Y}_i} \otimes \tilde{C}_i \\ \tilde{C} = C \otimes C_1' \otimes \cdots \otimes C_n' \end{array} \right\}. \tag{5}$$

Notice that, in this construction, the merge operator is applied only to finite sets of operands. In summary, once we have fixed the constraint domain $\bar{\mathcal{D}}$ and the interpretation of atomic constraints $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}}$, the meaning of a CLP($\mathsf{C}$) program P over $\bar{\mathcal{D}}$ is encoded into the $T_P^{\bar{\mathcal{D}}}$ operator. Before rushing to require that $T_P^{\bar{\mathcal{D}}}$ must be continuous on the complete lattice $\bar{\mathcal{D}}$ we better have a closer look to our real needs.

Given our current focus on data-flow analysis of CLP programs, we only consider, for simplicity, the typical case in this field. On one hand we have a "concrete" constraint system $\bar{\mathcal{D}}^\natural$: it must capture the properties of interest, it must ensure the existence of the least fixpoint of $T_{P^\natural}^{\bar{\mathcal{D}}^\natural}$, that is, of *the* meaning of each program P. And, of course, this meaning must correspond to the one obtained by means of the top-down construction representing the operational model of the language (namely, some kind of extended SLD-resolution). This last requirement implies, as shown in [24], that $\bar{\mathcal{D}}^\natural$ must be closed and completely distributive, hence a complete lattice.

One the other hand, in data-flow analysis, we have an "abstract" constraint system $\bar{\mathcal{D}}^\sharp$. Here we are much less demanding: we simply want to compute in a *finite* way an approximation of a post-fixpoint of $T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}$ (the least fixpoint might not even exist, or it might be too expensive to compute). And, of course, we need a guarantee that what we compute is a *correct* approximation of the concrete meaning. Finite computability can be ensured, in general, by using a widening operator.

Thus, in this setting, the concrete and abstract iteration sequences defining, respectively, the concrete meaning and approximations of the abstract meaning of programs are quite different.

Definition 18 (Concrete and abstract iteration sequences.) *Consider a closed and completely distributive constraint system $\bar{\mathcal{D}}^\natural$, and a CLP($\bar{\mathcal{D}}^\natural$) program $P^\natural$. The* concrete iteration sequence *for $P^\natural$ is inductively defined as follows, for all ordinals $\kappa \in \mathbb{O}$:*

$$\begin{cases} T_{P^\natural}^{\bar{\mathcal{D}}^\natural} \uparrow 0 \stackrel{\text{def}}{=} \mathbf{0}^\natural, \\ T_{P^\natural}^{\bar{\mathcal{D}}^\natural} \uparrow (\kappa+1) \stackrel{\text{def}}{=} T_{P^\natural}^{\bar{\mathcal{D}}^\natural}\Big(T_{P^\natural}^{\bar{\mathcal{D}}^\natural} \uparrow \kappa\Big), \\ T_{P^\natural}^{\bar{\mathcal{D}}^\natural} \uparrow \kappa \stackrel{\text{def}}{=} \bigoplus_{\beta<\kappa}\Big(T_{P^\natural}^{\bar{\mathcal{D}}^\natural} \uparrow \beta\Big), \quad \textit{when } \kappa > 0 \textit{ is a limit ordinal.} \end{cases} \tag{6}$$

Let $\bar{\mathcal{D}}^\sharp$ be any constraint system, and let $\nabla^\sharp$ be a widening operator over $\bar{\mathcal{D}}^\sharp$. For a CLP($\bar{\mathcal{D}}^\sharp$) *program $P^\sharp$, the* abstract iteration sequence for $P^\sharp$ with widening $\nabla^\sharp$ *is inductively defined by*

$$\begin{cases} T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} \Uparrow 0 \stackrel{\text{def}}{=} \mathbf{0}^\sharp, \\ T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} \Uparrow (k+1) \stackrel{\text{def}}{=} \Big(T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} \Uparrow k\Big) \nabla^\sharp T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}\Big(T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} \Uparrow k\Big), \quad \textit{for } k \in \mathbb{N}. \end{cases} \tag{7}$$

Observe that, when $\bar{\mathcal{D}}^\sharp$ is Noetherian or when termination can be ensured in other ways, π_2 (the second projection) can be substituted for $\nabla^\sharp$ in (7). In

these cases, indeed, the restriction of π_2 to the iterates' values is a widening operator.

The following fact is easily shown with standard techniques [24].

Theorem 19 *If $\bar{\mathcal{D}}^\sharp$ is a closed and completely distributive constraint system then, for each CLP($\bar{\mathcal{D}}^\sharp$) program $P^\sharp$ the least fixpoint of $T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}$ exists and is given by $lfp(T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}) = T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} \uparrow \omega$.*

We now come at the problem of ensuring the correctness of the analysis. We use an *abstraction correspondence* between the concrete and the abstract constraint systems, which induces an abstraction correspondence between the respective semantics [7,16].

Definition 20 (Abstraction function.) *Let $\bar{\mathcal{D}}^\natural$ and $\bar{\mathcal{D}}^\sharp$ be two constraint systems as in* Definition 18. *A function $\alpha\colon \mathcal{D}^\natural \to \mathcal{D}^\sharp$ is an* abstraction function *of $\bar{\mathcal{D}}^\natural$ into $\bar{\mathcal{D}}^\sharp$ if and only if*

A_1. *α is a* semi-morphism, *namely, for each $C^\natural, C_1^\natural, C_2^\natural, d_{\bar{X}\bar{Y}}^\natural \in \mathcal{D}^\natural$ and $\vec{\Lambda} \in \Lambda^\star$:*

$$\begin{aligned}
\alpha(C_1^\natural \otimes^\natural C_2^\natural) &\vdash^\sharp \alpha(C_1^\natural) \otimes^\sharp \alpha(C_2^\natural),\\
\alpha(C_1^\natural \oplus^\natural C_2^\natural) &\vdash^\sharp \alpha(C_1^\natural) \oplus^\sharp \alpha(C_2^\natural),\\
\alpha(\mathbf{0}^\natural) &\vdash^\sharp \mathbf{0}^\sharp,\\
\alpha\Big(\bar{\exists}_{\vec{\Lambda}}^\natural C^\natural\Big) &\vdash^\sharp \bar{\exists}_{\vec{\Lambda}}^\sharp \alpha(C^\natural),\\
\alpha\Big(d_{\bar{X}\bar{Y}}^\natural\Big) &\vdash^\sharp d_{\bar{X}\bar{Y}}^\sharp;
\end{aligned}$$

A_2. *for each increasing chain $\{C_j^\natural \in \mathcal{D}^\natural\}_{j\in\mathbb{N}}$,*

$$\exists C^\sharp \in \mathcal{D}^\sharp \,.\, \forall j \in \mathbb{N} : \alpha(C_j^\natural) \vdash^\sharp C^\sharp \quad \Longrightarrow \quad \alpha\Big(\bigoplus_{j\in\mathbb{N}}^\natural C_j^\natural\Big) \vdash^\sharp C^\sharp;$$

A_3. *for each $C^\natural \in \mathcal{D}^\natural$ and each renaming $[\bar{Y}/\bar{X}]$ for $C^\natural$, it happens that*

$$\alpha(C^\natural)[\bar{Y}/\bar{X}] = \alpha\Big(C^\natural[\bar{Y}/\bar{X}]\Big).$$

Any abstraction function $\alpha\colon \mathcal{D}^\natural \to \mathcal{D}^\sharp$ is naturally extended to $\alpha\colon \mathcal{I}_{P^\natural}^{\bar{\mathcal{D}}^\natural} \to \mathcal{I}_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}$, when $\#P^\natural = \#P^\sharp$, in the obvious way.

As anticipated above, one of the beautiful things of the generalized approach is that the abstract meaning of CLP programs can be encoded into other CLP programs. We have thus an *abstract compilation* approach, where the soundness of the *compilation function* $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\sharp}$ is expressed, for CLP(C) programs, by the requirement $\alpha \circ [\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\natural} \vdash^\sharp [\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\sharp}$. The following result is crucial for proving the correctness of the methodology.

Lemma 21 *Consider a* CLP(C) *program* P*, two constraint systems* $\bar{\mathcal{D}}^\natural$ *and* $\bar{\mathcal{D}}^\sharp$*, the constraint interpretations* $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\natural}$ *and* $[\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\sharp}$*, and the abstraction function* $\alpha\colon \mathcal{D}^\natural \to \mathcal{D}^\sharp$ *such that* $\alpha \circ [\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\natural} \vdash^\sharp [\![\cdot]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\sharp}$*,* $P^\natural = [\![P]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\natural}$ *and* $P^\sharp = [\![P]\!]_{\mathsf{C}}^{\bar{\mathcal{D}}^\sharp}$*. Then*

$$\forall I^\natural \in \mathcal{I}_{P^\natural}^{\bar{\mathcal{D}}^\natural} : \forall I^\sharp \in \mathcal{I}_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} : \alpha(I^\natural) \vdash^\sharp I^\sharp \implies \alpha\Big(T_{P^\natural}^{\bar{\mathcal{D}}^\natural}(I^\natural)\Big) \vdash^\sharp T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}(I^\sharp).$$

PROOF. It is enough to show that, for each $r = 1, \ldots, \#P$ we have

$$\forall I^\natural \in \mathcal{I}_{P^\natural}^{\bar{\mathcal{D}}^\natural} : \forall I^\sharp \in \mathcal{I}_{P^\sharp}^{\bar{\mathcal{D}}^\sharp} : \alpha(I^\natural) \vdash^\sharp I^\sharp \implies \alpha\Big(T_{P^\natural}^{\bar{\mathcal{D}}^\natural}(r, I^\natural)\Big) \vdash^\sharp T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}(r, I^\sharp).$$

Suppose that $I^\natural$ and $I^\sharp$ satisfy the hypothesis, i.e., for each clause r' such that $1 \leq r' \leq \#P$ we have $\alpha(I^\natural(r')) \vdash^\sharp I^\sharp(r')$. Then, for

$$P^\natural[r] \equiv p(\vec{\Lambda}) :- C^\natural \,\square\, \Big\{p_1(\bar{X}_1), \ldots, p_n(\bar{X}_n)\Big\},$$

we have $T_{P^\natural}^{\bar{\mathcal{D}}^\natural}\Big(r, I^\natural\Big) = \bigoplus_{j\in J}^\natural \hat{C}_j^\natural$ and $T_{P^\sharp}^{\bar{\mathcal{D}}^\sharp}\Big(r, I^\sharp\Big) = \bigoplus_{j\in J}^\sharp \hat{C}_j^\sharp$, for some finite set of indices J. Moreover, we can stipulate without prejudice that, for each $j \in J$ and each $i = 1, \ldots, n$, the clause r_{ij} has been used to "resolve" against the i-th atom in the body of r in order to produce *both* $\hat{C}_j^\natural$ and $\hat{C}_j^\sharp$. Thus

$$\hat{C}_j^\natural = \bar{\exists}_{\vec{\Lambda}}^\natural\left(C^\natural \otimes^\natural \bigotimes_{i=1}^n{}^\natural\Big(d_{\bar{X}_i\bar{Y}_i}^\natural \otimes^\natural \tilde{C}_{ij}^\natural\Big)\right) \quad \text{and}$$
$$\hat{C}_j^\sharp = \bar{\exists}_{\vec{\Lambda}}^\sharp\left(C^\sharp \otimes^\sharp \bigotimes_{i=1}^n{}^\sharp\Big(d_{\bar{X}_i\bar{Y}_i}^\sharp \otimes^\sharp \tilde{C}_{ij}^\sharp\Big)\right),$$

where $\tilde{C}_{ij}^\natural = I^\natural(r_{ij})[\bar{Y}_i/\vec{\Lambda}_i]$ and $\tilde{C}_{ij}^\sharp = I^\sharp(r_{ij})[\bar{Y}_i/\vec{\Lambda}_i]$. By the hypotheses we have $\alpha(C^\natural) \vdash^\sharp C^\sharp$, and, using Hypothesis 8, we have also that for each $i = 1, \ldots, n$ and each $j \in J$ it is

$$\alpha\Big(I^\natural(r_{ij})[\bar{Y}_i/\vec{\Lambda}_i]\Big) = \alpha\Big(I^\natural(r_{ij})\Big)[\bar{Y}_i/\vec{\Lambda}_i] \vdash^\sharp I^\sharp(r_{ij})[\bar{Y}_i/\vec{\Lambda}_i],$$

thus $\alpha(\tilde{C}_{ij}^\natural) \vdash^\sharp \tilde{C}_{ij}^\sharp$. Now we can easily conclude:

$$
\begin{aligned}
\alpha\Big(T^{\bar{\mathcal{D}}^\natural}_{P^\natural}\big(r, I^\natural\big)\Big) &= \alpha\Big(\bigoplus\nolimits^\natural_{j\in J} \hat{C}^\natural_j\Big) \\
&\vdash^\sharp \bigoplus\nolimits^\sharp_{j\in J} \alpha\big(\hat{C}^\natural_j\big) \\
&= \bigoplus\nolimits^\sharp_{j\in J} \alpha\Big(\bar{\exists}^\natural_{\vec{\Lambda}}\Big(C^\natural \otimes^\natural \bigotimes\nolimits^{n\,\natural}_{i=1}\big(d^\natural_{\bar{X}_i\bar{Y}_i} \otimes^\natural \tilde{C}^\natural_{ij}\big)\Big)\Big) \\
&\vdash^\sharp \bigoplus\nolimits^\sharp_{j\in J} \bar{\exists}^\sharp_{\vec{\Lambda}}\, \alpha\Big(C^\natural \otimes^\natural \bigotimes\nolimits^{n\,\natural}_{i=1}\big(d^\natural_{\bar{X}_i\bar{Y}_i} \otimes^\natural \tilde{C}^\natural_{ij}\big)\Big) \\
&\vdash^\sharp \bigoplus\nolimits^\sharp_{j\in J} \bar{\exists}^\sharp_{\vec{\Lambda}}\Big(C^\sharp \otimes^\sharp \bigotimes\nolimits^{n\,\sharp}_{i=1}\Big(\alpha\big(d^\natural_{\bar{X}_i\bar{Y}_i}\big) \otimes^\sharp \alpha\big(\tilde{C}^\natural_{ij}\big)\Big)\Big) \\
&\vdash^\sharp \bigoplus\nolimits^\sharp_{j\in J} \bar{\exists}^\sharp_{\vec{\Lambda}}\Big(C^\sharp \otimes^\sharp \bigotimes\nolimits^{n\,\sharp}_{i=1}\big(d^\sharp_{\bar{X}_i\bar{Y}_i} \otimes^\sharp \tilde{C}^\sharp_{ij}\big)\Big) \\
&= T^{\bar{\mathcal{D}}^\sharp}_{P^\sharp}\big(r, I^\sharp\big). \qquad \square
\end{aligned}
$$

Theorem 22 *Given a* CLP(C) *program P, two constraint systems $\bar{\mathcal{D}}^\natural$ and $\bar{\mathcal{D}}^\sharp$, the constraint interpretations $[\![\cdot]\!]^{\bar{\mathcal{D}}^\natural}_{\mathsf{C}}$ and $[\![\cdot]\!]^{\bar{\mathcal{D}}^\sharp}_{\mathsf{C}}$, and the abstraction function $\alpha\colon \mathcal{D}^\natural \to \mathcal{D}^\sharp$ such that $\alpha \circ [\![\cdot]\!]^{\bar{\mathcal{D}}^\natural}_{\mathsf{C}} \vdash^\sharp [\![\cdot]\!]^{\bar{\mathcal{D}}^\sharp}_{\mathsf{C}}$, $P^\natural = [\![P]\!]^{\bar{\mathcal{D}}^\natural}_{\mathsf{C}}$ and $P^\sharp = [\![P]\!]^{\bar{\mathcal{D}}^\sharp}_{\mathsf{C}}$, we have that the abstract iteration with widening* (7) *is eventually stable after $\ell \in \mathbb{N}$ steps and*

$$
\alpha\Big(\mathit{lfp}(T^{\bar{\mathcal{D}}^\natural}_{P^\natural})\Big) = \alpha\Big(T^{\bar{\mathcal{D}}^\natural}_{P^\natural} \uparrow \omega\Big) \vdash^\sharp \Big(T^{\bar{\mathcal{D}}^\sharp}_{P^\sharp} \Uparrow \ell\Big).
$$

PROOF. A straightforward application of a theorem in [16, Proposition 6.20]. Stability of the iteration (7) after $\ell \in \mathbb{N}$ comes from the properties of widenings. The rest of the proof is carried on using transfinite induction: the base case is given by property A_1 of abstraction functions, non-limit ordinals are handled through Lemma 21, whereas for limit ordinals property A_2 is exploited. $\square$

We now describe a hierarchy of constraint systems which capture most of the analysis domains used for deriving monotonic properties of programs, as well as the "concrete" collecting semantics they abstract.

The basis is constituted by any constraint system which satisfies the conditions of Definition 7. First we show a way (which, of course, is not the only one) of defining such a constraint system. We start from a set of finite constraints, each expressing some partial information about a program execution's state (i.e., a constraint-store). Once this is given (simple constraint systems, Section 4), we provide standard ways of representing and composing finite constraints (determinate constraint systems, Section 5). Then we introduce a well-known

construction which allows us to treat *disjunctive information* (powerset constraint systems, Section 6). Later we will show how the notion of *dependency* can be built into the constraint system (ask-and-tell constraint systems Section 7). Finally, in Section 8 we sketch how to achieve combination of domains by considering dependencies within *product constraint systems*. We feel that, indeed, this is one of the more important contributions of this work.

4 Simple constraint systems

The basic blocks of our construction are *simple constraint systems* (or s.c.s.), very similar to those of [45], but with a *totally uninformative* token ($\top$) as in [47].

