Algorithmic Debugging of Wrong Answers in Constraint Functional-Logic Programming

Rafael Caballero Roldán, Mario Rodríguez Artalejo, and Rafael del Vado Vírseda

TECHNICAL REPORT SIP - 03/2006
Dep. Lenguajes, Sistemas Informáticos y Programación
Univ. Complutense de Madrid

Dpto. de Sistemas Informáticos y Programación,
Universidad Complutense de Madrid
{rafa,mario,rdelvado}@sip.ucm.es

Abstract. We present a declarative method for diagnosing wrong computed answers in $CFLP(D)$, a newly proposed generic scheme for lazy Constraint Functional Logic Programming which can be instantiated by any constraint domain $D$ given as parameter, and supports a powerful combination of functional and constraint logic programming over $D$. Our approach extends and combines declarative debugging techniques previously developed for less expressive programming paradigms, namely the $CLP(D)$ scheme and lazy functional logic languages. Debugging starts with the observation of a wrong computed answer which the user regards as incorrect w.r.t. an intended model that provides a declarative description of the program’s semantics. Debugging proceeds by exploring an abridged proof tree that provides a purely declarative view of the computation, so that the user does not need to understand the complex underlying operational mechanisms. Debugging ends with the detection of a function rule in the program that is incorrect w.r.t. the intended model. We prove the logical correctness of the debugging method for any sound $CFLP(D)$-system whose computed answers are logical consequences of the program, and we describe a practical tool which implements the debugging method for the domain of arithmetic constraints over the real numbers.

1 Introduction

Debugging tools are a practical need for diagnosing the causes of erroneous computations. Declarative programming paradigms involving complex operational details, such as constraint solving and lazy evaluation, do not fit well to traditional debugging techniques relying on the inspection of low-level computation traces. As a solution to this problem, declarative diagnosis uses Computation Trees (shortly, CTs) in place of traces. CTs are built a posteriori to represent...
the structure of a computation whose top level outcome is regarded as an \textit{error symptom} by the user. Each node in a CT represents the computation of some observable result, depending on the results of its children nodes. Declarative diagnosis explores a CT looking for a so-called \textit{buggy node} which computes an incorrect result from children whose results are correct; such a node must point to an incorrect program fragment. The search for a buggy node can be implemented with the help of an external \textit{oracle} (usually the user with some semiautomatic support) who has a reliable declarative knowledge of the expected program semantics, the so-called \textit{intended interpretation}.

The generic description of declarative diagnosis in the previous paragraph follows [14]. Declarative diagnosis was first proposed in the field of logic programming [17, 8], and it has been successfully extended to other declarative programming paradigms, including lazy functional programming [15, 16], constraint logic programming [18, 9] and functional logic programming [4, 5]. In contrast to recent approaches to error diagnosis using \textit{abstract interpretation} (as e.g. [6, 11, 1] and some of the approaches described in [7]), declarative diagnosis often involves complex queries to the user. This problem has been tackled by means of various techniques, such as user-given partial specifications of the program’s semantics [2, 5], safe inference of information from answers previously given by the user [4], or CTS tailored to the needs of a particular debugging problem over a particular computation domain [9]. Current research in declarative diagnosis has still to face many challenges regarding both the foundations and the development of practical tools.

The aim of this report is to present a declarative method for diagnosing wrong computed answers in CFLP(D), a newly proposed generic programming scheme which can be instantiated by any constraint domain \(D\) given as parameter, and supports a powerful combination of functional and constraint logic programming over \(D\) [12]. Borrowing ideas from \textit{CFLP(D)} declarative semantics we obtain a suitable notion of intended interpretation, as well as a kind of abridged proof trees with a sound logical meaning to play the role of CTS. Our aim is to achieve a natural combination of previous approaches that were separately developed for the \textit{CLP(D)} scheme [18] and for lazy functional logic languages [4]. We give theoretical results showing that the proposed debugging method is logically correct for any sound \textit{CFLP(D)}-system whose computed answers are logical consequences of the program in the sense of \textit{CFLP(D)} semantics. We also present a practical debugger called \textit{DDT}, developed as an extension of previously existing but less powerful tools [3, 5]. \textit{DDT} implements the proposed diagnosis method for \textit{CFLP(R)}-programming in the \textit{TOY} system [13] using the domain \(R\) of arithmetic constraints over the real numbers.