Definition 23 (Simple constraint system.) *A* simple constraint system *is a structure* $\langle \mathcal{C}, \vdash, \bot, \top \rangle$*, where* $\mathcal{C}$ *is a set of constraints,* $\bot \in \mathcal{C}$*,* $\top \in \mathcal{C}$*, and* $\vdash \subseteq \wp_f(\mathcal{C}) \times \mathcal{C}$ *is an* entailment relation *such that, for each* $C, C' \in \wp_f(\mathcal{C})$*, each* $c, c' \in \mathcal{C}$*, and* $X, Y \in Vars$*:*

$E_1.\ c \in C \quad \Longrightarrow \quad C \vdash c;$
$E_2.\ C \vdash \top;$
$E_3.\ (C \vdash c) \wedge (\forall c' \in C : C' \vdash c') \quad \Longrightarrow \quad C' \vdash c;$
$E_4.\ \{\bot\} \vdash c;$
$E_5.\ C \vdash c \quad \Longrightarrow \quad C[Y/X] \vdash c[Y/X].$

The '$\vdash$' symbol is overloaded to denote also the extension $\vdash \subseteq \wp(\mathcal{C}) \times \wp(\mathcal{C})$ *such that, for each* $C, C' \in \wp(\mathcal{C})$*,*

$$C \vdash C' \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \forall c' \in C' : \exists C'' \subseteq_f C \,.\, C'' \vdash c'.$$

It is clear that condition E_1 implies reflexivity of $\vdash$, while condition E_3 amounts to transitivity. E_2 qualifies $\top$ as the least informative token: it will be needed just as a "marker" when the *product* of simple constraint systems will be considered (see Section 8). E_4 ensures that $\mathcal{C}$ is a finitely generable element (see Definition 25). Condition E_5, referred to as *genericity* states that the entailment is insensible to variables' names [5].

By axioms E_1 and E_3 of Definition 23 the entailment relation of a simple constraint system is a preorder. Now, instead of considering the quotient poset

[5] In [43] a stronger notion of genericity is used, namely $C[t/X] \vdash c[t/X]$ whenever $C \vdash c$, for any term t. This is too strong for our purposes. For instance, it would force us to treat non-linear numeric constraints in the same way as linear ones in CLP($\mathcal{R}$).

with respect to the induced equivalence relation, a particular choice of the equivalence classes' representatives is made: closed sets with respect to entailment. This representation is a very convenient domain-independent strong normal form for constraints.

Definition 24 (Elements.) [45] *The* elements *of an s.c.s.* $\langle \mathcal{C}, \vdash, \bot, \top \rangle$ *are the* entailment-closed *subsets of* $\mathcal{C}$*, namely those* $C \subseteq \mathcal{C}$ *such that, whenever* $\exists C' \subseteq_f C \,.\, C' \vdash c$*, then* $c \in C$*. The set of elements of* $\langle \mathcal{C}, \vdash, \bot, \top \rangle$ *is denoted by* $|\mathcal{C}|$*.*

The poset of elements is thus given by $\langle |\mathcal{C}|, \supseteq \rangle$. Notice that we deviate from [45] in that we order our constraint systems in the dual way.

Definition 25 (Inference map, finite elements.) *Given a simple constraint system* $\langle \mathcal{C}, \vdash, \bot, \top \rangle$*, the* inference map *of* $\langle \mathcal{C}, \vdash, \bot, \top \rangle$ *is* $\rho \colon \wp(\mathcal{C}) \to \wp(\mathcal{C})$ *given, for each* $C \subseteq \mathcal{C}$*, by*

$$\rho(C) \stackrel{\text{def}}{=} \{\, c \mid \exists C' \subseteq_f C \,.\, C' \vdash c \,\}.$$

It is well known that ρ *is a kernel operator, over the complete lattice* $\langle \wp(\mathcal{C}), \supseteq \rangle$*, whose image is* $|\mathcal{C}|$*. The image of the restriction of* ρ *onto* $\wp_f(\mathcal{C})$ *is denoted by* $|\mathcal{C}|_0$*. Elements of* $|\mathcal{C}|_0$ *are called* finitely generated constraints *or simply* finite constraints.

From here on we will only work with finitely generated constraints, since we are not concerned with infinite behavior of (CLP) programs.

In general, describing the "standard" semantics of a CLP($\mathcal{X}$) language is done as follows. Let T be the theory which corresponds to the domain $\mathcal{X}$ [30]. Let D be an appropriate set of formulas in the vocabulary of T closed under conjunction and existential quantification. Define $\Gamma \vdash c$ iff Γ entails c in the logic, with non-logical axioms T. Then $(D, \vdash)$ is the required simple constraint system. For CLP($\mathcal{H}$) (i.e. pure Prolog) one takes the Clark's theory of equality in some disguise (see Section 4.3). For CLP($\mathbb{R}$)[6] the theory RCF of real closed fields would do the job. We see now some examples of simple constraint systems.

4.1 The atomic simple constraint system

This is probably the simplest useful example of s.c.s. The tokens include variable names. A variable name, when present in a constraint, expresses the fact

[6] Beware not to confuse CLP($\mathbb{R}$), the *idealized* language over the reals [32], with CLP($\mathcal{R}$), the (far from ideal) implemented language and system [31].

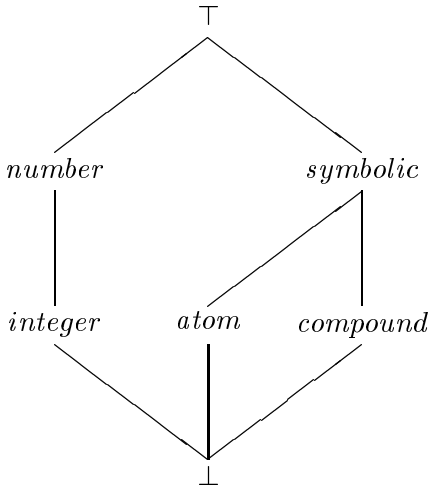

Fig. 1. A lattice of simple types.

that the variable has some (unspecified) property. For instance, being definitely bound to a *ground* value. In this case, X is just a shorthand for $ground(X)$. This s.c.s. is thus given by $\mathcal{C} \stackrel{\text{def}}{=} Vars \cup \{\bot, \top\}$ and by the smallest relation $\vdash \subseteq \wp_f(\mathcal{C}) \times \mathcal{C}$ satisfying conditions E_1–E_5 of Definition 23. In the sequel we will refer to this structure as to the *atomic* s.c.s.

A useful extension is to include tokens involving two variable names. These tokens state that the two variables involved share the property of interest: one enjoys it iff the other one does. More formally, we have

$$\mathcal{C}' \stackrel{\text{def}}{=} \mathcal{C} \cup \{\, X \leftrightharpoons Y \mid X, Y \in Vars \,\},$$

and the entailment relation is suitably extended to C' requiring, for each $X, Y, Z \in Vars$:

$$\begin{aligned} \{X \leftrightharpoons Y\} &\vdash Y \leftrightharpoons X; \\ \{X \leftrightharpoons Y, Y \leftrightharpoons Z\} &\vdash X \leftrightharpoons Z; \\ \{X, X \leftrightharpoons Y\} &\vdash Y. \end{aligned}$$

4.2 A simple constraint system for simple types

A slightly more interesting example is when we have more than one monadic (constraint) predicate. This is the case of domains of *simple types* where tokens like $number(X)$ or $atom(X)$ indicate that the variable X is bound to take numerical values, or Herbrand constants, respectively. The reader can easily figure out how to define such a simple constraint system. Figure 1 suggests, by means of a Hasse diagram, a possible set of tokens together with its entailment relation.

Since almost any constraint logic-based language is an extension of Prolog, the Herbrand (or finite trees) constraint system plays a fundamental role in the field. If taken seriously, this is a quite complicated constraint system. This is due to the fact that Herbrand constraints in themselves are quantified formulas, which is not the case for most other constraint languages. For our purposes we need a clear separation between "real" program variables (in unification theory called *eliminable variables*) from quantified variables appearing only in the constraints (called *parameters*). We also wish to avoid having to talk *modulo renaming*. For these reasons [7] here we give a quite detailed account of a simple constraint system capturing Herbrand constraints.

Basically, the tokens are systems of equations in solved form (see [35]). Besides that, they are also *minimal* (i.e. they do not contain useless equations, and the scope of parameters is as tight as possible), and *canonical* (i.e. the parameters' names are selected in a unique way). Formally, the set of tokens, $\mathcal{E}$, contains the symbol $\bot$ and all the syntactic objects of the form

$$\lambda\langle Y_1, \ldots, Y_p\rangle \centerdot \langle X_1 = t_1, \ldots, X_n = t_n\rangle$$

such that

(i) $\{X_1 = t_1, \ldots, X_n = t_n\}$ is in solved form (i.e. $X_1, \ldots, X_n$ are all distinct and do not occur on right-hand sides) with parameters $\{Y_1, \ldots, Y_p\} = \bigcup_{i=1}^{n} vars(t_i)$.

(ii) Equations of the form $X_i = Y_j$ where Y_j does not occur elsewhere are useless and thus forbidden: for each $i \in \{1, \ldots, n\}$, if $t_i \equiv Y_j$, then there exists $k \in \{1, \ldots, n\}$ with $k \neq i$ such that $Y_j \in vars(t_k)$.

(iii) The scope of each parameter cannot be restricted to a proper subset of the equations at hand: the graph with nodes $\{1, \ldots, n\}$ and edges

$$\left\{ (i,j) \;\middle|\; i,j = 1, \ldots, n \text{ and } vars(t_i) \cap vars(t_j) \neq \varnothing \right\}$$

is strongly connected.

(iv) The parameters' names are completely determined by the equations. With respect to the total ordering of variables we have [8]:

a. $X_1 < X_2 < \cdots < X_n \prec Y_1 \prec Y_2 \prec \cdots \prec Y_p$. This identifies the variable symbols to be used.

b. They are assigned on a first-seen basis traversing the right sides of the equations in some standard order: if $\langle Y_{i_1}, \ldots, Y_{i_l}\rangle$ is the sequence of vari-

[7] And also because, unfortunately, we were not able to find in the literature a precise description (in terms of simple constraint system) to refer the reader to.

[8] In this context, $X \prec Y$ means that Y immediately follows X in the order.

ables encountered in a depth-first, left-to-right traversal of $\langle t_1, \ldots, t_n \rangle$, then [9] for each $h, k \in \{1, \ldots, l\}$ with $h < k$

$$\left.\begin{array}{l} \forall h' < h, h' \geq 1 : Y_{i_{h'}} \neq Y_{i_h} \\ \forall k' < k, k' \geq 1 : Y_{i_{k'}} \neq Y_{i_k} \end{array}\right\} \implies Y_{i_h} < Y_{i_k}.$$

Notice that, by selecting the parameter's names in a unique way, we will avoid all the burden of talking "modulo renaming". Tokens of the form $\lambda\varepsilon \,.\, \bar{E}$ can be simply denoted by $\bar{E}$. The token $\lambda\varepsilon \,.\, \varepsilon$ is denoted by $\top$.

The entailment relation $\vdash \subseteq \wp_f(\mathcal{E}) \times \mathcal{E}$ is defined by suitably augmenting the conditions of Definition 23. First we must say how we combine tokens to get other tokens:

$$\{c_1, c_2\} \vdash c, \quad \text{if } c \in \sigma(c_1, c_2), \tag{8}$$

where $\sigma \colon \mathcal{E} \times \mathcal{E} \to \wp_f(\mathcal{E})$ is computed as follows.

(i) If $c_1 \equiv \bot$ or $c_2 \equiv \bot$ then return $\{\bot\}$. Otherwise, let $c_1 \equiv \lambda\bar{Y}_1 \,.\, \bar{E}_1$ and $c_2 \equiv \lambda\bar{Y}_2 \,.\, \bar{E}_2$.

(ii) Consistently rename the parameters $\bar{Y}_2$ of c_2 apart from $\bar{E}_1$. Let $\lambda\bar{Y}_2' \,.\, \bar{E}_2'$ be the result.

(iii) Compute the solved form of $\bar{E}_1 \cup \bar{E}_2'$ with parameters $\bar{Y}_1 \cup \bar{Y}_2'$. If the system is unsolvable return $\{\bot\}$. Otherwise, let $\bar{F} = \{X_1 = t_1, \ldots, X_m = t_m\}$ be the solved form obtained.

(iv) Define the graph

$$G \stackrel{\text{def}}{=} \left\langle \bar{F}, \left\{ (e_i, e_j) \;\middle|\; e_i, e_j \in \bar{F} \text{ and } \mathit{vars}(e_i) \cap \mathit{vars}(e_j) \neq \varnothing \right\} \right\rangle$$

and let $\{\bar{F}_1, \ldots, \bar{F}_s\}$ be the nodes of the condensed graph G^* (i.e. the strongly connected components of G).

(v) From each $\bar{F}_i$ obtain the token $\lambda\bar{Z}_i \,.\, \bar{H}_i$ (by ordering the equations, suitably renaming the parameters and so on).

(vi) Return $\{\, \lambda\bar{Z}_i \,.\, \bar{H}_i \mid i = 1, \ldots, s \,\}$.

Now the entailment must be closed by anti-instance, i.e.

$$\{c'\} \vdash c, \quad \text{if } c' \vdash c, \tag{9}$$

where $\vdash \subseteq \mathcal{E} \times \mathcal{E}$ is such that

$$\lambda\bar{Y}_1 \,.\, \langle X_1 = t_1, \ldots, X_n = t_n \rangle \vdash \lambda\bar{Y}_2 \,.\, \langle Z_1 = s_1, \ldots, Z_m = s_m \rangle$$

[9] Notice that we treat $\langle t_1, \ldots, t_n \rangle$ as a special term (or tree) with a fictitious root added.

if and only if $\{Z_1, \ldots, Z_m\} \subseteq \{X_1, \ldots, X_n\}$ and there exists a substitution θ such that [10]

$$Z_1 \equiv X_{i_1}, \ldots, Z_m \equiv X_{i_m} \quad \text{and} \quad \langle t_{i_1}, \ldots, t_{i_m} \rangle \equiv \langle s_1, \ldots, s_m \rangle \theta.$$

The effect of a renaming $[\bar{W}/\bar{V}]$ onto a token $\lambda \bar{Y} \,.\, \bar{E}$ is to substitute the non-parameters in $\bar{V}$ with the correspondent ones in $\bar{W}$ (notice that, by definition, $(\bar{W} \cup \bar{Y}) \cap FV(\lambda \bar{Y} \,.\, \bar{E}) = \varnothing$), and then to rename the parameters $\bar{Y}$ (there is a unique way to do that) so to ensure that the result is still a token.

The definition is completed by saying that $\vdash \subseteq \wp_f(\mathcal{E}) \times \mathcal{E}$ is the smallest relation satisfying (8), (9), and conditions E_1–E_5 of Definition 23. All these complications have the great advantage of being confined here. We will see, in fact, that with this definition equivalence of constraints will amount to the *equality* of the correspondent set of tokens. Similarly, extracting the common information of two Herbrand constraints will be done by taking the intersection of their sets of tokens.

4.4 Bounds and relations analysis for numeric domains

The analysis described in [5,6,4] is based on constraint inference, a variant of constraint propagation [20]. This technique, developed in the field of artificial intelligence, has been applied to temporal and spatial reasoning [2,49,50].

Let us focus our attention to arithmetic domains, where the constraints are binary relations over expressions. Let E be the set of arithmetic expressions of interest. Let $\mathsf{F} \subset \mathbb{R}$ a computable set of numbers, e.g. some family of rational or floating point numbers. The set B of *boundaries* over F is given by

$$\mathsf{B} \stackrel{\text{def}}{=} \mathsf{F} \cup \{+\infty, -\infty\},$$

and is ordered by the natural extension of the $\leq$ relation. The set I of intervals is

$$\begin{aligned} \mathsf{I} \stackrel{\text{def}}{=} & \left\{ (b_1, b_2) \;\middle|\; b_1 \in \mathsf{B}, b_2 \in \mathsf{B} \right\} \cup \left\{ [\, b_1, b_2) \;\middle|\; b_1 \in \mathsf{F}, b_2 \in \mathsf{B} \right\} \\ & \cup \left\{ (b_1, b_2\,] \;\middle|\; b_1 \in \mathsf{B}, b_2 \in \mathsf{F} \right\} \cup \left\{ [\, b_1, b_2\,] \;\middle|\; b_1 \in \mathsf{F}, b_2 \in \mathsf{F} \right\}. \end{aligned}$$

Since any $I \in \mathsf{I}$ is a finite representations of a subset of $\mathbb{R}$ we will confuse intervals with their denotation. Thus we can state that intervals are closed

[10] Again, we regard $\langle \ldots \rangle$ as a special function symbol.

under intersection, i.e., for each $I_1, I_2 \in \mathsf{I}$, $I_1 \cap I_2 \in \mathsf{I}$. The set of arithmetic relations is $\mathsf{R} \stackrel{\text{def}}{=} \{=, \neq, \leq <, \geq, >\}$ and our constraints are given by

$$\mathcal{C} \stackrel{\text{def}}{=} \left\{ e_1 \bowtie e_2 \;\middle|\; e_1, e_2 \in E, \bowtie \in \mathsf{R} \right\} \cup \{ e \lhd I \mid e \in E, I \in \mathsf{I} \} \cup \{\bot, \top\}.$$

The meaning of the constraint $e \lhd I$ is the obvious one: any real value the expression e can take is contained in I. Thus $\mathcal{C}$ provides a mixture of qualitative (relationships between expressions) and quantitative (bounds on the values of the expressions) knowledge.

The approximate inference techniques we are interested in can be encoded into an entailment relation '$\vdash$' over $\mathcal{C}$. First we need to specify how we deal with intervals: we can intersect them, weaken them, and we detect failure by recognizing empty ones:

$$\begin{aligned} \{e \lhd I_1, e \lhd I_2\} &\vdash e \lhd I_1 \cap I_2, \\ \{e \lhd I\} &\vdash e \lhd I', && \text{if } I \subseteq I', \\ \{e \lhd I\} &\vdash \bot, && \text{if } I = \varnothing. \end{aligned}$$

Two techniques for exploiting pure qualitative information are *symmetric* and *transitive closure*:

$$\begin{aligned} \{e_1 \bowtie e_2\} &\vdash e_2 \bowtie^{-1} e_1, \\ \{e_1 \bowtie e_2, e_2 \bowtie' e_3\} &\vdash e_1 \bowtie'' e_3, && \text{if } \bowtie'' = tc(\bowtie, \bowtie'), \end{aligned}$$

where $\bowtie^{-1}$ is the inverse of $\bowtie$ (e.g. $<$ is the inverse of $>$, $\geq$ of $\leq$ and so on), and $tc \colon \mathsf{R} \times \mathsf{R} \rightarrowtail \mathsf{R}$ is the partial function individuated by the following table:

tc	$<$	$\leq$	$>$	$\geq$	$=$	$\neq$
$<$	$<$	$<$			$<$	
$\leq$	$<$	$\leq$			$\leq$	
$>$			$>$	$>$	$>$	
$\geq$			$>$	$\geq$	$\geq$	
$=$	$<$	$\leq$	$>$	$\geq$	$=$	$\neq$
$\neq$					$\neq$	

This technique allows the inference of $A < C$ from $A \leq B$ and $B < C$. Of course, qualitative information can be combined and can led to the detection of inconsistencies:

$$\begin{aligned} \{e_1 \bowtie e_2, e_1 \bowtie' e_2\} &\vdash e_1 \bowtie'' e_2, && \text{if } \forall x, y \in \mathbb{R} : (x \bowtie y \wedge x \bowtie' y) \Rightarrow x \bowtie'' y, \\ \{e_1 \bowtie e_2, e_1 \bowtie' e_2\} &\vdash \bot, && \text{if } \forall x, y \in \mathbb{R} : \neg(x \bowtie y \wedge x \bowtie' y). \end{aligned}$$

A classical quantitative technique is *interval arithmetic* which allows to infer the variation interval of an expression from the intervals of its sub-expressions.

Let $f(e_1, \ldots, e_k)$ be any arithmetic expression having $e_1, \ldots, e_k$ as subexpressions. Then

$$\Big\{ f(e_1, \ldots, e_k) \lhd I, e_1 \lhd I_1, \ldots, e_k \lhd I_k \Big\} \vdash f(e_1, \ldots, e_k) \lhd \ddot{f}(I_1, \ldots, I_k),$$

where $\ddot{f} \colon \mathsf{I}^k \to \mathsf{I}$ is such that for each $x_1 \in I_1, \ldots, x_k \in I_k$, it happens that $f(x_1, \ldots, x_k) \in \ddot{f}(I_1, \ldots, I_k)$. An example inference is: $A \lhd [\,3, 6\,) \wedge B \lhd [\,-1, 5\,] \vdash A + B \lhd [\,2, 11\,)$. Another technique is *numeric constraint propagation*, which consists in determining the relationship between two expressions when their associated intervals do not overlap, except possibly at their endpoints. The associated family of axioms is

$$\{ e_1 \lhd I_1, e_2 \lhd I_2 \} \vdash e_1 \bowtie e_2, \quad \text{if } \forall x_1 \in I_1, x_2 \in I_2 : x_1 \bowtie x_2.$$

For example, if $A \in (-\infty, 2\,]$, $B \in [\,2, +\infty)$, and $C \in [\,5, 10\,]$, we can infer that $A \leq B$ and $A < C$. It is also possible to go the other way around, i.e. knowing that $U < V$ may allow to refine the intervals associated to U and V so that they do not overlap. We call this *weak interval refinement*:

$$\{ e_1 \bowtie e_2, e_1 \lhd I_1, e_2 \lhd I_2 \} \vdash e_1 \lhd I_1'$$

where $I_1' \stackrel{\text{def}}{=} \{\, x_1 \in I_1 \mid \exists x_2 \in I_2 \;.\; x_1 \bowtie x_2 \,\}$. This is an example of local-consistency technique [41,38,23]. In summary, by considering the transitive closure of $\vdash$ and with some minor technical additions we end up with a simple constraint system which characterizes precisely the combination of the above techniques. Other techniques, such as *interval refinement*, can be easily incorporated. What we have just presented is a watered-down version of the numerical component (presented as a simple constraint system) employed in the China analyzer [4].

Now we are in position to introduce an important class of members of the hierarchy.

5 Determinate constraint systems

Determinate constraint systems are at the bottom of the hierarchy. Such a construction is uniquely determined by a simple constraint system together with an appropriate merge operator. Notice that, for simplicity, we only present the *finite fragment* of the constraint system, that is, the sub-structure consisting of the finite elements only.

Definition 26 (Determinate constraint system.) *Let* $\mathcal{S} \stackrel{\text{def}}{=} \langle \mathcal{C}, \vdash, \bot, \top \rangle$ *be a simple constraint system. Let* $\mathbf{0}, \mathbf{1} \in |\mathcal{C}|_0$ *and* $\otimes \colon |\mathcal{C}|_0 \times |\mathcal{C}|_0 \to |\mathcal{C}|_0$ *be given, for each* $C_1, C_2 \in |\mathcal{C}|_0$, *by*

$$\mathbf{0} \stackrel{\text{def}}{=} \mathcal{C}, \qquad C_1 \otimes C_2 \stackrel{\text{def}}{=} \rho(C_1 \cup C_2).$$
$$\mathbf{1} \stackrel{\text{def}}{=} \rho(\varnothing),$$

Let $\oplus\colon |\mathcal{C}|_0 \times |\mathcal{C}|_0 \to |\mathcal{C}|_0$ *be an operator satisfying conditions* G_2 *and* G_4 *of* Definition 7. *The projection operators* $\bar{\exists}_{\vec{\Lambda}}\colon |\mathcal{C}|_0 \to |\mathcal{C}|_0$ *are given, for each* $\vec{\Lambda} \in \Lambda^\star$ *and each* $C \in |\mathcal{C}|_0$, *by*

$$\bar{\exists}_{\vec{\Lambda}} C \stackrel{\text{def}}{=} \rho\Big(\Big\{\, c \in C \;\Big|\; FV(c) \subseteq \vec{\Lambda} \,\Big\}\Big).$$

Finally, let $\{d_{\bar{X}\bar{Y}}\}_{\bar{X},\bar{Y} \in \mathit{Vars}^\star}$ *a family of elements of* $|\mathcal{C}|_0$. *We will call the structure* $\langle |\mathcal{C}|_0, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{\Lambda}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$ *a* determinate constraint system *over* $\mathcal{S}$ *and '*$\oplus$*'.*

The following is an adaptation to our more relaxed hypotheses of a result in [43, Proposition 2.3].

Lemma 27 *Let* $\langle \mathcal{C}, \vdash, \bot, \top\rangle$ *be a simple constraint system. For each* $C \subseteq \mathcal{C}$ *we have* $FV(\rho(C)) \subseteq FV(C)$.

PROOF. Suppose $X \in FV(\rho(C))$. By Eq. 1 of Definition 6 we have that there exist $c \in \rho(C)$ and $Z \in \mathit{Vars}$ such that $c[Z/X] \notin \rho(C)$. This implies that there exists $C' \subseteq_f C$ such that $C' \vdash c$ (otherwise $c \notin \rho(C)$). Now suppose, towards a contradiction, that $X \notin FV(C)$. This means that for each $c' \in C'$ and each $Y \in \mathit{Vars}$ we have $c'[Y/X] \in C$, and thus $C'[Y/X] \subseteq_f C$. By the genericity axiom E_5 of Definition 23, this implies that, for each $Y \in \mathit{Vars}$, $C'[Y/X] \vdash c[Y/X]$ and thus that $c[Y/X] \in \rho(C)$, contradicting the hypothesis $X \in FV(\rho(C))$. $\square$

Theorem 28 *Each determinate constraint system is indeed a constraint system. Also, for each* $C_1, C_2 \in |\mathcal{C}|_0$, *we have* $C_1 \vdash C_2 \iff C_1 \supseteq C_2$.

PROOF. With reference to Definition 7, G_0 is true because of point (ii) in Definition 5. G_1 clearly holds by definition of $\otimes$ and ρ. G_2 and G_4 are enforced by the choice of the merge operator. For G_3, if $C \in |\mathcal{C}|_0$ then $C \otimes \mathbf{0} = \rho(C \cup \mathcal{C}) = \rho(\mathcal{C}) = \mathbf{0}$. Then, by definition of $\vdash$, $C_1 \vdash C_2$ iff $\rho(C_1 \cup C_2) = C_1$. Thus, if $C_1 \vdash C_2$ we have, by ρ extensivity, $C_1 \cup C_2 \subseteq \rho(C_1 \cup C_2) = C_1$ which implies $C_1 \supseteq C_2$. Conversely, assuming $C_1 \supseteq C_2$, ρ idempotence gives $\rho(C_1 \cup C_2) = \rho(C_1) = C_1$. Finally, G_5 is an immediate consequence of the definition of $\bar{\exists}_{\vec{\Lambda}}$ and of Lemma 27. $\square$

The choice of a suitable merge operator, required in addition to an s.c.s. to obtain a determinate constraint system, can be done with relative freedom. This freedom can often be conveniently exploited in order to get a reasonable complexity/precision tradeoff. The same will apply to the *ask-and-tell constraint systems* of Section 7.

Given $C_1, C_2 \in |\mathcal{C}|_0$, there is no *a priori* guarantee that $C = C_1 \cap C_2 \in |\mathcal{C}|_0$. In fact, there are simple constraint systems where this is false [11]. However, since ρ is an algebraic closure operator by its very definition, if it turns out that $C \in |\mathcal{C}|_0$, then there exists $C_0 \subseteq_f C$ such that $\rho(C_0) = C$ [8]. Said that, defining the merge operator as set intersection works in many cases.

A trivial example of merge operator is the following, whose definition is independent from the simple constraint system at hand:

$$C_1 \oplus C_2 \stackrel{\text{def}}{=} \begin{cases} C_1, & \text{if } C_1 = C_2 \text{ or } C_2 = \mathbf{0}; \\ C_2, & \text{if } C_1 = \mathbf{0}; \\ \mathbf{1}, & \text{otherwise.} \end{cases} \tag{10}$$

For a less trivial example, suppose we are approximating subsets of $\mathbb{R}^n$ by means of (closed) convex polyhedra. Of course they will be represented by sets of linear disequations over $x_1, \ldots, x_n$, but, for the purpose of the present example, we will consider the polyhedra themselves. For any convex polyhedra $X, Y \subseteq \mathbb{R}^n$, define $X \vdash Y$ iff $X \subseteq Y$ and

$$X \oplus Y \stackrel{\text{def}}{=} \begin{cases} X, & \text{if } X = Y \text{ or } Y = \varnothing; \\ Y, & \text{if } X = \varnothing; \\ \mathrm{bb}(X \cup Y), & \text{otherwise,} \end{cases} \tag{11}$$

where $\mathrm{bb}(Z)$ is the smallest "bounding box" containing $Z \subseteq \mathbb{R}^n$, i.e.,

$$\mathrm{bb}(Z) \stackrel{\text{def}}{=} \Big\{ (x_1, \ldots, x_n) \;\Big|\; \forall i = 1, \ldots, n : \inf \pi_i(Z) \leq x_i \leq \sup \pi_i(Z) \Big\}.$$

The most precise merge operator is, of course, given by the convex hull, i.e.

$$X \oplus Y \stackrel{\text{def}}{=} \min\Big\{ W \subseteq \mathbb{R}^n \;\Big|\; W \supseteq X \cup Y \text{ and } W \text{ is a c.p.} \Big\}. \tag{12}$$

Notice that (12) satisfies both the absorption laws (thus giving rise to a lattice), (10) and (11) do not. None of them results in a distributive constraint system.

[11] For the interested reader: consider the set of tokens $\{\bot, a, b, \top\} \cup \{t_i\}_{i \in \mathbb{N}}$. Choose the least entailment relation such that: $\{t_i\} \vdash t_j$ iff $i \geq j$, $\{a\} \vdash \{t_i\}_{i \in \mathbb{N}}$, $\{b\} \vdash \{t_i\}_{i \in \mathbb{N}}$, and $\{a, b\} \vdash \bot$. It is easy to see that the intersection of the finite elements generated by $\{a\}$ and $\{b\}$, respectively, is $\{t_i\}_{i \in \mathbb{N}}$, which is not finite.

Furthermore, (10) and (11) are closed, while (12) is not.

5.1 Definiteness analysis: Con

Consider the extension of the *atomic* simple constraint system, $\mathcal{C}'$, introduced in Section 4.1, and apply to it the determinate constraint system construction with

$$C_1 \oplus C_2 \stackrel{\text{def}}{=} C_1 \cap C_2, \quad \text{for each } C_1, C_2 \in |\mathcal{C}'|.$$

Let also the diagonal elements be given, for each $\bar{X}, \bar{Y} \in \mathit{Vars}^\star$ of the same cardinality, by

$$d_{\bar{X}\bar{Y}} \stackrel{\text{def}}{=} \rho\Big(\{\, \pi_i(\bar{X}) \leftrightharpoons \pi_i(\bar{Y}) \mid 1 \leq i \leq \#\,\bar{X} \,\}\Big).$$

The resulting domain (a closed and Noetherian d.c.s.) is the simplest one for definiteness analysis, and it was used in early groundness analyzers [40,34]. The name *Con* comes from the fact that elements of the form $\{X_1, \ldots, X_n\}$ are usually regarded as the conjunction $X_1 \wedge \cdots \wedge X_n$, meaning that $X_1, \ldots, X_n$ are definitely bound to a unique value. In this view $\otimes$ amounts to logical conjunction.

Con is a very weak domain for definiteness analysis. It cannot capture neither "aliasing" (apart from the special kind of aliasing arising from parameter passing) nor more complex dependencies between variables such as those implied by "concrete" constraints like $A = f(B, C)$ and $A + B + C = 0$. Moreover it cannot represent or exploit disjunctive information.

5.2 A domain for structural information: Pattern

Endowing the Herbrand simple constraint system of Section 4.3 with the merge operator

$$C_1 \oplus C_2 \stackrel{\text{def}}{=} C_1 \cap C_2, \quad \text{for each } C_1, C_2 \in |\mathcal{E}|_0.$$

and the diagonals (we assume that $\pi_i(\bar{X}) \leq \pi_i(\bar{Y})$ for all $i = 1, \ldots, n$ for simplicity)

$$d_{\bar{X}\bar{Y}} \stackrel{\text{def}}{=} \rho\Big(\Big\{\, \lambda\langle Z_i\rangle \,.\, \langle \pi_i(\bar{X}) = Z_i, \pi_i(\bar{Y}) = Z_i\rangle \;\Big|\; 1 \leq i \leq \#\,\bar{X}, \pi_i(\bar{Y}) \prec Z_i \,\Big\}\Big).$$

yields a closed and Noetherian d.c.s. suitable for structural analysis. Observe that all the finitely generable elements in $|\mathcal{E}|_0 \backslash \mathbf{0}$ are finite, since there is at most one normalized greatest common instance for each finite set of terms (axiom

(8) of the entailment relation) and only a finite number of (normalized) anti-instances for any given set of terms (axiom (9)) [35]. As the ordering is reverse set inclusion, Noetherianity clearly follows.

Since the tokens are normalized and elements are closed by anti-instance, merging two elements of $|\mathcal{E}|_0$ makes implicit the fact that to each eliminable variable in the result will be assigned the least common anti-instance (*lca*) of the terms assigned in the elements to be merged (and all its further anti-instances). In a real implementation, where closure by anti-instance is obviously not performed, this will correspond to the use of some anti-unification algorithm to compute the *lca* of terms assigned to the same eliminable variable.

The *Pattern* domain presented here, which is a reformulation of the ones defined in [42,36], deals only with pure structural information. In [12] a much more powerful domain is presented, `Pat(`$\Re$`)`, parametric with respect to any abstract domain $\Re$ in their framework (which is not restricted to monotonic properties). It is possible to modify the *Pattern* domain presented in this section so to make it parametric with respect to any constraint system $\bar{\mathcal{D}}$, still obtaining a constraint system. In this way one can achieve the same results of the parametric domain of [12], though in the restricted context of monotonic properties. Of course, the back-side of this restriction is a greater simplicity in the definition of the parametric domain $Pattern(\bar{\mathcal{D}})$.

Now that we have seen how many constraint systems can be built, we will show how the induced members of the hierarchy look like.

6 Powerset constraint systems

For the purpose of program analysis of monotonic properties it is not necessary to represent the "real disjunction" of constraints collected through different computation paths, since we are interested in the common information only. To this end, a weaker notion of disjunction suffices. We define *powerset constraint systems*, which are instances of a well known construction, i.e. disjunctive completion [16]. For doing that we need some notions from the theory of posets.

Given a poset $\langle L, \bot, \leq \rangle$, the relation $\preceq \subseteq \wp(L) \times \wp(L)$ induced by $\leq$ is given, for each $S_1, S_2 \in \wp(L)$ by

$$(S_1 \preceq S_2) \iff (\forall m_1 \in S_1 : \exists m_2 \in S_2 \,.\, m_1 \leq m_2).$$

A subset $S \in \wp(L)$ is said *non-redundant* iff $\bot \notin S$ and

$$\forall m_1, m_2 \in S : m_1 \leq m_2 \implies m_1 = m_2.$$

The set of non-redundant subsets of L wrt $\leq$ is denoted by $\wp_n(L,\leq)$. The function $\Omega^{\leq}_L : \wp(L) \to \wp_n(L,\leq)$ mapping each set into its non-redundant counterpart is given, for each $S \in \wp(L)$, by

$$\Omega^{\leq}_L(S) = S \setminus \{\, m \in S \mid m = \bot \vee \exists m' \in S \,.\, m < m' \,\}.$$

Thus, for $S \in \wp(L)$, $\Omega^{\leq}_L(S)$ is the set of maximal elements of S. However, there is no guarantee, in general, that such maximal elements exist: L could be an infinite chain without an upper bound in L, and thus would be mapped to $\varnothing$ by $\Omega^{\leq}_L$. We will denote by $\wp_c(L)$ the set of all those $S \in \wp(L)$ such that, if S contains an infinite chain C, then it also contains an upper bound for C. Observe that $\wp_f(L) \subseteq \wp_c(L)$ and that, if L satisfies the ascending chain condition, then $\wp(L) = \wp_c(L)$.

Proposition 29 *If $\langle L, \bot, \leq\rangle$ is a poset the following hold:*

(i) *$\langle \wp_n(L,\leq), \preceq\rangle$ is a poset;*
(ii) *for each $S \in \wp_c(L)$, we have both $\Omega^{\leq}_L(S) \preceq S$ and $S \preceq \Omega^{\leq}_L(S)$;*
(iii) *for each family $\{S_i \in \wp(L)\}_{i\in I}$ we have $\Omega^{\leq}_L\big(\bigcup_{i\in I} \Omega^{\leq}_L(S_i)\big) = \Omega^{\leq}_L(\bigcup_{i\in I} S_i)$;*
(iv) *if $\langle L, \bot, \leq, \wedge\rangle$ is a meet-semilattice then for each $x \in L$ and $S \in \wp_c(L)$*

$$\Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in \Omega^{\leq}_L(S) \,\}\big) = \Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in S \,\}\big).$$

PROOF.