The rest of the report is organized as follows: Section 2 motivates our approach by presenting a debugging example which is used as illustration along the rest of the report. Section 3 recalls the \textit{CFLP(D)} scheme from [12] to the extent needed for understanding the theoretical results in this report. Section 4 presents a correct method for the declarative diagnosis of wrong computed answers in any soundly implemented \textit{CFLP(D)}-system. Section 5 describes the
debugging tool \textit{DDT}. Section 6 concludes and points to some plans for future work.

The report includes only brief proof sketches for the main results. The final appendix includes the detailed proofs.

2 A Motivating Example

As a motivation for the rest of the report, we consider the following program fragment written in \textit{TOY} [13], a programming system which supports several instances of the \textit{CFLP}(D) scheme:

\textit{Example 1 (Building ladders in \textit{TOY}).}

\begin{verbatim}
infixr 40 &&
&& :: bool → bool → bool
false && Y = false
true && Y = Y

definitions
head :: [A] → A
head [X|Xs] = X

type point = (real,real)
type figure = point → bool

rect :: point → real → real → figure
rect (X,Y) LX LY (X',Y') = (X' ≥ X) && (X' ≤ X+LX) && (Y' ≤ Y) && (Y' ≤ Y+LY)
% This program rule is incorrect. It should be . . . (Y' ≥ Y) . . .

intersect :: figure → figure → figure
intersect F1 F2 P = F1 P && F2 P

ladder :: point → real → real → [figure]
ladder (X,Y) LX LY = [rect (X,Y) LX LY | ladder (X+LX, Y+LY) LX LY]
\end{verbatim}

Here, \textit{TOY} is used to implement the instance \textit{CFLP}(R) of the \textit{CFLP}(D) scheme, with the parameter D replaced by the real number domain R, which provides real numbers, arithmetic operations and various arithmetic constraints, including equalities, disequalities and inequalities. The type \textit{figure} is intended to represent geometric figures as boolean functions, the function \textit{rect} is intended to represent rectangles (more precisely, a rectangle \textit{rect (X,Y) LX LY} is intended to have two opposite vertices of coordinates (X,Y) and (X+LX,Y+LY), respectively); and the function \textit{ladder} is intended to build an infinite list of rectangles in the shape of a ladder. Although the text of the program seems to include no constraints, it uses arithmetic and comparison operators that give rise to constraint solving in execution time. More precisely, consider the following session in \textit{TOY}:

\begin{verbatim}
Toy> /run(examples/debug/ladder) % compile ladder.toy
Toy> /cflpr
Toy(R)> intersect (head (ladder (20,20) 50 20))
              (head (ladder (5,5) 30 40)) (X,Y) == R % goal
\end{verbatim}

Here, R → true \{ Y ≤ 5, X ≥ 2.0E+01, X ≤ 35 \} % computed answer
The goal asks for the membership of a generic point \((X,Y)\) to the intersection of the two rectangles \((\text{rect } (20,20) 50 20)\) and \((\text{rect } (5,5) 30 40)\), computed indirectly as the first steps of two particular ladders. The diagram included in Example 1 shows these two rectangles as well as the rectangle corresponding to their intersection (highlighted in black). The \textit{TOY} system has solved the goal by a combination of lazy narrowing and constraint solving; the computed answer consists of the substitution \(R \rightarrow \text{true}\) and three constraints imposed on the variables \(X\) and \(Y\). The only constraint imposed on \(Y\) (namely \(Y \leq 5\)) allows for arbitrarily small values of \(Y\), which cannot correspond to points belonging to the rectangle expected as intersection. Therefore, the user will view the computed answer as wrong w.r.t. the intended meaning of the program. As we will see in Sections 4 and 5, the declarative debugging technique presented in this report leads to the diagnosis of the program rule for the function \textit{rect} as responsible for the wrong answer. Indeed, this program rule is incorrect w.r.t. the intended program semantics; as shown in Example 1, the third inequality at the right hand side should be \(Y' \geq Y\) instead of \(Y' \leq Y\). After this correction, no more wrong computed answers will be observed for the goal discussed above.

As any debugging technique, declarative diagnosis has limitations. A ”corrected” program fragment can still include more subtle bugs that can be observed in the computed answers for other goals. In our case, we can consider the goal

\[
\text{Toy}(R) > \text{intersect } (\text{head } (\text{ladder } (70,40) -50 -20)) \\
(\text{head } (\text{ladder } (35,45) -30 -40)) (X,Y) == R
\]

whose meaning w.r.t. the intended semantics is the same as for the previous goal, except that the rectangles playing the role of initial steps of the two ladders are represented differently. Since the boolean expression at the right hand side of the ”corrected” program rule for function \textit{rect} yields the result \textit{false} whenever \(LX\) or \(LY\) is bound to a negative number, wrong answers including the substitution \(R \rightarrow \text{false}\) will be computed. Moreover, other answers including the substitution \(R \rightarrow \text{true}\) will be expected by the user but missing to occur among the computed answers. The traditional approach to declarative debugging in the \textit{CLP(D)} scheme includes the diagnosis of both \textit{wrong} and \textit{missing} computed answers [18]. However, the declarative diagnosis of missing answers falls outside the scope of this report.

3 The \textit{CFLP(D)} Programming Scheme

In this section we recall the essentials of the \textit{CFLP(D)} scheme [12] for lazy Constraint Functional Logic Programming over a parametrically given constraint domain \(D\), which serves as a logical and semantic framework for the declarative diagnosis method presented in the report.

\footnote{There are other five computed answers consisting of the substitution \(R \rightarrow \text{false}\) and various constraints imposed on \(X\) and \(Y\).}
3.1 Preliminary Notions

We consider a universal signature $\Sigma = \langle DC, FS \rangle$, where $DC = \bigcup_{n \in \mathbb{N}} DC^n$ and $FS = \bigcup_{n \in \mathbb{N}} FS^n$ are countably infinite and mutually disjoint sets of data constructors resp. evaluable function symbols, indexed by arities. Evaluable functions are further classified into domain dependent primitive functions $PF^n \subseteq FS^n$ and user defined functions $DF^n = FS^n \setminus PF^n$ for each $n \in \mathbb{N}$. We write $\Sigma_\bot$ for the result of extending $DC^0$ with the special symbol $\bot$, intended to denote an undefined data value and we assume that $DC$ includes the two constants $true$ and $false$ and the usual list constructors. We use the notations $c, d \in DC, f, g \in FS$ and $h \in DC \cup FS$. We also assume a countably infinite set $V$ of variables $X, Y, \ldots$ and a set $U$ of primitive elements $u, v, \ldots$ (as e.g. the set $\mathbb{R}$ of the real numbers) mutually disjoint and disjoint from $\Sigma_\bot$.

Expressions $e \in \text{Exp}_\bot(U)$ have the following syntax:

$$e ::= \bot \mid u \mid X \mid h \mid (e_1 e_2)$$

where $u \in U, X \in V, h \in DC \cup FS$. An important subclass of expressions is the set of patterns $s, t \in \text{Pat}_\bot(U)$, whose syntax is defined as follows:

$$t ::= \bot \mid u \mid X \mid c t_m \mid f t_m$$

where $u \in U, X \in V, c \in DC^n$ with $m \leq n$, and $f \in FS^n$ with $m < n$. Patterns are used as representations of possibly functional data values. For instance, the rectangle $(\text{rect } (5, 5) 30 40)$ we met when discussing Example 1 is a functional data value represented as pattern.

As usual, we define substitutions $\sigma \in \text{Sub}_\bot(U)$ as mappings $\sigma : V \rightarrow \text{Pat}_\bot(U)$ extended to $\sigma : \text{Exp}_\bot(U) \rightarrow \text{Exp}_\bot(U)$ in the natural way. By convention, we write $e\sigma$ instead of $\sigma(e)$ for any $e \in \text{Exp}_\bot(U)$, and $\sigma\theta$ for the composition of $\sigma$ and $\theta$. A substitution $\sigma$ such that $\sigma\sigma = \sigma$ is called idempotent.

3.2 Constraints over a Constraint Domain

Intuitively, a constraint domain provides a set of specific data elements, along with certain primitive functions operating upon them. Primitive predicates can be modelled as primitive functions returning boolean values. Formally, a constraint domain with primitive elements $U$ and primitive functions $PF \subseteq FS$ is any structure $D = \langle D_U, \{p^D \mid p \in PF\} \rangle$ with carrier set $D_U$ the set of ground patterns (i.e., without variables) over $U$ and interpretations $p^D \subseteq D^U_n \times D_U$ of each $p \in PF^n$ satisfying the technical monotonicity, antimonotonicity and radicality requirements given in [12]. We use the notation $p^D \sqsubseteq t \rightarrow t$ to indicate that $(\bar{t}_n, t) \in p^D$.