(i) $\preceq$ is easily seen to be preorder relation. For antisymmetry, consider a pair $S_1, S_2 \in \wp_n(L,\leq)$ such that $S_1 \preceq S_2$ and $S_2 \preceq S_1$. If $m_1 \in S_1$ then there exists $m_2 \in S_2$ with $m_1 \leq m_2$. But then again there exists $m_1' \in S_1$ such that $m_1 \leq m_2 \leq m_1'$. By non-redundancy we must have $m_1 = m_2 = m_1'$, so that $m_1 \in S_2$ and $S_1 \subseteq S_2$. A symmetric argument proves that, indeed, $S_1 = S_2$.

(ii) Observe that $\Omega^{\leq}_L(S) \subseteq S$ and that, if $S \in \wp_c(L)$ and $x \in S$, then either $x \in \Omega^{\leq}_L(S)$ or there exists $y \in \Omega^{\leq}_L(S)$ such that $x < y$.

(iii) Straightforward.

(iv) We have that

$$\begin{aligned}
\Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in \Omega^{\leq}_L(S) \,\}\big) &= \Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in \Omega^{\leq}_L(S) \,\} \cup \\
&\qquad \{\, x \wedge y \;\big|\; y \in S \setminus \Omega^{\leq}_L(S), \exists y' \in \Omega^{\leq}_L(S) \,.\, x \wedge y \leq x \wedge y' \,\}\big) \\
&= \Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in \Omega^{\leq}_L(S) \,\} \cup \{\, x \wedge y \;\big|\; y \in S \setminus \Omega^{\leq}_L(S) \,\}\big) \\
&= \Omega^{\leq}_L\big(\{\, x \wedge y \mid y \in S \,\}\big),
\end{aligned}$$

since, for each $x \in L$, $S \in \wp_c(L)$ and $y \in S \setminus \Omega^{\leq}_L(S)$, there is always a $y' \in \Omega^{\leq}_L(S)$ such that $y < y'$. The condition $\exists y' \in \Omega^{\leq}_L(S) \,.\, x \wedge y \leq x \wedge y'$ above is thus always satisfied by $\wedge$ monotonicity. $\Box$

The powerset construction upgrades a domain by considering sets of elements of the base-level domain which are non-redundant with respect to the approximation ordering.

Definition 30 (Powerset constraint systems.) *Given a Noetherian constraint system* $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{\Lambda}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$*, the* powerset constraint system *over* $\bar{\mathcal{D}}$ *is given by*

$$\Big\langle \wp_n(\mathcal{D}, \vdash), \otimes_{\mathrm{P}}, \oplus_{\mathrm{P}}, \mathbf{0}_{\mathrm{P}}, \mathbf{1}_{\mathrm{P}}\{\bar{\exists}^{\mathrm{P}}_{\vec{\Lambda}}\}, \{d^{\mathrm{P}}_{\bar{X}\bar{Y}}\}\Big\rangle,$$

where

$$\begin{aligned}
S_1 \otimes_{\mathrm{P}} S_2 &\stackrel{\mathrm{def}}{=} \Omega^{\vdash}_{\mathcal{D}}\Big(\{\, C_1 \otimes C_2 \mid C_1 \in S_1, C_2 \in S_2 \,\}\Big),\\
S_1 \oplus_{\mathrm{P}} S_2 &\stackrel{\mathrm{def}}{=} \Omega^{\vdash}_{\mathcal{D}}(S_1 \cup S_2),\\
\mathbf{0}_{\mathrm{P}} &\stackrel{\mathrm{def}}{=} \varnothing,\\
\mathbf{1}_{\mathrm{P}} &\stackrel{\mathrm{def}}{=} \{\mathbf{1}\},\\
\bar{\exists}^{\mathrm{P}}_{\vec{\Lambda}}\, S &\stackrel{\mathrm{def}}{=} \Omega^{\vdash}_{\mathcal{D}}\Big(\{\, \bar{\exists}_{\vec{\Lambda}}\, C \mid C \in S \,\}\Big),\\
d^{\mathrm{P}}_{\bar{X}\bar{Y}} &\stackrel{\mathrm{def}}{=} \{d_{\bar{X}\bar{Y}}\}.
\end{aligned}$$

If $\bar{\mathcal{D}}$ *is* any *constraint system, the* finite powerset constraint system *over* $\bar{\mathcal{D}}$ *is*

$$\Big\langle \wp_n(\mathcal{D}, \vdash) \cap \wp_f(\mathcal{D}), \otimes_{\mathrm{P}}, \oplus_{\mathrm{P}}, \mathbf{0}_{\mathrm{P}}, \mathbf{1}_{\mathrm{P}}\{\bar{\exists}^{\mathrm{P}}_{\vec{\Lambda}}\}, \{d^{\mathrm{P}}_{\bar{X}\bar{Y}}\}\Big\rangle,$$

where all the operators are as above.

This double definition reflects the two possible uses of powerset constraint systems. One is to define concrete domains in those cases where the base-level constraint system is Noetherian. The other is when designing abstract domains and, clearly, only the finite elements are of interest. In both cases, point (ii) of Proposition 29 tells us that, when we deal with monotonic properties, we loose nothing if we restrict ourselves to non-redundant sets in order to capture the non-determinism of CLP languages. Of course, when the base-level c.s. is not Noetherian, one has to consider all the subsets in the design of a concrete domain.

Observe that the powerset construction completely disregards the merge operator of the base-level constraint system. Thus it can be applied to structures weaker than constraint systems, where the merge operator is missing. Instead of devoting a definition to them we rely on the fact that it is always possible to augment such structures with the trivial merge operator defined in (10) so to obtain a constraint system in the sense of Definition 7. This way, for example, any simple constraint system can indirectly constitute the basis for a powerset construction.

Theorem 31 *Any powerset constraint system built over a Noetherian c.s.* $\bar{\mathcal{D}}$*,*

$$\Big\langle \wp_n(\mathcal{D},\vdash), \otimes_{\mathrm{P}}, \oplus_{\mathrm{P}}, \mathbf{0}_{\mathrm{P}}, \mathbf{1}_{\mathrm{P}}\{\bar{\exists}^{\mathrm{P}}_{\bar{\Lambda}}\}, \{d^{\mathrm{P}}_{\bar{X}\bar{Y}}\}\Big\rangle,$$

is a closed and completely distributive constraint system, where the ordering is given, for each $S_1, S_2 \in \wp_n(\mathcal{D},\vdash)$*, by*

$$S_1 \vdash_{\mathrm{P}} S_2 \iff \forall C_1 \in S_1 : \exists C_2 \in S_2 \,.\, C_1 \vdash C_2. \tag{13}$$

For any c.s. $\bar{\mathcal{D}}$*, the finite powerset c.s. built over* $\bar{\mathcal{D}}$ *is a distributive constraint system, where the ordering is given by* (13)*, for* $S_1, S_2 \in \wp_n(\mathcal{D},\vdash) \cap \wp_f(\mathcal{D})$*.*

PROOF. Let $\bar{\mathcal{D}}$ a Noetherian c.s. We start by showing that $S_1 \otimes_{\mathrm{P}} S_2$ is the *glb* of S_1 and S_2 with respect to $\vdash_{\mathrm{P}}$. Clearly $S_1 \otimes_{\mathrm{P}} S_2 \vdash_{\mathrm{P}} S_1$ and $S_1 \otimes_{\mathrm{P}} S_2 \vdash_{\mathrm{P}} S_2$ since, for each $C \in S_1 \otimes_{\mathrm{P}} S_2$ there are some $C_1 \in S_1$ and $C_2 \in S_2$ such that $C_1 \otimes C_2 = C$. This implies $C \vdash C_1$ and $C \vdash C_2$. Suppose now to have $S \in \wp_n\Big(\mathcal{D},\vdash\Big)$ such that $S \vdash_{\mathrm{P}} S_1$ and $S \vdash_{\mathrm{P}} S_2$. Then $S \vdash_{\mathrm{P}} S_1 \otimes_{\mathrm{P}} S_2$, since

$$\left.\begin{array}{l} \forall C \in S : \exists C_1 \in S_1 \,.\, C \vdash C_1 \\ \forall C \in S : \exists C_2 \in S_2 \,.\, C \vdash C_2 \end{array}\right\} \implies$$
$$\forall C \in S : \exists C_1 \in S_1, C_2 \in S_2 \,.\, C \vdash C_1 \otimes C_2,$$

and either $C_1 \otimes C_2 \in S_1 \otimes_{\mathrm{P}} S_2$ or there exists $C' \in S_1 \otimes_{\mathrm{P}} S_2$ such that $C_1 \otimes C_2 \vdash C'$. In a similar way $S_1 \oplus_{\mathrm{P}} S_2$ is shown to be the *lub* of S_1 and S_2 with respect to $\vdash_{\mathrm{P}}$. In fact it is clear that $S_1 \vdash_{\mathrm{P}} S_1 \oplus_{\mathrm{P}} S_2$ and $S_2 \vdash_{\mathrm{P}} S1 \oplus_{\mathrm{P}} S_2$. Furthermore, if $S \in \wp_n(\mathcal{D},\vdash)$ is such that $S_1 \vdash_{\mathrm{P}} S$ and $S_2 \vdash_{\mathrm{P}} S$, then, since

$$\left.\begin{array}{l} \forall C_1 \in S_1 : \exists C_1' \in S \,.\, C_1 \vdash C_1' \\ \forall C_2 \in S_2 : \exists C_2' \in S \,.\, C_2 \vdash C_2' \end{array}\right\} \implies$$
$$\forall C \in \Omega^{\vdash}_{\mathcal{D}}(S_1 \cup S_2) : \exists C' \in S \,.\, C \vdash C',$$

we have $S_1 \oplus_{\mathrm{P}} S_2 \vdash_{\mathrm{P}} S$. The minimum and maximum elements of the lattice are clearly $\varnothing$ and $\{\mathbf{1}\}$, respectively. We now show, using points (iii) and (iv) of Proposition 29, that complete meet-distributivity holds:

$$\begin{aligned}
\bigoplus_{i\in I} S \otimes_{\mathrm{P}} \bigoplus_{i\in I}{}_{\mathrm{P}}\, S_i &= \Omega^{\vdash}_{\mathcal{D}}\Big(\{\, C \otimes C' \mid C \in S, C' \in \Omega^{\vdash}_{\mathcal{D}}(\textstyle\bigcup_{i\in I} S_i)\,\}\Big)\\
&= \Omega^{\vdash}_{\mathcal{D}}\Big(\{\, C \otimes C' \mid C \in S, C \in \textstyle\bigcup_{i\in I} S_i\,\}\Big)\\
&= \Omega^{\vdash}_{\mathcal{D}}\Big(\textstyle\bigcup_{i\in I}\{\, C \otimes C' \mid C \in S, C' \in S_i\,\}\Big)\\
&= \Omega^{\vdash}_{\mathcal{D}}\Big(\textstyle\bigcup_{i\in I} \Omega^{\vdash}_{\mathcal{D}}\Big(\{\, C \otimes C' \mid C \in S, C' \in S_i\,\}\Big)\Big)\\
&= \bigoplus_{i\in I}{}_{\mathrm{P}}(S \otimes_{\mathrm{P}} S_i).
\end{aligned}$$

In particular we have shown that $\langle \wp_n(\mathcal{D},\vdash), \otimes_{\mathrm{P}}, \oplus_{\mathrm{P}}, \mathbf{0}_{\mathrm{P}}, \mathbf{1}_{\mathrm{P}}\rangle$ is a distributive lattice so that G_1–G_4 of Definition 7 are satisfied. G_0, G_5, and closedness are implicit in the definition. The above proof can be replayed substituting $\wp_n(\mathcal{D})$ with $\wp_n(\mathcal{D},\vdash) \cap \wp_f(\mathcal{D})$, I with $\{1,2\}$, and, of course, omitting closedness. □

6.1 A collecting semantics for logic programs

When interested in monotonic properties of logic programs, a suitable collecting semantics can be defined over the domain resulting from the application of the powerset construction to the *Pattern* d.c.s. of Section 5.2, which is Noetherian.

6.2 Structural analysis: more than Pattern

One possibility for obtaining more precise structural information than possible with *Pattern*, is to use the domain of the previous section together with a suitable widening operator $\nabla\colon\ \wp_n(|\mathcal{E}|_0)^2 \to \wp_n(|\mathcal{E}|_0)$ to ensure termination.

A very crude widening operator for any powerset c.s. can be defined in terms of the base-level merge operator as follows:

$$S_1 \nabla S_2 \stackrel{\text{def}}{=} \Omega^{\vdash}_{\mathcal{D}}\Big(\Big\{\bigoplus(S_1 \oplus_{\mathrm{P}} S_2)\Big\}\Big).$$

Of course this destroys, as soon as it is applied, all the extra-precision gained by passing to the powerset. Things can be improved by using derived operators like

$$S_1 \nabla' S_2 \stackrel{\text{def}}{=} \begin{cases} S_1 \nabla S_2, & \text{if } p(S_1,S_2);\\ S_2, & \text{otherwise,}\end{cases}$$

where the predicate $p(S_1,S_2)$ is true if, on passing from S_1 to S_2 (usually S_1 and S_2 are the results of two adjacent iterates computed during the analysis)

"something has grown".

A better widening for the current example of structural analysis can be defined as follows. Take $S_1, S_2 \in \wp_n(|\mathcal{E}|_0)$, and let $S = S_1 \oplus_{\mathrm{P}} S_2$. From each $C \in S$ take out all the tokens involving terms of depth greater than some fixed k; call C' the result and S' the set of all the C' so obtained. Now $S_1 \nabla S_2$ is obtained from S' by removing all the redundant elements. This widening roughly corresponds to the use of depth-k approximations as in [46,39]. It is still not very accurate, as it "cuts" also the structures which have not grown. A more precise widening can be obtained on these lines by restricting the "depth-k cut" to those variables such that the maximum depth of the associated patterns in S_2 is greater than the maximum depth of the associated patterns in S_1.

7 Ask-and-tell constraint systems

We now consider constraint systems having additional structure. This additional structure allows to express, at the constraint system level, that the imposition of certain constraints must be delayed until some other constraints are imposed. In [44] similar constructions are called *ask-and-tell constraint systems*. In our construction, ask-and-tell constraint systems are built from constraint systems by regarding some kernel operators as constraints. We follow [44] in considering cc as *the* language framework for expressing and computing with kernel operators [12] . For this reason we will present kernel operators as cc agents. For our current purposes we only need a very simple fragment of the determinate cc language: the one of *finite* cc *agents*. This fragment is described in [45] by means of a declarative semantics. Here we give an operational characterization which is better suited to our needs.

Definition 32 (Finite cc agents: syntax.) *A* finite cc agent *over a constraint system* $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{X}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$ *is any string generated by the following grammar:*

$$\mathbf{Agent} ::= \mathrm{tell}(C) \mid \mathrm{ask}(C) \rightarrow \mathbf{Agent} \mid \mathbf{Agent} \parallel \mathbf{Agent}$$

where $C \in \mathcal{D}$. *We will denote by* $\mathcal{A}(\bar{\mathcal{D}})$ *the language of such strings. The following explicit definition is also given:*

$$\begin{aligned} &\mathrm{ask}(C_1; \ldots ; C_n) \rightarrow \mathbf{Agent} \equiv \\ &\Big(\mathrm{ask}(C_1) \rightarrow \mathbf{Agent}\Big) \parallel \cdots \parallel \Big(\mathrm{ask}(C_n) \rightarrow \mathbf{Agent}\Big). \end{aligned} \tag{14}$$

[12] At least for a relevant class of them. See Section 7.1 for more on that subject.

When this will not cause confusion we will freely drop the syntactic sugar, writing C and $C_1 \to C_2$ where $\mathrm{tell}(C)$ and $\mathrm{ask}(C_1) \to \mathrm{tell}(C_2)$ are intended.

One of the beautiful properties of kernel operators is that they can be uniquely represented by their range, i.e. the set of their fixed points [27]. The denotational semantics of finite cc agents over $\bar{\mathcal{D}}$ is thus conveniently expressed by a function $[\![\cdot]\!]\colon \mathcal{A}(\bar{\mathcal{D}}) \to \wp(\mathcal{D})$ defined following [45].

Definition 33 (Semantics of finite cc agents.) *The semantics of finite* cc *agents over a constraint systems* $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{X}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$ *is given by the following equations:*

$$[\![C]\!] \stackrel{\text{def}}{=} {\downarrow} C, \tag{15}$$

$$[\![C \to A]\!] \stackrel{\text{def}}{=} \overline{{\downarrow} C} \cup {\downarrow} A, \tag{16}$$

$$[\![A \parallel B]\!] \stackrel{\text{def}}{=} [\![A]\!] \cap [\![B]\!]. \tag{17}$$

Observe that the actual kernel operator A^K corresponding to a finite agent $A \in \mathcal{A}(\bar{\mathcal{D}})$ can be recovered from $[\![A]\!]$ as

$$A^K \stackrel{\text{def}}{=} \lambda C \,.\, \sup\Big(({\downarrow} C) \cap [\![A]\!]\Big). \tag{18}$$

The introduction of a syntactic normal form for finite cc agents allows to simplify the subsequent semantic treatment.

Definition 34 (Finite cc agents: syntactic normal form.) *The transformation* η *over* $\mathcal{A}(\bar{\mathcal{D}})$ *is defined, for each* $C^a, C_1^a, C_2^a, C^t \in \mathcal{D}$ *and* $A, A_1, A_2 \in \mathcal{A}(\bar{\mathcal{D}})$*, as follows:*

$$\eta(C^a \to C^t) \stackrel{\text{def}}{=} \begin{cases} \mathbf{1} \to \mathbf{1}, & \text{if } C^a \vdash C^t; \\ C^a \to (C^a \otimes C^t), & \text{otherwise;} \end{cases}$$

$$\eta(C^t) \stackrel{\text{def}}{=} \mathbf{1} \to C^t,$$

$$\eta\Big(C_1^a \to (C_2^a \to A)\Big) \stackrel{\text{def}}{=} \eta\Big((C_1^a \otimes C_2^a) \to A\Big),$$

$$\eta\Big(C^a \to (A_1 \parallel A_2)\Big) \stackrel{\text{def}}{=} \eta\Big((C^a \to A_1) \parallel (C^a \to A_2)\Big),$$

$$\eta(A_1 \parallel A_2) \stackrel{\text{def}}{=} \eta(A_1) \parallel \eta(A_2).$$

The following fact is easily proved.