Constraints over a given constraint domain $D$ are logical statements built from atomic constraints by means of logical conjunction $\land$ and existential quantification $\exists$. Atomic constraints can have the form $\Diamond$ (standing for truth), $\checkmark$

---

2 Note that (5, 5) can be seen as syntactic sugar for $(\text{pair } 5 5)$, pair being a constructor for ordered pairs.
Example 2 (Constraint domain $\mathcal{R}$). The constraint domain $\mathcal{R}$ has the carrier set $D_\mathcal{R}$ of ground patterns over $\mathbb{R}$ and the primitives defined below:

1. $eq_\mathbb{R}$, equality primitive for real numbers, such that: $eq_\mathbb{R}^R u u \rightarrow true$ for all $u \in \mathbb{R}$; $eq_\mathbb{R}^R v v \rightarrow false$ for all $u, v \in \mathbb{R}, u \neq v$; $eq_\mathbb{R}^R s t \rightarrow \bot$ otherwise.

2. $\mathrm{seq}$, strict equality primitive for ground patterns over the real numbers, such that: $\mathrm{seq}^R t t \rightarrow true$ for all total $t \in D_\mathcal{R}$; $\mathrm{seq}^R t s \rightarrow false$ for all $t, s \in D_\mathcal{R}$ such that $t, s$ have no common upper bound w.r.t. the information ordering introduced in [12] and defined in the Appendix; $\mathrm{seq}^R t s \rightarrow \bot$ otherwise. In the sequel, $e_1 \triangleright e_2$ abbreviates $\triangleright$, $e_2 \triangleright e_1 \rightarrow false$.

3. $+, -, \ast$, for addition, subtraction, and multiplication, such that: $x + \mathcal{R} y \rightarrow x + \mathcal{R} y$ for all $x, y \in \mathbb{R}$; $x + \mathcal{R} y \rightarrow \bot$ whenever $t \notin \mathbb{R}$ or $s \notin \mathbb{R}$; and analogously for $-\mathcal{R}$ and $\ast \mathcal{R}$.

4. $<, \leq, >, \geq$, for numeric comparisons, such that: $x \mathcal{R} y \rightarrow true$ for all $x, y \in \mathbb{R}$ with $x < \mathcal{R} y$; $x \mathcal{R} y \rightarrow false$ for all $x, y \in \mathbb{R}$ with $x \geq \mathcal{R} y$; $i \mathcal{R} s \rightarrow \bot$ whenever $t \notin \mathbb{R}$ or $s \notin \mathbb{R}$; and analogously for $\leq \mathcal{R}$, $\mathcal{R} >$, $\geq \mathcal{R}$. In the sequel, $e_1 < e_2$ abbreviates $e_1 \rightarrow e_2 \rightarrow false$ (analogously for other comparison primitives).

The set of valuations over a constraint domain $\mathcal{D}$ is defined as the set $Val_\mathcal{D}(\mathcal{D})$ of ground substitutions (i.e., mappings from variables into ground patterns). The semantics of constraints relies on the idea that a given valuation can satisfy or not a given constraint. Therefore, the set of solutions of $\pi \in PCon_\mathcal{D}(\mathcal{D})$ can be defined as a subset $Sol_\mathcal{D}(\pi) \subseteq Val_\mathcal{D}(\mathcal{D})$ as follow: $Sol_\mathcal{D}(\emptyset) = Val_\mathcal{D}(\mathcal{D})$, $Sol_\mathcal{D}(\ast) = \emptyset$ and $Sol_\mathcal{D}(p \bar{t}_n \rightarrow t) = \{ \eta \in Val_\mathcal{D}(\mathcal{D}) \mid t \eta \text{ is total and } p^\mathcal{D} \bar{t}_n \eta \rightarrow t \eta \}$. Moreover, the set of solutions of $\Pi \subseteq PCon_\mathcal{D}(\mathcal{D})$ is $Sol_\mathcal{D}(\Pi) = \bigcap_{\pi \in \Pi} Sol_\mathcal{D}(\pi)$.

3.3 Constraint Functional-Logic Programming

For any given constraint domain $\mathcal{D}$, a CFLP($\mathcal{D}$)-program $\mathcal{P}$ is presented as a set of constrained rewrite rules, called program rules, that define the behavior of user-defined functions. More precisely, a constrained program rule $R$ for $f \in DF^n$ has the form $R : f \bar{t}_n \rightarrow r \iff \Delta$ (abbreviated as $f \bar{t}_n \rightarrow r \Delta$ if $\Delta$ is empty) and is required to satisfy the conditions listed below: 3

1. The left-hand side $f \bar{t}_n$ is a linear expression (i.e., there is no variable having more than one occurrence), and for all $1 \leq i \leq n$, $t_i \in Pat_\mathcal{D}(\mathcal{U})$ are total patterns. The right-hand side $r \in \text{Exp}_\mathcal{D}(\mathcal{U})$ is also total.