Proposition 35 *The transformation η of* Definition 34 *is well defined. Furthermore, if $A \in \mathcal{A}(\bar{\mathcal{D}})$ then $[\![\eta(A)]\!] = [\![A]\!]$ and $\eta(A)$ is of the form*

$$(C_1^a \to C_1^t) \parallel \cdots \parallel (C_n^a \to C_n^t).$$

where $C_i^t \Vdash C_i^a$ for each $i = 1, \ldots, n$.

PROOF. Observe that each agent is in one and only one of the forms appearing in the left-hand sides of the equations. Given an agent, define its *complexity* as the number obtained by summing up the number 3 for each connective (i.e. '$\parallel$' and '$\to$') occurring in a guarded context (i.e. in $C \to A$ the connectives in A are worth 3), and the number 1 for all the other connectives. It is immediate to verify that in the recursive equations of Definition 34 the arguments of η in the right-hand sides have complexity strictly less than the ones in the left-hand sides, while the right-hand sides of non-recursive equation are of the form $C^a \to C^t$. Thus η is indeed a function, and its range is as stated. The fact that η is semantic-preserving can be shown by total induction on the complexity of agents. The base cases are trivial. For the induction step we have, for instance,

$$\begin{aligned}
[\![C^a \to (A_1 \parallel A_2)]\!] &= \overline{\downarrow C^a} \cup \Big([\![A_1]\!] \cap [\![A_2]\!]\Big) \\
&= \Big(\overline{\downarrow C^a} \cup [\![A_1]\!]\Big) \cap \Big(\overline{\downarrow C^a} \cup [\![A_2]\!]\Big) \\
&= \Big[\!\Big[(C^a \to A_1) \parallel (C^a \to A_2)\Big]\!\Big] \\
&= \Big[\!\Big[\eta\Big((C^a \to A_1) \parallel (C^a \to A_2)\Big)\Big]\!\Big] \\
&= \Big[\!\Big[\eta\Big(C^a \to (A_1 \parallel A_2)\Big)\Big]\!\Big]. \qquad \Box
\end{aligned}$$

Thus, by considering only agents of the form $\|_{i=1}^n C_i^a \to C_i^t$ we do not loose any generality. We will call elementary agents of the kind $C^a \to C^t$ *ask-tell pairs*.

Now we express the operational semantics of finite cc agents by means of rewrite rules. An agent in syntactic normal form is rewritten by applying the logical rules of the calculus modulo a structural congruence. This congruence states, intuitively, that we can regard an agent as a set of (concurrent) ask-tell pairs. The semantics of parallel composition stated in (17) clearly allows that.

Definition 36 (A calculus of finite cc agents.) *Let $\mathbf{1}_{\mathrm{A}} \stackrel{\text{def}}{=} \mathbf{1} \to \mathbf{1}$. The* structural congruence *of the calculus is the smallest congruence relation $\equiv_s$ such that $\langle \mathcal{A}(\bar{\mathcal{D}}), \|, \mathbf{1}_{\mathrm{A}} \rangle_{/\equiv_s}$ is a commutative and idempotent monoid. The reduction rules of the calculus are given in* Figure 2. *We also define the relation*

Structure

$$\frac{A_1 \equiv_s A_1' \quad A_1' \longmapsto A_2' \quad A_2' \equiv_s A_2}{A_1 \longmapsto A_2} \qquad \frac{A_1 \longmapsto A_1'}{A_1 \parallel A_2 \longmapsto A_1' \parallel A_2}$$

Reduction $r(1,2)$

$$\frac{C_1^a \vdash C_2^a \qquad C_1^a \otimes C_2^t \vdash C_1^t}{(C_1^a \to C_1^t) \parallel (C_2^a \to C_2^t) \longmapsto (C_2^a \to C_2^t)}$$

Deduction $d(1,2)$

$$\frac{C_1^t \vdash C_2^a \qquad C_1^t \nvdash C_2^t}{(C_1^a \to C_1^t) \parallel (C_2^a \to C_2^t) \longmapsto \Big(C_1^a \to (C_1^t \otimes C_2^t)\Big) \parallel (C_2^a \to C_2^t)}$$

Absorption $a(1,2)$

$$\frac{C_1^a \Vdash C_2^a \qquad C_1^a \nvdash C_2^t \qquad C_1^t \Vdash C_1^a \otimes C_2^t}{(C_1^a \to C_1^t) \parallel (C_2^a \to C_2^t) \longmapsto \Big((C_1^a \otimes C_2^t) \to C_1^t\Big) \parallel (C_2^a \to C_2^t)}$$

Fig. 2. Reduction rules for finite cc agents.

$\rho_{\mathrm{A}} \subseteq \mathcal{A}(\bar{\mathcal{D}}) \times \mathcal{A}(\bar{\mathcal{D}})$ *given, for each* $A, A' \in \mathcal{A}(\bar{\mathcal{D}})$, *by*

$$A \;\rho_{\mathrm{A}}\; A' \stackrel{\text{def}}{\Longleftrightarrow} \exists n \in \mathbb{N} \,.\, A = A_1 \wedge A_n = A' \wedge A_1 \mapsto A_2 \mapsto \cdots \mapsto A_n \mapsto\!\!\!\!\!\!\rightarrow$$

In the following we will systematically abuse the notation denoting $\mathcal{A}(\bar{\mathcal{D}})_{/\equiv_s}$ simply by $\mathcal{A}(\bar{\mathcal{D}})$. Consequently, every assertion concerning $\mathcal{A}(\bar{\mathcal{D}})$ is to be intended *modulo structural congruence*.

Lemma 37 *The term-rewriting system depicted in* Figure 2 *is terminating. Thus, for each* $A \in \mathcal{A}(\bar{\mathcal{D}})$ *there is always an* $A' \in \mathcal{A}(\bar{\mathcal{D}})$ *such that* $A \;\rho_{\mathrm{A}}\; A'$.

PROOF. Consider an agent in syntactic normal form $A = \|_{i=1}^{n} A_i$. Each rewriting step results either in the removal of a pair (at most $n-1$ such steps can be performed using the reduction rule), or in the strict strengthening of the ask or tell constraint of a pair. An upper bound for the number of such steps can be obtained by reasoning as follows. The tell constraint of each of the n pairs can be strengthened at most $n-1$ times. Thus at most $n(n-1)$ applications of the deduction rule are possible. Similarly, the absorption rule will be applied, in the worst conceivable case, at most $n(n-1)$ times. Consequently, A will be maximally rewritten in $O(n^2)$ steps. $\square$

We introduce now, following [45], a normal form for finite cc agents.

Definition 38 (Semantic normal form.) [45] *An agent $A \in \mathcal{A}(\bar{\mathcal{D}})$ is* in semantic normal form *if and only if $A = \mathbf{1}_{\mathrm{A}}$ or $A = \|_{i=1}^{n} C_i^a \to C_i^t$ and, for each $i, j \in \{1, \ldots, n\}$:*

N_1. $C_i^t \Vdash C_i^a$;
N_2. $i \neq j \implies C_i^a \neq C_j^a$;
N_3. $C_i^a \Vdash C_j^a \implies C_i^a \Vdash C_j^t$;
N_4. $C_i^t \vdash C_j^a \implies C_i^t \vdash C_j^t$.

It turns out that this normal form is indeed very strong, whence its name.

Theorem 39 [45] *Two agents $A_1, A_2 \in \mathcal{A}(\bar{\mathcal{D}})$ have the same semantic normal form if and only if $[\![A_1]\!] = [\![A2]\!]$.*

The purpose of our rewriting system is to put finite cc agents into semantic normal form, preserving their original semantics.

Lemma 40 *For each agent $A \in \mathcal{A}(\bar{\mathcal{D}})$ in syntactic normal form, if $A \ \rho_{\mathrm{A}} \ A'$ then $[\![A]\!] = [\![A']\!]$ and A' is in semantic normal form.*

PROOF. It is immediate to verify that the rules of the calculus preserve the syntactic normal form, thus A' satisfies condition N_1.

Suppose N_2 is not satisfied, i.e. $C_i^a = C_j^a$ and, consequently, $C_i^t \neq C_j^t$, $C_i^t \Vdash C_j^a$, and $C_j^t \Vdash C_i^a$. Since either $C_i^t \nvdash C_j^t$ or $C_j^t \nvdash C_i^t$ must hold, we can apply the deduction rule $d(i,j)$ or $d(j,i)$, respectively.

Now, should N_3 not be satisfied, namely $C_i^a \Vdash C_j^a$ and $C_i^a \nVdash C_j^t$ (implying $C_i^t \Vdash C_j^a$) there are several cases. If $C_i^a = C_j^t$ then $C_i^t \Vdash C_i^a = C_j^t$, thus $C_j^t \vdash C_i^a$ and $C_j^t \nvdash C_i^t$ which means $d(j,i)$ is applicable. The other possibility is when $C_i^a \nvdash C_j^t$ and either $C_j^t \vdash C_i^t$ or $C_j^t \nvdash C_i^t$. In the former case we have $C_j^t \vdash C_i^t \Vdash C_i^a$, whence $C_i^a \otimes C_j^t = C_j^t \vdash C_i^t$ and $r(i,j)$ can fire. The latter case is further split as follows: if $C_i^t \nvdash C_j^t$ then rule $d(i,j)$ is applicable, otherwise we have $C_i^t \Vdash C_j^t$, which implies $C_i^t \vdash C_i^a \otimes C_j^t$. If this last entailment is strict the absorption rule $a(i,j)$ can fire, if not (namely $C_i^t = C_i^a \otimes C_j^t$), then we can apply $r(i,j)$.

Finally, negating N_4 we obtain $C_i^t \vdash C_j^a$ and $C_i^t \nvdash C_j^t$, which is exactly the applicability condition for $d(i,j)$.

Preservation of semantics is readily verified. For reduction, we show that if $C_1^a \vdash C_2^a$ and $C_1^a \otimes C_2^t \vdash C_1^t$ then $[\![(C_1^a \to C_1^t) \,\|\, (C_2^a \to C_2^t)]\!] = [\![C_2^a \to C_2^t]\!]$, or,

equivalently,

$$\forall C \in \mathcal{D} : [\![C_2^a \to C_2^t]\!]^K(C) \vdash [\![C_1^a \to C_1^t]\!]^K(C).$$

In fact, if $C \not\vdash C_1^a$ then $[\![C_1^a \to C_1^t]\!]^K(C) = C$ and the thesis hold by extensivity of $[\![C_2^a \to C_2^t]\!]^K$. If $C \vdash C_1^a$ then $C \vdash C_2^a$ and $[\![C_2^a \to C_2^t]\!]^K(C) = C \otimes C_2^t = C \otimes C_1^a \otimes C_2^t \vdash C \otimes C_1^t = [\![C_1^a \to C_1^t]\!]^K(C)$. The reader is also referred to [45] where less constrained versions of deduction and absorption are reported as laws *L12* and *L11*, respectively. □

Proposition 41 *The term-rewriting system depicted in* Figure 2 *is strongly normalizing. Thus the relation* ρ_{A} *is indeed a function* $\rho_{\mathrm{A}}\colon\ \mathcal{A}(\bar{\mathcal{D}}) \to \mathcal{A}(\bar{\mathcal{D}})$.

PROOF. Let $A \in \mathcal{A}(\bar{\mathcal{D}})$ in syntactic normal form, and suppose $A\ \rho_{\mathrm{A}}\ A'$ and $A\ \rho_{\mathrm{A}}\ A''$. By Lemma 40 both A' and A'' are in semantic normal form, and $[\![A']\!] = [\![A]\!] = [\![A'']\!]$. By Theorem 39 we can conclude that $A' = A''$.

The final result is now easily obtained.

Corollary 42 *For* $A_1, A_2 \in \mathcal{A}(\bar{\mathcal{D}})$ *we have* $\rho_{\mathrm{A}}(A_1) = \rho_{\mathrm{A}}(A_2)$ *iff* $[\![A_1]\!] = [\![A2]\!]$.

PROOF. By Proposition 41 $\rho_{\mathrm{A}}(A_1)$ and $\rho_{\mathrm{A}}(A_2)$ are well defined while, by Lemma 40, we have $[\![A_1]\!] = [\![\rho_{\mathrm{A}}(A_1)]\!]$ and $[\![A_2]\!] = [\![\rho_{\mathrm{A}}(A_2)]\!]$ and both $\rho_{\mathrm{A}}(A_1)$ and $\rho_{\mathrm{A}}(A_2)$ are in semantic normal form. Thus $\rho_{\mathrm{A}}(A_1) = \rho_{\mathrm{A}}(A_2)$ if and only if A_1 and A_2 have the same normal form. Theorem 39 ensures that this is equivalent to $[\![A_1]\!] = [\![A2]\!]$. □

The situation here is almost identical to the one of Definition 25, in that we have a domain-independent strong normal form also for the present class of constraints (i.e. agents) incorporating the notion of dependency.

Definition 43 (Elements.) *The* elements *of* $\mathcal{A}(\bar{\mathcal{D}})$ *are those which are closed under (are the fixed points of) the* inference map ρ_{A}. *The set of elements of* $\mathcal{A}(\bar{\mathcal{D}})$ *will be denoted by* $|\mathcal{A}(\bar{\mathcal{D}})|$.

We are now in position to introduce a new class in our hierarchy of constraint systems. Again we present only the finite fragment of the constraint system. Here, the finite elements are precisely the finite cc agents in $|\mathcal{A}(\bar{\mathcal{D}})|$.

Definition 44 (Ask-and-tell constraint system.) *Given a constraint system* $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\bar{\Lambda}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$, *let* $\mathcal{A} = |\mathcal{A}(\bar{\mathcal{D}})|$. *Then let* $\mathbf{0}_{\mathrm{A}}, \mathbf{1}_{\mathrm{A}} \in \mathcal{A}$,

and $\otimes_{\mathrm{A}} : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ *be given, for each* $A_1, A_2 \in \mathcal{A}$*, by*

$$\mathbf{0}_{\mathrm{A}} \stackrel{\text{def}}{=} \mathbf{1} \to \mathbf{0}, \qquad A_1 \otimes_{\mathrm{A}} A_2 \stackrel{\text{def}}{=} \rho_{\mathrm{A}}(A_1 \parallel A_2).$$
$$\mathbf{1}_{\mathrm{A}} \stackrel{\text{def}}{=} \mathbf{1} \to \mathbf{1},$$

The projection operators $\bar{\exists}^{\mathrm{A}}_{\vec{\Lambda}} : \mathcal{A} \to \mathcal{A}$ *are given, for each* $\vec{\Lambda} \subseteq_f Vars$ *and* $A \in \mathcal{A}$*, by*[13]

$$\bar{\exists}^{\mathrm{A}}_{\vec{\Lambda}} A \stackrel{\text{def}}{=} \rho_{\mathrm{A}} \left(\left\{ \left(\bar{\exists}_{\vec{\Lambda}} C^a \to \bar{\exists}_{\vec{\Lambda}} C^t \right) \;\middle|\; \begin{array}{l} \left(C^t \to C^a \right) \in A \quad \textit{and} \\ \left(\left(\mathbf{1} \to \bar{\exists}_{\vec{\Lambda}} C^a \right) \otimes_{\mathrm{A}} A \right) \vdash_{\mathrm{A}} \left(\mathbf{1} \to C^a \right) \end{array} \right\} \right).$$

Finally, let $\oplus_{\mathrm{A}} : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ *be an operator satisfying the conditions* G_2 *and* G_4 *of* Definition 7*. For any indexed family* $\{d^{\mathrm{A}}_{\bar{X}\bar{Y}}\}_{\bar{X},\bar{Y} \in Vars^\star}$ *of elements of* $\mathcal{A}$*, we will refer to* $\langle \mathcal{A}(\bar{\mathcal{D}}), \otimes_{\mathrm{A}}, \oplus_{\mathrm{A}}, \mathbf{0}_{\mathrm{A}}, \mathbf{1}_{\mathrm{A}}, \{\bar{\exists}^{\mathrm{A}}_{\vec{\Lambda}}\}, \{d^{\mathrm{A}}_{\bar{X}\bar{Y}}\} \rangle$ *as to an* ask-and-tell constraint system *over* $\bar{\mathcal{D}}$ *and* $\oplus_{\mathrm{A}}$*.*

Notice that, as far as the diagonal elements are concerned, we have left complete freedom. This is because, in an ask-and-tell construction, the induced diagonals $d^{\mathrm{A}}_{\bar{X}\bar{Y}} = \mathbf{1} \to d_{\bar{X}\bar{Y}}$ are not necessarily a good choice (see Section 7.3 for a simple example).

The projection operators are indeed quite complicated. The problem is originated from requirement N_3 of the normal form of Definition 38. This requirement enforces the need of the absorption rule in the calculus. The rule, by strengthening the ask-constraint of pairs, introduces "false dependencies". Consider, for instance, a constraint system where elements include the finite subsets of $\{\, p(X), q(X), r(X) \mid X \in Vars \,\}$ and the operators $\otimes$ and $\oplus$ are set union and intersection, respectively. The non-normalized cc agent over this constraint system

$$A = \mathbf{1} \to \{q(Y)\} \parallel \{p(X)\} \to \{r(X), q(Y)\}$$

is normalized, by means of the absorption rule, to

$$A' = \mathbf{1} \to \{q(Y)\} \parallel \{p(X), q(Y)\} \to \{r(X), q(Y)\}.$$

The absorption rule has thus introduced the dependency of $r(X)$ from $q(Y)$, which is indeed false in the context of A' (as it was in the context of A). A definition of the projection operators not taking into account this phenomenon would cause the inaccurate result $\bar{\exists}^{\mathrm{A}}_{X} A' = \mathbf{1}_{\mathrm{A}}$. The projection operators given in Definition 44, instead, recognize the false dependency by noting that $\{p(X)\} = \bar{\exists}_X \{p(X), q(Y)\}$ is, in the context of A', equivalent to

[13] Notice that, for simplicity, we regard an agent as the set of its ask-tell pairs.

$\{p(X), q(Y)\}$, that is

$$\mathbf{1} \to \{p(X)\} \parallel A' \quad \vdash_{\mathrm{A}} \quad \mathbf{1} \to \{p(X), q(Y)\}.$$

We can thus obtain the expected result $\bar{\exists}^{\mathrm{A}}_X A' = \{p(X)\} \to \{r(X)\}$. We will see in a moment other problems provoked by the absorption rule and, in turn, by the normal form we employ for agents.

Theorem 45 *If $\bar{\mathcal{D}}$ is a constraint system $\langle |\mathcal{A}(\bar{\mathcal{D}})|, \otimes_{\mathrm{A}}, \oplus_{\mathrm{A}}, \mathbf{0}_{\mathrm{A}}, \mathbf{1}_{\mathrm{A}}, \{\bar{\exists}^{\mathrm{A}}_{\vec{X}}\}, d^{\mathrm{A}}_{\vec{X}\vec{Y}} \rangle$ is so.*

PROOF. An ask-tell pair is a constraint by virtue of point (iii) in Definition 5, viewing '$\to$' as a binary (meta-level) predicate. Thus condition G_0 is true by point (ii) of the same definition. $\langle \mathcal{A}(\bar{\mathcal{D}}), \otimes_{\mathrm{A}}, \mathbf{1}_{\mathrm{A}} \rangle$ is immediately verified being a commutative and idempotent monoid with zero element $\mathbf{0}_{\mathrm{A}}$, thus satisfying axioms G_1 and G_3. The requirements G_2, G_4, and G_5 are immediate consequences of the definition of ask-and-tell c.s. $\square$

7.1 Merge operators

Even though the ask-and-tell construction is parameterized with respect to a merge operator, it is possible to induce such an operator from the one of the base-level constraint system. Since this is a problematic point we proceed with care.

Suppose that the base-level constraint system $\bar{\mathcal{D}}$ is a lattice. Thus kernel operators over $\bar{\mathcal{D}}$ form again a lattice, where the *lub* is given, for k_1 and k_2 kernel operators and for each $C \in \mathcal{D}$, by

$$(k_1 \sqcup k_2)(C) \stackrel{\mathrm{def}}{=} k_1(C) \oplus k_2(C), \quad \text{for } C \in \mathcal{D}, \tag{19}$$

whose fixed points are

$$(k_1 \sqcup k_2)(\mathcal{D}) = \Big\{ C_1 \oplus C_2 \;\Big|\; C_1, C_2 \in k_1(\mathcal{D}) \cup k_2(\mathcal{D}) \Big\}.$$

In terms of kernel operators, as pointed out in [44], this can be thought of as a kind of *determinate disjunction*: $k_1 \sqcup k_2$ gives, on any input C, the strongest common information between k_1 and k_2. The computational significance of this concept has been first recognized in [51], where determinate disjunction allows for significant improvements in some constraint propagation algorithms.

The problem is that, even when k_1 and k_2 are represented by finite cc agents A_1 and A_2, namely $k_1 = A_1^K$ and $k_2 = A_2^K$, we have no guarantees whatsoever

that $k_1 \sqcup k_2$ is representable by a finite cc agent [14]. In other words, (syntactic) finite cc agents are not, in general, closed under the (semantic) *lub* operation. As a consequence, we must content ourselves with upper bounds (unless we are willing to enrich our representation language with a construct like $A_1 + A_2$ expressing determinate disjunction, and we are not). Observe that the very precise effect of (19) can be obtained (at a consequently high cost) applying a powerset construction (Section 6) to the ask-and-tell constraint system considered. This way, when merging two (non-redundant) agents we will keep both of them, thus realizing, in practice, the '+' construct mentioned above. If we do that, obviously, there is no need at all to define a merge operator at the ask-and-tell level.

In our general situation, the base-level constraint system $\bar{\mathcal{D}}$ might not be a lattice, and (19) might not define a kernel operator. In these cases, an upper bound on the poset of kernel operators over $\bar{\mathcal{D}}$ can be given as

$$(k_1 \tilde{\sqcup} k_2)(C) \stackrel{\text{def}}{=} C \otimes \Big(k_1(C) \oplus k_2(C)\Big), \quad \text{for } C \in \mathcal{D}, \tag{20}$$

which, still, is not guaranteed to correspond to any finite cc agent over $\bar{\mathcal{D}}$.

We stress again that our non-commitment to lattices in the general definition of constraint systems (Section 3.3) is not merely dictated by the desire of freely managing the complexity/precision tradeoff. In cases like the one at hand we have no other sensible choice due to representation problems.

The journey towards computable merge operators starts with a simple operation merging two (not necessarily normalized) agents into one. This is done, roughly speaking, by taking the meet of the ask constraints, and the merge of the tell constraints.

Definition 46 (Merge operator over agents.) *Consider a constraint system* $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\bar{\Lambda}}\}, \{d_{\bar{X}\bar{Y}}\}\rangle$*, and any two finite* cc *agents over* $\bar{\mathcal{D}}$ *in syntactic normal form:*

$$A_1 = \|_{i=1}^{n} C_i^a \to C_i^t \quad \textit{and} \quad A_2 = \|_{j=1}^{m} D_j^a \to D_j^t.$$

Then

$$A_1 \,\tilde{\oplus}_{\mathrm{A}}\, A_2 \stackrel{\text{def}}{=} \|_{i=1}^{n} \|_{j=1}^{m} (C_i^a \to C_i^t) \,\tilde{\oplus}_{\mathrm{A}}\, (D_j^a \to D_j^t), \tag{21}$$

[14] For the interested reader: consider a c.s. with distinct elements $\{\mathbf{0}, \mathbf{1}\} \cup \{C_i\}_{i \in \mathbb{N}_0}$ and such that $C_i \vdash C_j$ iff $1 \leq i \leq j$. The *lub* of $\mathbf{1} \to C_0$ and $\mathbf{1} \to C_1$ is not expressible by a finite cc agent. The same happens if the ordering is such that $C_i \nvdash C_j$ for all i and j.

where, if we let $C^a_{ij} \stackrel{\text{def}}{=} C^a_i \otimes D^a_j$ *and* $C^t_{ij} \stackrel{\text{def}}{=} C^t_i \oplus D^t_j$*, we have*

$$(C^a_i \to C^t_i) \,\tilde{\oplus}_{\text{A}}\, (D^a_j \to D^t_j) \stackrel{\text{def}}{=} \begin{cases} \mathbf{1}_{\text{A}}, & \text{if } C^a_{ij} \vdash C^t_{ij}; \\ C^a_{ij} \to (C^a_{ij} \otimes C^t_{ij}), & \text{otherwise.} \end{cases} \tag{22}$$

It is easy to see that this syntactic operation corresponds, at the semantic level, to an upper bound.

Proposition 47 *If* A_1 *and* A_2 *are as stated in* Definition 46*, then* $A_1 \,\tilde{\oplus}_{\text{A}}\, A_2$ *is in syntactic normal form. Further, we have both* $[\![A_1]\!] \subseteq [\![A_1 \,\tilde{\oplus}_{\text{A}}\, A_2]\!]$ *and* $[\![A_2]\!] \subseteq [\![A_1 \,\tilde{\oplus}_{\text{A}}\, A_2]\!]$*, that is,* $A_1 \vdash_{\text{A}} A_1 \,\tilde{\oplus}_{\text{A}}\, A_2$ *and* $A_2 \vdash_{\text{A}} A_1 \,\tilde{\oplus}_{\text{A}}\, A_2$*.*

PROOF. Preservation of syntactic normal form is clearly guaranteed in (22). Then, for each $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$, we have $C^a_i \otimes D^a_j \vdash C^a_i$ which implies $\downarrow\!(C^a_i \otimes D^a_j) \subseteq \downarrow\! C^a_i$, that is $\overline{\downarrow\! C^a_i} \subseteq \overline{\downarrow\!(C^a_i \otimes D^a_j)}$. Similarly, from the correctness of the base-level merge operator, namely $C^t_i \vdash C^t_i \oplus D^t_j$, we get $\downarrow\! C^t_i \subseteq \downarrow\!(C^t_i \oplus D^t_j)$. Combining these two relations we obtain, for each i and j,

$$\overline{\downarrow\! C^a_i} \cup \downarrow\! C^t_i \subseteq \overline{\downarrow\!(C^a_i \otimes D^a_j)} \cup \downarrow\!(C^t_i \oplus D^t_j),$$

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

$$\overline{\downarrow\! C^a_i} \cup \downarrow\! C^t_i \subseteq \bigcap_{j=1}^{m} \Big(\overline{\downarrow\!(C^a_i \otimes D^a_j)} \cup \downarrow\!(C^t_i \oplus D^t_j) \Big),$$

from which

$$[\![A_1]\!] = \bigcap_{i=1}^{n} [\![C^a_i \to C^t_i]\!] \subseteq \bigcap_{i=1}^{n} \Big[\!\Big[\|_{j=1}^{m} C^a_i \otimes D^a_j \to C^t_i \oplus D^t_j \Big]\!\Big] = [\![A_1 \,\tilde{\oplus}_{\text{A}}\, A_2]\!]$$

follows. A symmetric argument proves that $[\![A_2]\!] \subseteq [\![A_1 \,\tilde{\oplus}_{\text{A}}\, A_2]\!]$. $\square$

We now have an obvious merge operator which is completely determined by the underlying, base-level constraint system.

Definition 48 (Canonical ask-tell merge operator.) *Let* $\mathcal{A} \stackrel{\text{def}}{=} |\mathcal{A}(\bar{\mathcal{D}})|$*. The operator* $\hat{\oplus}_{\text{A}} \colon \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ *given, for each* $A_1, A_2 \in \mathcal{A}$*, by*

$$A_1 \,\hat{\oplus}_{\text{A}}\, A_2 \stackrel{\text{def}}{=} \rho_{\text{A}}(A_1 \,\tilde{\oplus}_{\text{A}}\, A_2)$$

is called the canonical merge operator over $\mathcal{A}$ induced by $\mathcal{D}$*.*

Notice that canonical ask-and-tell constraint systems subsume their base-level c.s., where only "tells" are considered. In fact we have $\eta(C_1) \otimes_{\mathrm{A}} \eta(C_2) = \eta(C_1 \otimes C_2)$ and $\eta(C_1) \hat{\oplus}_{\mathrm{A}} \eta(C_2) = \eta(C_1 \oplus C_2)$.

Unfortunately, the canonical merge operator turns out to be inaccurate, due to the normal form employed for agents. Consider the ask-and-tell construction applied to the *Con* domain of Section 5.1, and the agents in normal form [15]

$$A_1 \stackrel{\text{def}}{=} \mathbf{1} \to Z \parallel XZ \to XYZ \quad \text{and} \quad A_2 \stackrel{\text{def}}{=} X \to XY.$$

It easy to see that the canonical merge operator gives

$$A_1 \hat{\oplus}_{\mathrm{A}} A_2 \stackrel{\text{def}}{=} \rho_{\mathrm{A}}(A_1 \tilde{\oplus}_{\mathrm{A}} A_2) = XZ \to XYZ.$$

If we consider the non-normalized agent $A_1' = \mathbf{1} \to Z \parallel X \to XYZ$, we have $[\![A_1']\!] = [\![A_1]\!]$ but $\rho_{\mathrm{A}}(A_1' \tilde{\oplus}_{\mathrm{A}} A_2) = X \to XY$, which is strictly stronger than $A_1 \hat{\oplus}_{\mathrm{A}} A_2$.

The problem can be tracked down, as in the case of the projection operators, to the introduction, by means of the absorption rule, of "unnecessary dependencies" needed to satisfy condition N_3 of the semantic normal form. However, while for projection operators we had a standard solution, here the situation is more difficult. Moreover, looking at the example above, one is caught by the doubt that, perhaps, the choice of the normal form of Definition 38 was a poor one, since it is based on maximal strengthening of both *tell* and *ask* constraints. We are thus lead to the following question:

> Does it exist an alternative normal form for finite cc agents based on maximal strengthening of tell constraints and maximal *weakening* of ask constraints?

We might tentatively go as follows. Consider a Noetherian constraint system $\bar{\mathcal{D}}$ and an agent $A = \|_{i=1}^{n} C_i^a \to C_i^t$ over $\bar{\mathcal{D}}$ in semantic normal form (Definition 38). For each $j \in \{1, \ldots, n\}$, let the agent A_{-j} be given by

$$A_{-j} \stackrel{\text{def}}{=} \mathop{\Big\|}_{\substack{i=1 \\ i \neq j}}^{n} C_i^a \to C_i^t,$$

and define the set of constraints

$$D_j \stackrel{\text{def}}{=} \Omega_{\mathcal{D}}^{\vdash}\Big(\big\{ C \in \mathcal{D} \;\big|\; [\![C \to C_j^t \parallel A_{-j}]\!] = [\![A]\!] \big\} \Big).$$

In words, for each ask-tell pair in the original agent A, we consider the set of minimal constraints that can be substituted in the ask part without changing

[15] For simplicity we use juxtaposition instead of the usual set notation.

the semantics of A. Observe that, for each $j = 1, \ldots, n$, either $D_j = \{C_j^a\}$ or D_j contains only incomparable constraints strictly weaker than C_j^a. Whenever the base-level constraint system $\bar{\mathcal{D}}$ is such to ensure that all the D_j's so obtained will always be finite, then the answer to the above question is positive, and the normal form of A (in this new sense) is given by

$$\bigparallel_{j=1}^{n} \bigparallel_{C \in D_j} C \to C_j^t.$$

Such a normal form would give us, in the same spirit of Definition 48, a very precise merge operator while allowing for a simplification of the projection operators. However, even in the cases where this normal form exists, we remain with the problem of computing it. This requires something very different from the rewriting system of Figure 2, as we will need mechanisms for

(i) *weakening* constraints (now we only *strengthen* them), and
(ii) *splitting* ask-tell pairs (now we only *combine* them).

Moreover, while our current rewriting system is *local*, i.e. each rewriting depends on only two pairs, computing the new normal form requires looking at all the agents being normalized. This, together with the fact that splitting can give rise to an exponential number of new pairs, could push us beyond polynomial complexity.

While this is certainly a subject for further study, we now give a general way of defining merge and widening operators for the ask-and-tell construction which are more precise than the canonical merge operator. First of all, let us deal with the problem of constraints' weakening.

Definition 49 (Weakening.) *An operation $\circledcirc \colon \mathcal{D} \to \mathcal{D}$ on a constraint system $\bar{\mathcal{D}} = \langle \mathcal{D}, \otimes, \oplus, \mathbf{0}, \mathbf{1}, \{\bar{\exists}_{\vec{X}}\}, \{d_{\vec{X}\vec{Y}}\}\rangle$ which satisfies for each $C, C_1, C_2 \in \mathcal{D}$:*

Q_1. $(C_1 \circledcirc C_2) \otimes C_1 = C_1$,
Q_2. $(C_1 \circledcirc C_2) \otimes C_2 = C_1 \otimes C_2$,
Q_3. $(C_1 \circledcirc C_2) \circledcirc C_2 = C_1 \circledcirc C_2$,

is said a weakening operator for $\bar{\mathcal{D}}$.

The intuitive explanation of this axiomatization is as follows. Condition Q_1, which can be restated as $C_1 \vdash C_1 \circledcirc C_2$, means that the weakening operation is correct (it does not add anything). Condition Q_2 states that weakenings are not too aggressive: a weakened constraint can be restored by *adding* what was *taken out*. Q_3 says that taking out twice the same thing is pointless. Observe that these conditions are very weak, while being sufficient for what follows. A class of powerful weakening operators is defined next.

Definition 50 (Best weakening operator.) *A weakening operator over a*

constraint system $\bar{\mathcal{D}}$ *is a* best weakening *if and only if, for each* $C_1, C_2 \in \mathcal{D}$,

Q_4. $\forall C \in \mathcal{D} : C \otimes C_2 = C_1 \otimes C_2 \implies C \vdash (C_1 \circledcirc C_2)$.

Notice that conditions Q_2 and Q_4 are sufficient to define best weakenings, as Q_1 and Q_3 necessarily follow. Best weakenings are also monotonic on the first argument and antitonic on the second one [16] .

Example 51 (Weakening over intervals.) *Consider a domain for numerical bounds analysis based on intervals. For instance, take the simple constraint system of* Section 4.4, *restricted to the intervals component, and apply to it the determinate c.s. construction. A weakening operator can be defined along the following lines, considering, for simplicity, only closed intervals:*

$$[\, l_1, u_1 \,] \circledcirc [\, l_2, u_2 \,] \stackrel{\text{def}}{=} [\, l, u \,],$$

where

$$l \stackrel{\text{def}}{=} \begin{cases} -\infty, & \text{if } l_1 \leq l_2; \\ l_1, & \text{otherwise;} \end{cases} \qquad \text{and} \qquad u \stackrel{\text{def}}{=} \begin{cases} +\infty, & \text{if } u_1 \geq u_2; \\ u_1, & \text{otherwise.} \end{cases}$$

Such an operator is easily verified being a weakening. It is also monotonic on the first argument and antitonic on the second one. All these extra-properties, however, are not necessary for what follows.

The following lemma will be useful in the sequel.

Lemma 52 *Let* $\circledcirc$ *be a weakening over a c.s.* $\bar{\mathcal{D}}$. *For each* $C_1, C_2 \in \mathcal{D}$, *if* $C \in \mathcal{D}$ *is such that* $C \vdash C_2$ *and* $C \nvdash C_1$, *then* $C \nvdash (C_1 \circledcirc C_2)$.

PROOF. Suppose that $C \vdash C_2$, $C \nvdash C_1$, and $C \vdash (C_1 \circledcirc C_2)$. In other words, we have $C \otimes C_2 = C$, $C \otimes C_1 \neq C$, $C \otimes (C_1 \circledcirc C_2) = C$, and, by axiom Q_2, $(C_1 \circledcirc C_2) \otimes C_2 = C_1 \otimes C_2$. So,

$$\begin{aligned} C \otimes C_2 &= \Big(C \otimes (C_1 \circledcirc C_2)\Big) \otimes C_2 \\ &= C \otimes \Big((C_1 \circledcirc C_2) \otimes C_2\Big) \\ &= C \otimes (C_1 \otimes C_2) \\ &= (C \otimes C_2) \otimes C_1 \\ &= C \otimes C_1 \\ &\neq C, \end{aligned}$$

[16] The connection between our weakenings and the class of *weak relative pseudo-complements* over meet-semilattices, recently introduced in [25], needs to be studied.

thus reaching the absurd conclusion $C \nvdash C_2$. $\square$

We are now in position to define a class of procedures for weakening the ask constraints of finite cc agents while preserving the semantics. As this operation is somewhat opposite to the absorption rewrite rule of our rewriting system, we call it *de-absorption*. This includes the possibility of *splitting* ask-tell pairs.