3 In practice, TOY and similar languages require program rules to be well-typed in a polymorphic type system. However, the CFLP($\mathcal{D}$) scheme can deal also with untyped programs. Well-typedness is viewed as an additional requirement, not as part of program semantics.


2. $\Delta \subseteq DCon_\perp(D)$ is a finite set of total constraints, intended to be interpreted as conjunction, and possibly including occurrences of user-defined functions.

Program defined functions can be higher-order and/or non-deterministic. For instance, the $TOY$ program presented in Section 2 can be interpreted as an example of $CFLP(R)$-program. The reader is referred to [12] for more explanations and examples in other constraint domains.

The intended use of programs is to perform computations by solving goals proposed by the user. An admissible goal for a given $CFLP(D)$-program must have the form $G : \exists \overline{U}. (P \sqcap \Delta)$, where $\overline{U}$ is a finite set of so-called existential variables of the goal $G$ (the rest of variables in $G$ are called free variables and denoted by $fvar(G)$), $P$ is a finite conjunction of so-called productions of the form $e \rightarrow s$ fulfilling the admissibility conditions given in [12], and $\Delta \subseteq DCon_\perp(D)$ is a finite conjunction of total user-defined constraints. Two special kinds of admissible goals are interesting. Initial goals, where $\overline{U}$ and $P$ are both empty (i.e., $G$ has only a constrained part $\Delta$ without occurrences of existential variables), and solved goals (also called solved forms) of the form $S : \exists \overline{U}. (\sigma \sqcap P)$, where $\sigma$ is a finite set of productions $X \rightarrow t$ or $s \rightarrow Y$ interpreted as the variable bindings of an idempotent substitution (see Appendix) and $P \subseteq PCon_\perp(D)$ is a finite conjunction of total user-defined constraints. Finally, a goal solving system for $CFLP(D)$ is expected to accept a program $P$ and an initial goal $G$ from the user, and to obtain one or more solved forms $S_i$ as computed answers. For instance, an initial goal $G$ for the $CFLP(R)$-program shown in Example 1 could be intersect (head (ladder (20, 20) 50 20)) (head (ladder (5, 5) 30 40)) (X, Y) $\leftarrow$ R, and then a computed answer $S$ for $G$ is $R \rightarrow true \iff X \leq 35 \land X \geq 20 \land Y \leq 5$.

Goal solving systems can be implementations of $CFLP$ languages such as Curry [10] or $TOY$ [13], or formal goal solving calculi including recent proposals such as the $CDNC(D)$ calculus [19], which is sound and complete w.r.t. the declarative semantics discussed in the next subsection, and behaves as a faithful formal model for actual computations in the $TOY$ system.

3.4 Declarative Semantics

In this subsection we recall some notions and results on the declarative semantics of $CFLP(D)$-programs which were developed in [12] and are needed for the rest of this report. Given a constraint domain $D$ we consider two different kinds of constrained statements (briefly, $c$-statements) involving partial patterns $t$, $t_i \in Pat_\perp(U)$, partial expressions $e$, $e_i \in Exp_\perp(U)$, and a finite set $P \subseteq PCon_\perp(D)$ of primitive constraints:

1. $c$-productions $e \rightarrow t \leftarrow \Pi$, with $e \in Exp_\perp(U)$ (if $\Pi$ is empty they boil down to unconstrained productions written as $e \rightarrow t$). As a particular kind of $c$-productions useful for debugging we distinguish $c$-facts $f \overline{t}_n \rightarrow t \leftarrow \Pi$ with $f \in DF_n$. A $c$-production is called trivial iff $t = \bot$ or $Sol_D(\Pi) = \emptyset$.

2. $c$-atoms $p\overline{\iota}_n \rightarrow !t \leftarrow \Pi$, with $p \in PF_n$ and $t$ total (if $\Pi$ is empty they boil down to unconstrained atoms written as $p\overline{\iota}_n \rightarrow !t$). A $c$-atom is called trivial iff $Sol_D(\Pi) = \emptyset$. 