Definition 53 (De-absorption step.) *Let $A = \|_{i=1}^{n} C_i^a \to C_i^t$ an agent in syntactic normal form over a c.s. $\bar{\mathcal{D}}$, and let $\circledcirc$ be a weakening over $\bar{\mathcal{D}}$. Then A' is obtained from A by means of a* de-absorption step based on $\circledcirc$ *if and only if $h, k \in \{1, \ldots, n\}$ are such that $C_h^a \vdash C_k^a$, the condition $C_h^a \neq (C_h^a \circledcirc C_k^t) \otimes C_k^a$ holds, and*

$$A' = \left((C_h^a \circledcirc C_k^t) \otimes C_k^a \to C_h^t\right) \| A.$$

Observe that any de-absorption step results in the strict weakening of an ask constraint. In fact, we have $C_h^a \vdash (C_h^a \circledcirc C_k^t)$ by Q_1, and $C_h^a \vdash C_k^a$ by hypothesis, thus $C_h^a \Vdash (C_h^a \circledcirc C_k^t) \otimes C_k^a$.

Lemma 54 *If an agent A' is obtained by a de-absorption step from A, then $[\![A']\!] = [\![A]\!]$*

PROOF. In the hypotheses of Definition 53, let $D_h^a \stackrel{\text{def}}{=} (C_h^a \circledcirc C_k^t) \otimes C_k^a$. We will prove that semantics is *locally* preserved, namely

$$[\![C_h^a \to C_h^t \| C_k^a \to C_k^t]\!] = [\![D_h^a \to C_h^t \| C_k^a \to C_k^t]\!].$$

From the hypotheses we have $C_h^t \Vdash C_h^a \vdash C_k^a$ and $C_h^t \Vdash D_h^a \vdash C_k^a$. We can thus derive the following facts:

- since $C_h^t \Vdash C_k^a$ we have $\downarrow C_h^t \subset \downarrow C_k^a$ and $\downarrow C_h^t \cap \overline{\downarrow C_k^a} = \varnothing$;
- since $C_h^a \vdash C_k^a$ we have $\overline{\downarrow C_k^a} \subseteq \overline{\downarrow C_h^a}$ and $\overline{\downarrow C_h^a} \cap \overline{\downarrow C_k^a} = \overline{\downarrow C_k^a}$;
- similarly, from $D_h^a \vdash C_k^a$ we have $\overline{\downarrow D_h^a} \cap \overline{\downarrow C_k^a} = \overline{\downarrow C_k^a}$;
- since $C_h^t \Vdash C_h^a$ we have $\downarrow C_h^t \subset \downarrow C_h^a$ and $\downarrow C_h^t \cap \overline{\downarrow C_h^a} = \varnothing$;
- similarly, from $C_h^t \Vdash D_h^a$ we have $\downarrow C_h^t \cap \overline{\downarrow D_h^a} = \varnothing$;
- since $C_k^t \Vdash C_k^a$ we have $\downarrow C_k^t \subset \downarrow C_k^a$ and $\downarrow C_k^t \cap \overline{\downarrow C_k^a} = \varnothing$.

These allows us to state that

$$\begin{aligned}
[\![C_h^a \to C_h^t \parallel C_k^a \to C_k^t]\!] &= \left(\overline{\downarrow C_h^a} \cup \downarrow C_h^t\right) \cap \left(\overline{\downarrow C_k^a} \cup \downarrow C_k^t\right) \\
&= \left(\overline{\downarrow C_h^a} \cap \overline{\downarrow C_k^a}\right) \cup \left(\overline{\downarrow C_h^a} \cap \downarrow C_k^t\right) \cup \\
&\qquad \left(\downarrow C_h^t \cap \overline{\downarrow C_k^a}\right) \cup \left(\downarrow C_h^t \cap \downarrow C_k^t\right) \\
&= \overline{\downarrow C_k^a} \cup \left(\overline{\downarrow C_h^a} \cap \downarrow C_k^t\right) \cup \left(\downarrow C_h^t \cap \downarrow C_k^t\right) \\
&= \overline{\downarrow C_k^a} \uplus \left(\overline{\downarrow C_h^a} \cap \downarrow C_k^t\right) \uplus \left(\downarrow C_h^t \cap \downarrow C_k^t\right),
\end{aligned}$$

and, by the same reasoning,

$$[\![D_h^a \to C_h^t \parallel C_k^a \to C_k^t]\!] = \overline{\downarrow C_k^a} \uplus \left(\overline{\downarrow D_h^a} \cap \downarrow C_k^t\right) \uplus \left(\downarrow C_h^t \cap \downarrow C_k^t\right),$$

where $\uplus$ denotes disjoint union. Since $C_h^a \Vdash D_h^a$ implies

$$\left(\overline{\downarrow C_h^a} \cap \downarrow C_k^t\right) \supseteq \left(\overline{\downarrow D_h^a} \cap \downarrow C_k^t\right),$$

what we are left to show is that

$$\left(\overline{\downarrow C_h^a} \cap \downarrow C_k^t\right) \subseteq \left(\overline{\downarrow D_h^a} \cap \downarrow C_k^t\right),$$

that is to say $\forall C \in \mathcal{D} : (C \vdash C_k^t \wedge C \nvdash C_h^a) \implies C \nvdash D_h^a$. Now Lemma 52 comes in handy, as from $C \vdash C_k^t$ and $C \nvdash C_h^a$ we can derive $C \nvdash (C_h^a \circledcirc C_k^t)$ and thus $C \nvdash (C_h^a \circledcirc C_k^t) \otimes C_k^a = D_h^a$. □

We now define the promised class of procedures.

Definition 55 (De-absorption procedure.) *A* de-absorption procedure *is any algorithm transforming a finite* cc *agents in syntactic normal form which can be characterized as follows:*

phase 1. *transform the input agent A into A' by performing any number of de-absorption steps;*

phase 2. *transform A' into the output agent A'' by applying the rewriting system of* Figure 2 restricted to the structural and reduction rules.

A de-absorption procedure will be called maximal *if it applies all the possible de-absorption steps.*

Theorem 56 *Any de-absorption procedure is semantics-preserving.*

PROOF. Immediate from Lemma 54 and Lemma 40. □

In all those cases where we have a de-absorption procedure which is a function over $|\mathcal{A}(\bar{\mathcal{D}})|$ we have an obvious way to define a merge operator.

Definition 57 (Merge operator with de-absorption.) *Let $\bar{\mathcal{D}}$ be a constraint system, and let $\delta_{\circledcirc} : |\mathcal{A}(\bar{\mathcal{D}})| \to \mathcal{A}(\bar{\mathcal{D}})$ be a de-absorption procedure. The* merge operator based on $\delta_{\circledcirc}$ *is given, for each $A_1, A_2 \in |\mathcal{A}(\bar{\mathcal{D}})|$, by*

$$A_1 \mathbin{\dot{\oplus}_{\mathrm{A}}} A_2 \stackrel{\text{def}}{=} \rho_{\mathrm{A}}\Big(\delta_{\circledcirc}(A_1) \mathbin{\tilde{\oplus}_{\mathrm{A}}} \delta_{\circledcirc}(A_2)\Big).$$

Any such operator, by virtue of Theorem 56 and Proposition 47, is clearly a merge operator in the sense of Definition 7. De-absorption procedures which are not functions are still useful for designing widening operators.

We now quickly show some examples of ask-and-tell constraint systems. For the more exciting things we have to wait until the next section, where combination of constraint domains are introduced.

7.2 More bounds and relations analysis for numeric domains

Ask-and-tell constraint system are suitable for modeling approximate inference techniques which are very useful in a practical setting. Following Section 4.4, there is another technique which is used for the analysis described in [5,6,4]: *relational arithmetic* [50]. This technique allows to infer constraints on the qualitative relationship of an expression to its arguments. Consider the simple constraint system of Section 4.4, and apply to it the determinate construction of Section 5. Now apply the ask-and-tell construction to the result. Relational arithmetic can be described by a number of (concurrent) agents. Here are some of them, where x and y are arithmetic expressions, and $\bowtie$ ranges in $\mathsf{R} \stackrel{\text{def}}{=} \{=, \neq, \leq <, \geq, >\}$:

$$\begin{aligned}
\mathrm{ask}(x \bowtie 0) &\to \mathrm{tell}\Big((x + y) \bowtie y\Big) \\
\mathrm{ask}(x > 0 \wedge y > 0 \wedge x \bowtie 1) &\to \mathrm{tell}\Big((x * y) \bowtie y\Big) \\
\mathrm{ask}(x > 0 \wedge y < 0 \wedge x \bowtie 1) &\to \mathrm{tell}\Big(y \bowtie (x * y)\Big) \\
\mathrm{ask}(x > 0 \wedge y < 0 \wedge x \bowtie -y) &\to \mathrm{tell}\Big(-1 \bowtie (x/y)\Big) \\
\mathrm{ask}(x \bowtie y) &\to \mathrm{tell}(e^x \bowtie e^y)
\end{aligned}$$

An example of inference is deducing $X + 1 \leq Y + 2X + 1$ from $X \geq 0 \wedge Y \geq 0$. Notice that there is no restriction to linear constraints.

7.3 Definiteness analysis: Def

The prototypical example of data-flow analysis taking advantage of dependency information is definiteness (or groundness) analysis. In our setting a domain for definiteness can be obtained as follows. Take the *atomic* s.c.s. of Section 4.1. Apply to it the determinate construction as outlined in Section 5.1. Now apply the ask-and-tell construction to the result, with the merge operator obtained along the lines of Definition 57 choosing:

(i) set-theoretic difference as weakening operator;
(ii) the maximal de-absorption procedure (i.e. the one which applies all the possible de-absorption steps).

The definition is complete by defining the diagonals (here only in the monadic case, for simplicity) as $d^{\mathrm{A}}_{XY} \stackrel{\mathrm{def}}{=} \{X\} \to \{X,Y\} \parallel \{Y\} \to \{X,Y\}$. It can be shown that the domain so obtained is *Def* [19,3]. Its elements can keep track of non-trivial dependencies like the ones induced by symbolic and numeric constraints. For example, the dependencies of $A = f(B,C)$ and $A+B+C=0$ are captured, respectively, by the agents

$$\{A\} \to \{B,C\} \parallel \{B,C\} \to \{A\},$$

and

$$\{A,B\} \to \{C\} \parallel \{A,C\} \to \{B\} \parallel \{B,C\} \to \{A\}.$$

This example gives us the possibility of pointing out that the entire business of weakenings and de-absorption procedures is not something we can easily avoid. When using definite sentences to represent dependencies, as in our case and in the representations for *Def* studied in [3], obtaining a maximal weakening of the antecedents is crucial for obtaining precise merge operators, let alone for computing the join when it exists. Our present requirement of employing maximal de-absorption corresponds to the requirement, in the representations studied in [3], of the sentences being in *orthogonal* form (which has its costs, since orthogonality must be obtained and preserved by all the domain's operations). In [3] it is also presented a merge operator, for the representation RCNF_{Def}, intended to trade precision for efficiency. It does that by not insisting on orthogonality, which in our setting corresponds to the use of a partial de-absorption procedure.

7.4 Definiteness analysis: more than Pos

Pos is (like *Def*) a domain of boolean functions [11,3]. It consists precisely of those functions assuming the true value under the *everything-is-true* as-

signment. In [3] it is shown that *Pos* is strictly more precise than *Def* for groundness analysis. If we apply the powerset construction of Section 6 to the ask-and-tell c.s. of the previous section we obtain a very precise (and complex) domain for simple dependencies. In [26] it is referred to as $\mathcal{U}(Def)$ (where $\mathcal{U}$ denotes disjunctive completion) and is shown to be equivalent to $\mathcal{U}(Pos)$. On the other hand, in [22] it has been shown that $\mathcal{U}(Pos)$ is strictly more precise than *Pos*, even though this extra-precision is not needed for definiteness analysis.

8 Combination of domains

It is well known that different data-flow analyses can be combined together. In the framework of abstract interpretation this can be achieved by means of standard constructions such as reduced product and down-set completion [14,15]. The key point is that the combined analysis can be more precise than each of the component ones for they can mutually improve each other. However, the degree of cross-fertilization is highly dependent on the degree and quality of interaction taking place among the component domains.

We now propose a general methodology for domain combination with asynchronous interaction. The interaction among domains is asynchronous in that it can occur at any time, or, in other words, it is not synchronized with the domain's operations.

This is achieved by considering ask-and-tell constraint systems built over *product* constraint systems. These constraint systems allow to express communication among domains in a very simple way. They also inherit all the semantic elegance of concurrent constraint programming languages, which provide the basis for their construction. Recently, a methodology for the combination of abstract domains has been proposed in [12], which is directly based onto low-level actions such as *tests* and *queries*. While the approach in [12] is immediately applicable to a wider range of analyses (including the ones dealing with non-monotonic properties) the approach we follow here for our restricted set of analyses has the merit of being much more elegant.

We start with a finite set of constraint systems each expressing some properties of interest, and we wish to combine them so to:

(i) perform all the analyses at the same time; and
(ii) have the domains cooperate to the intent of mutually improving each other.

The first goal is achieved by considering the product of the given constraint

systems.

8.1 Product constraint systems

The product construction over constraint systems is absolutely standard.

Definition 58 (Direct product of constraint systems.) *Given a finite family of constraint systems*

$$\bar{\mathcal{D}}_i = \langle \mathcal{D}_i, \otimes_i, \oplus_i, \mathbf{0}_i, \mathbf{1}_i, \{\bar{\exists}^i_{\vec{\Lambda}}\}, \{d^i_{\vec{X}\vec{Y}}\}\rangle, \quad \textit{for } i = 1, \ldots, n,$$

the product constraint system of $\bar{\mathcal{D}}_1, \ldots, \bar{\mathcal{D}}_n$ *is the algebraic direct product of* $\bar{\mathcal{D}}_1, \ldots, \bar{\mathcal{D}}_n$*, and is denoted by*

$$\prod_{i=1}^{n} \bar{\mathcal{D}}_i = \langle \mathcal{D}_\times, \otimes_\times, \oplus_\times, \mathbf{0}_\times, \mathbf{1}_\times, \{\bar{\exists}^\times_{\vec{\Lambda}}\}, \{d^\times_{\vec{X}\vec{Y}}\}\rangle.$$

Thus all the operations of a product c.s. are defined coordinate-wise and, in particular, we have

$$\langle C'_1, \ldots, C'_n\rangle \vdash_\times \langle C''_1, \ldots, C''_n\rangle \quad \Longleftrightarrow \quad \forall i = 1, \ldots, n : C'_i \vdash C''_i.$$

An alternative way of obtaining a product constraint system is to start from a collection of simple constraint systems and then applying the determinate construction.

Definition 59 (Product of simple constraint systems.) *Given a finite family of simple constraint systems* $\mathcal{S}_i = \langle \mathcal{C}_i, \vdash_i, \bot_i, \top_i\rangle$ *for* $i = 1, \ldots, n$*, the* product *of the family is the structure given by*

$$\prod_{i=1}^{n} \mathcal{S}_i \stackrel{\text{def}}{=} \langle \mathcal{C}_\times, \vdash_\times, \bot_\times, \top_\times\rangle,$$

where the product tokens are

$$\begin{aligned}
\mathcal{C}_\times \stackrel{\text{def}}{=} & \left\{ (c_1, \top_2, \ldots, \top_n) \;\middle|\; c_1 \in \mathcal{C}_1 \right\} \\
& \cup \left\{ (\top_1, c_2, \top_3, \ldots, \top_n) \;\middle|\; c_2 \in \mathcal{C}_2 \right\} \\
& \vdots \\
& \cup \left\{ (\top_1, \ldots, \top_{n-1}, c_n) \;\middle|\; c_n \in \mathcal{C}_n \right\} \\
& \cup \{\bot_\times\}.
\end{aligned}$$

The product entailment is defined as the least relation satisfying conditions E_1–E_5 *of* Definition 23 *and the following ones, for each* $C \in \wp_f(\mathcal{C}_\times)$*:*

$$\begin{array}{ccc} \pi_1(C) \vdash_1 c_1 & \Longrightarrow & C \vdash_\times (c_1, \top_2, \ldots, \top_n) \\ \vdots & \vdots & \vdots \\ \pi_n(C) \vdash_n c_n & \Longrightarrow & C \vdash_\times (\top_1, \ldots, \top_{n-1}, c_n). \end{array}$$

Finally, $\bot_\times \stackrel{\text{def}}{=} (\bot_1, \ldots, \bot_n)$ *and* $\top_\times \stackrel{\text{def}}{=} (\top_1, \ldots, \top_n)$.

Taking the product of constraint systems, we have realized the simplest form of domain combination. It corresponds to the direct product construction of [14], allowing for different analyses to be carried out at the same time. Notice that there is no communication at all among the domains.

However, as soon as we consider the ask-and-tell constraint system built over the product, we can express asynchronous communication among the domains in complete freedom. At the very least we would like to have the *smash product* among the component domains. This is realized by the agent

$$\|_{i=1}^{n} \mathbf{0}_i \to \mathbf{0}_\times. \tag{23}$$

To say it operationally, the *smash* agent globalizes the (local) failure on any of the component domains. This is the only domain-independent agent we have.

Things become much more interesting when instantiated over particular constraint domains. In the CLP($\mathcal{R}$) system [31] non-linear constraints (like $X = Y * Z$) are delayed (i.e. not treated by the constraint solver) until they become linear (e.g. until either Y or Z are constrained to take a single value). In standard semantic treatments this is modeled in the operational semantics by carrying over, besides the sequence of goals yet to be solved, a set of delayed constraints. Constraints are taken out from this set (and incorporated into the constraint store) as soon as they become linear.

We believe that this can be viewed in an alternative way which is more elegant, as it easily allows for taking into account the delay mechanism also in the bottom-up semantics, and makes sense from an implementation point of view. The basic claim is the following: CLP($\mathcal{R}$) has *three* computation domains: Herbrand, $\mathbb{R}$ (well, an approximation of it), and *definiteness*.

In other words, it also manipulates, besides the usual ones, constraints of the kind $ground^\natural(X)$ which is interpreted as the variable X being definitively bound to a unique value. We can express the semantics of CLP($\mathcal{R}$) (at a certain level of abstraction) with delay of non-linear constraints by considering the ask-and-tell constraint system over the product of the above three domains. In this

view, a constraint of the form $X = Y * Z$ in a program actually corresponds to the agent

$$\mathrm{ask}\Big(\mathit{ground}^\natural(Y); \mathit{ground}^\natural(Z)\Big) \rightarrow \mathrm{tell}(X = Y * Z).$$

In fact, any CLP($\mathcal{R}$) user *must* know that $X = Y * Z$ is just a shorthand for that agent! (A similar treatment could probably be done for logic programs with delay declarations.)

Obviously, this cannot be forgotten in abstract constraint systems intended to formalize correct data-flow analyses of CLP($\mathcal{R}$). Referring back to sections 4.4 and 7.2, when the abstract constraint system extracts information from non-linear constraints, for example with the agent

$$A = \mathrm{ask}(Y > 0 \wedge Z > 0 \wedge Y \bowtie 1) \rightarrow \mathrm{tell}\Big((Y * Z) \bowtie Z\Big)$$

of relational arithmetic, you cannot simply let $X = Y * Z$ stand by itself. By doing this you would incur the risk of *overshooting* the concrete constraint system (thus loosing soundness), which is unable to deduce anything from non-linear constraints. The right thing to do is to combine the numeric abstract constraint system with one for definiteness (by the product and the ask-and-tell constructions) and using, instead of A, the agent

$$A' = \mathrm{ask}\Big(\mathit{ground}^\sharp(Y); \mathit{ground}^\sharp(Z)\Big) \rightarrow A.$$

Beware not to confuse $\mathit{ground}^\natural(X)$ with $\mathit{ground}^\sharp(X)$. The first is the *concrete one*: X is definite if and only if $\mathit{ground}^\natural(X)$ is entailed in the current concrete store. In contrast, having $\mathit{ground}^\sharp(X)$ entailed in the *abstract* constraint store at some program point, and assuming a correct definiteness analysis, means that X is certainly bound to a unique value in the concrete computation at that program point. The vice-versa, of course, does not necessarily hold.

Let us see another example. The analysis described in [28] aims at the compile-time detection of those non-linear constraints that will become linear at run time. This analysis is important for remedying the limitation of CLP($\mathcal{R}$) to linear constraints by incorporating powerful (and computationally complex) methods from computer algebra as the ones employed in RISC-CLP(Real) [29]. With the results of the above analysis this extension can be done in a smooth way: non-linear constraints which are guaranteed to become linear will be simply delayed, while only the other non-linear constraints will be treated with the special solving techniques. Thus, programs not requiring the extra power of these techniques will be hopefully recognized as such, and will not pay any penalties. The analysis of [28] is a kind of definiteness. One of its difficulties shows up when considering the simplest non-linear constraint: $X = Y * Z$. Clearly X is definite if Y and Z are such. But we cannot conclude that the definiteness of Y follows from the one of X and Z, as we need also

the condition $Z \neq 0$. Similarly, we would like to conclude that X is definite if Y or Z have a zero value. Thus we need approximations of the concrete values of variables (i.e. bounds analysis), something which is not captured by common definiteness analyses while being crucial when dealing with non-linear constraints. If we take the ask-and-tell construction over the product of a constraint system for definiteness with a numerical one we can solve the problem. $X = Y * Z$ would be *abstractly compiled* into the agent

$$\begin{aligned}
&\mathrm{ask}\Big(ground^\sharp(Y) \wedge ground^\sharp(Z)\Big) \rightarrow \mathrm{tell}\Big(ground^\sharp(X)\Big) \\
\| &\,\mathrm{ask}(Y = 0; Z = 0) \rightarrow \mathrm{tell}\Big(ground^\sharp(X)\Big) \\
\| &\,\mathrm{ask}\Big(ground^\sharp(X) \wedge ground^\sharp(Z) \wedge Z \neq 0\Big) \rightarrow \mathrm{tell}\Big(ground^\sharp(Y)\Big) \\
\| &\,\mathrm{ask}\Big(ground^\sharp(X) \wedge ground^\sharp(Y) \wedge Y \neq 0\Big) \rightarrow \mathrm{tell}\Big(ground^\sharp(Z)\Big).
\end{aligned}$$

Of course, this is much more precise than the *Def* formula $X \leftarrow Y \wedge Z$.

We have thus reconciled the two running examples of this paper (numerical bounds/relations and definiteness) by showing two examples of combination. In fact, when analyzing CLP($\mathcal{R}$) programs there is a bidirectional flow of information: definiteness information is required for a correct handling of delayed constraints and thus for deriving more precise numerical patterns which, in turn, are used to provide more precise definiteness information. There is another obvious way in which numerical bounds and relations improve definiteness (and any other analysis, indeed): by excluding computation paths which are doomed to fail (this is modeled in a domain-independent way by the *smash agent* seen above). It is thus evident that we are requiring a quite complicated interaction between domains. It is even more complicated if you consider that the numerical component we have sketched is the combination (in the sense of the present section) of a domain for intervals with one for arithmetic relationships (even though, for simplicity, it was not presented in that way).

8.2 Approximating built-ins behavior with reactive combinations

The techniques we propose are suitable for approximating the behavior of several common built-ins. Consider, for instance, the `functor/3` built-in. Consider a product constraint system with four components: one for *simple types* (for instance, the one of Section 4.2), one for definiteness, one incorporating numerical information (including at least signs, e.g. tokens of the kind $X \geq 0$, $X > 0$ and $X = 0$), and one involving symbolic, structural information (e.g., the one of Section 5.2). Then, the (success) semantics of `functor(T, F, N)` can be approximated easily and quite precisely by means of the following finite

agent over the product:

$$\begin{aligned}
&\mathrm{tell}\Big(symbolic(T), atom(F), ground(F), integer(N), N \geq 0, ground(N)\Big) \,\|\\
&\mathrm{ask}\Big(atom(T); N = 0; T = F\Big) \rightarrow\\
&\qquad \mathrm{tell}\Big(atom(T), ground^{\sharp}(T), N = 0, T = F\Big) \,\|\\
&\mathrm{ask}\Big(compound(T); N > 0; T \neq F\Big) \rightarrow\\
&\qquad \mathrm{tell}\Big(compound(T), N > 0, T \neq F\Big).
\end{aligned}$$

9 Conclusion and future work

We have shown a notion of constraint system which is general enough to encompass both the concrete domains of computation of actual constraint logic-based languages, and several of their abstract interpretations useful for data-flow analysis. We have also shown how these constraint systems are integrated within an appropriate framework for the definition of non-standard semantics of constraint logic-based languages. Some significant members of the introduced class of constraint systems have been presented, together with construction techniques which induce a hierarchy of domains. These domains have several nice features, both from a theoretical and an experimental viewpoint. In particular, we have proposed a general methodology for domain combination with asynchronous interaction. In this kind of combinations the communication among domains can be expressed in a very simple way. The methodology also inherits all the semantic elegance of concurrent constraint programming languages, which provide the basis on which it is built.

Ask-and-tell constraint systems have been satisfactorily implemented in the China analyzer [4]. Of course, since we strive (but not too much) for efficient analyzers, we have not implemented them *exactly* as described here. We have, however, a firm theoretical basis on which to base our implementation tricks. We have also implemented domain combinations along the lines of Section 8. In China, following an abstract compilation approach, CLP($\mathcal{R}$) constraints are compiled into finite cc agents over a product of domains for simple types, definiteness, numerical bounds and relations, and generic patterns. The experimental results obtained with the prototype implementation represent a strong encouragement to proceed along these lines.

Future work includes studying in depth the problem of the semantic normal form for finite cc agents, both in general and in particular cases. The aim is to find more satisfactory solutions to the problem of merging finite cc agents. We also would like to answer the following question: are there variations of

these ideas which are applicable also to analysis oriented towards "non-logical" properties?

Acknowledgement

I wish to thank Maurizio Gabbrielli, Roberto Giacobazzi, Giorgio Levi, Catiuscia Palamidessi, Francesca Rossi, Vijay Saraswat, and Enea Zaffanella for the discussions we had on the subject and for reading draft versions of this paper. Enea was especially kind in helping me with some technical issues. Special thanks to Giorgio for his extensive support.

References

[1] H. Aït-Kaci. *Warren's Abstract Machine. A Tutorial Reconstruction.* The MIT Press, Cambridge, Mass., 1991.

[2] J. F. Allen. Maintaining knowledge about temporal intervals. *Communications of the ACM*, 26(11):832–843, 1983.

[3] T. Armstrong, K. Marriott, P. Schachte, and H. Sondergaard. Two classes of boolean functions for dependency analysis. Technical Report 94/211, Dept. Computer Science, Monash University, Melbourne, 1994.

[4] R. Bagnara. On the detection of implicit and redundant numeric constraints in CLP programs. In M. Alpuente, R. Barbuti, and I. Ramos, editors, *Proceedings of the "1994 Joint Conference on Declarative Programming (GULP-PRODE '94)"*, pages 312–326, Peñíscola, Spain, September 1994.

[5] R. Bagnara, R. Giacobazzi, and G. Levi. Static analysis of CLP programs over numeric domains. In M. Billaud, P. Castéran, MM. Corsini, K. Musumbu, and A. Rauzy, editors, *Actes "Workshop on Static Analysis '92"*, volume 81–82 of *Bigre*, pages 43–50, Bordeaux, September 1992. Extended abstract.

[6] R. Bagnara, R. Giacobazzi, and G. Levi. An application of constraint propagation to data-flow analysis. In *Proceedings of "The Ninth Conference on Artificial Intelligence for Applications"*, pages 270–276, Orlando, Florida, March 1993. IEEE Computer Society Press, Los Alamitos, CA.

[7] R. Barbuti and A. Martelli. A Structured Approach to Semantics Correctness. *Science of Computer Programming*, 3:279–311, 1983.

[8] S. Burris and H. P. Sankappanavar. *A Course in Universal Algebra.* Springer-Verlag, Berlin, 1981.

[9] Michael Codish and Bart Demoen. Analysing logic programs using "Prop"-ositional logic programs and a magic wand. In Dale Miller, editor, *Logic Programming - Proceedings of the 1993 International Symposium*, pages 114–129, Vancouver, Canada, 1993. The MIT Press.

[10] P. Codognet and G. Filè. Computations, Abstractions and Constraints. In *Proc. Fourth IEEE Int'l Conference on Computer Languages*. IEEE Press, 1992.

[11] A. Cortesi, G. Filè, and W. Winsborough. *Prop* revisited: Propositional Formula as Abstract Domain for Groundness Analysis. In *Proc. Sixth IEEE Symp. on Logic In Computer Science*, pages 322–327. IEEE Computer Society Press, 1991.

[12] A. Cortesi, B. Le Charlier, and P. Van Hentenryck. Combinations of abstract domains for logic programming. In *Conference Record of POPL '94: 21st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 227–239, Portland, Oregon, January 1994.

[13] P. Cousot and R. Cousot. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. In *Proc. Fourth ACM Symp. Principles of Programming Languages*, pages 238–252, 1977.

[14] P. Cousot and R. Cousot. Systematic Design of Program Analysis Frameworks. In *Proc. Sixth ACM Symp. Principles of Programming Languages*, pages 269–282, 1979.

[15] P. Cousot and R. Cousot. Abstract Interpretation and Applications to Logic Programs. *Journal of Logic Programming*, 13(2 & 3):103–179, 1992.

[16] P. Cousot and R. Cousot. Abstract Interpretation Frameworks. *Journal of Logic and Computation*, 2(4):511–549, 1992.

[17] P. Cousot and R. Cousot. Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation. In M. Bruynooghe and M. Wirsing, editors, *Proc. of PLILP'92*, volume 631 of *Lecture Notes in Computer Science*, pages 269–295. Springer-Verlag, Berlin, 1992.

[18] P. Cousot and R. Cousot. Compositional and inductive semantic definitions in fixpoint, equational, constraint, closure-condition, rule-based and game theoretic form. In P. Wolper, editor, *Proceedings of the 7th International Conference on Computer-Aided Verification (CAV '95)*, volume 939 of *Lecture Notes in Computer Science*, pages 293–308. Springer-Verlag, Berlin, 1995. Invited paper.

[19] P. Dart. On Derived Dependencies and Connected Databases. *Journal of Logic Programming*, 11(2):163–188, 1991.

[20] E. Davis. Constraint propagation with interval labels. *Artificial Intelligence*, 32:281–331, 1987.

[21] S. Debray and R. Ramakrishnan. Abstract interpretation of logic programs using magic transformations. *The Journal of Logic Programming*, 18(2):149–176, February 1994.

[22] G. Filé and F. Ranzato. Improving abstract interpretations by systematic lifting to the powerset. In M. Bruynooghe, editor, *Proceedings of the 1994 International Logic Programming Symposium (ILPS '94)*, pages 655–669. The MIT Press, 1994.

[23] E. C. Freuder. Synthesizing constraint expressions. *Communications of the ACM*, 21(11):958–966, 1978.

[24] R. Giacobazzi, S.K. Debray, and G. Levi. Generalized Semantics and Abstract Interpretation for Constraint Logic Programs. *Journal of Logic Programming*, 25(3):191–247, 1995.

[25] R. Giacobazzi, C. Palamidessi, and F. Ranzato. Weak relative pseudo-complements of closure operators. Technical Report LIX/RR/95/04, Laboratoire d'Informatique, École Polytechnique, Paris, 1995. Available on WWW at URL `http://www.di.unipi.it/~giaco`.

[26] R. Giacobazzi and F. Ranzato. Compositional optimization od disjunctive abstract interpretations. In M. Gabbrielli, editor, *Informal Proceedings of the 4th Compulog-network subgroup meeting on Programming Languages*, 1995.

[27] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove, and D. S. Scott. *A Compendium of Continuous Lattices*. Springer-Verlag, Berlin, 1980.

[28] Michael Hanus. Analysis of nonlinear constraints in CLP($\mathcal{R}$). In David S. Warren, editor, *Proceedings of the Tenth International Conference on Logic Progra mming*, pages 83–99, Budapest, Hungary, 1993. The MIT Press.

[29] Hoon Hong. RISC-CLP(Real): Logic programming with non-linear constraints over the reals. In F. Benhamou and A. Colmerauer, editors, *Constraint Logic Programming: Selected Research*. The MIT Press, Cambridge, Mass., 1993.

[30] J. Jaffar and J.-L. Lassez. Constraint Logic Programming. In *Proc. Fourteenth Annual ACM Symp. on Principles of Programming Languages*, pages 111–119. ACM, 1987.

[31] J. Jaffar, S. Michaylov, P. Stuckey, and R. Yap. The CLP($\mathcal{R}$) Language and System. *ACM Transactions on Programming Languages and Systems*, 14(3):339–395, 1992.

[32] Joxan Jaffar and Michael J. Maher. Constraint logic programming: A survey. *The Journal of Logic Programming*, 19 & 20:503–582, May 1994.

[33] G. Janssens, M. Bruynooghe, and V. Englebert. Abstracting numerical values in CLP(H, N). In M. Hermenegildo and J. Penjam, editors, *Proc. Sixth Int'l Symp. on Programming Language Implementation and Logic Programming*, volume 844 of *Lecture Notes in Computer Science*, pages 400–414. Springer-Verlag, Berlin, 1994.

[34] N. D. Jones and H. Søndergaard. A Semantics-based Framework for the Abstract Interpretation of Prolog. In S. Abramsky and C. Hankin, editors, *Abstract Interpretation of Declarative Languages*, pages 123–142. Ellis Horwood Ltd, 1987.

[35] J.-L. Lassez, M. J. Maher, and K. Marriott. Unification Revisited. In J. Minker, editor, *Foundations of Deductive Databases and Logic Programming*, pages 587–625. Morgan Kaufmann, Los Altos, Ca., 1988.

[36] B. Le Charlier and P. Van Hentenryck. Experimental Evaluation of a Generic Abstract Interpretation Algorithm for Prolog. In *Proc. Fourth IEEE Int'l Conference on Computer Languages*, pages 137–146. IEEE Press, 1992.

[37] G. Levi and D. Micciancio. Analysis of pure PROLOG programs. In M. Alpuente and M. I. Sessa, editors, *Proceedings of the "1995 Joint Conference on Declarative Programming (GULP-PRODE '95)"*, pages 521–532, Marina di Vietri, Italy, September 1995.

[38] A. K. Mackworth. Consistency in networks of relations. *Artificial Intelligence*, 8:99–118, 1977.

[39] K. Marriott and H. Søndergaard. On Describing Success Patterns of Logic Programs. Technical Report 12, The University of Melbourne, 1988.

[40] C. Mellish. Some Global Optimizations for a Prolog Compiler. *Journal of Logic Programming*, 2:43–66, 1985.

[41] U. Montanari. Networks of constraints: Fundamental properties and applications to picture processing. *Inform. Sci.*, 7:95–132, 1974.

[42] K. Musumbu. *Interprétation Abstraite des Programmes Prolog.* PhD thesis, Facultés Universitaires Notre-Dame de la Paix – Namur Institut d'Informatique, Belgium, September 1990.

[43] V. A. Saraswat. The category of constraint systems is cartesian-closed. In *Proc. 7th IEEE Symp. on Logic in Computer Science*, Santa Cruz, 1992.

[44] V. A. Saraswat. *Concurrent Constraint Programming.* MIT Press Cambridge, Mass., 1993.

[45] V. A. Saraswat, M. Rinard, and P. Panangaden. Semantic Foundation of Concurrent Constraint Programming. In *Proc. Eighteenth Annual ACM Symp. on Principles of Programming Languages*, pages 333–353. ACM, 1991.

[46] T. Sato and H. Tamaki. Enumeration of Success Patterns in Logic Programs. *Theoretical Computer Science*, 34:227–240, 1984.

[47] D. Scott. Domains for Denotational Semantics. In M. Nielsen and E. M. Schmidt, editors, *Proc. ninth Int. Coll. on Automata, Languages and Programming*, volume 140 of *Lecture Notes in Computer Science*, pages 577–613. Springer-Verlag, Berlin, 1982.

[48] M. C. Scudellari. Analisi bottom-up di programmi logici con vincoli basata su trasformazioni *magic-set.* M.Sc. dissertation, R. Bagnara and G. Levi supervisors, University of Pisa, April 1996. In Italian, available on WWW at URL `http://www.di.unipi.it/~bagnara`.

[49] R. Simmons. Representing and reasoning about change in geologic interpretation. Technical Report 749, MIT AI Laboratory, 1983.

[50] R. Simmons. Commonsense arithmetic reasoning. In *Proc. AAAI-86*, pages 118–124, 1986.

[51] P. Van Hentenryck, V. Saraswat, and Y. Deville. Constraint logic programming over finite domains: the design, implementation, and applications of `cc(fd)`. Technical report, Brown University, Providence, RI, 1992.