In the sequel we use \( \varphi \) to denote any c-statement. A c-interpretation over \( \mathcal{D} \) is defined as any set \( I \) of c-facts including all the trivial c-facts and closed under \( \mathcal{D} \)-entailment, a generalization of the entailment notion introduced in [4] to arbitrary constraint domains. We write \( I \models_{\mathcal{D}} \varphi \) to indicate that the c-statement \( \varphi \) (not necessarily a c-fact) is semantically valid in the c-interpretation \( I \). This notation relies on a formal definition given in [12]. Now we are in a position to define various semantic notions which rely on a given c-interpretation \( I \) over \( \mathcal{D} \).

**Definition 1 (interpretation-dependent semantic notions).**

1. The set of solutions of \( \delta \) in \( DCon_{\bot}(\mathcal{D}) \) is a subset \( Sol_{I}(\delta) \subseteq Val_{\bot}(\mathcal{D}) \) defined as follows:
   (a) \( Sol_{I}(\pi) = Sol_{\mathcal{D}}(\pi) \), for any \( \pi \in PCon_{\bot}(\mathcal{D}) \).
   (b) \( Sol_{I}(\delta) = \{ \eta \in Val_{\bot}(\mathcal{D}) \mid I \models_{\mathcal{D}} \delta \eta \} \), for any \( \delta \in DCon_{\bot}(\mathcal{D}) \setminus PCon_{\bot}(\mathcal{D}) \).
   
   The set of solutions of a set of constraints \( \Delta \subseteq DCon_{\bot}(\mathcal{D}) \) is defined as \( Sol_{I}(\Delta) = \bigcap_{\delta \in \Delta} Sol_{I}(\delta) \).

2. The set of solutions of a production \( e \rightarrow t \) is a subset \( Sol_{I}(e \rightarrow t) \subseteq Val_{\bot}(\mathcal{D}) \) defined as \( Sol_{I}(e \rightarrow t) = \{ \eta \in Val_{\bot}(\mathcal{D}) \mid I \models_{\mathcal{D}} e\eta \rightarrow t\eta \} \). The set of solutions of a set of productions \( P \) is defined as \( Sol_{I}(P) = \bigcap_{(e \rightarrow t) \in P} Sol_{I}(e \rightarrow t) \).

3. The set of solutions of an admissible goal \( G : \exists U. (P \sqcap \Delta) \) is a subset \( Sol_{I}(G) \subseteq Val_{\bot}(\mathcal{D}) \) defined as follows: \( Sol_{I}(G) = \{ \eta \in Val_{\bot}(\mathcal{D}) \mid \eta' \in Sol_{I}(P) \cap Sol_{I}(\Delta) \text{ for some } \eta' = \eta \text{ except perhaps over } U \} \).

For primitive constraints one can easily check that \( Sol_{I}(H) = Sol_{\mathcal{D}}(H) \). Moreover, we note that \( Sol_{I}(S) = Sol_{\mathcal{D}}(S) \) for every solved form \( S \).

**Definition 2 (model-theoretic semantics).** Let \( \mathcal{P} \) a CFLP(\( \mathcal{D} \))-program and \( I \) a c-interpretation.

1. \( I \) is a model of \( \mathcal{P} \) (in symbols, \( I \models_{\mathcal{D}} \mathcal{P} \)) iff every constrained program rule \((f_{\eta} \rightarrow r \leftarrow \Delta) \in \mathcal{P} \) is valid in \( I \): for any ground substitution \( \eta \in Sub_{\bot}(U) \) and \( t \in Pat_{\bot}(U) \) ground such that \((f_{\eta} \rightarrow r \leftarrow \Delta)\eta \) is ground, \( I \models_{\mathcal{D}} \Delta\eta \) and \( I \models_{\mathcal{D}} r\eta \rightarrow t \) one has \( I \models_{\mathcal{D}} (f_{\eta}\eta) \rightarrow t \) (or equivalently, \((f_{\eta}\eta) \rightarrow t) \in I \).

2. A solved form \( S \) is a semantically valid answer for a goal \( G \) w.r.t. a program \( \mathcal{P} \) (in symbols, \( \mathcal{P} \models_{\mathcal{D}} G \leftarrow S \)) iff \( Sol_{\mathcal{D}}(S) \subseteq Sol_{I}(G) \) for all \( I \models_{\mathcal{D}} \mathcal{P} \).

## 4 Declarative Diagnosis of Wrong Answers in CFLP(\( \mathcal{D} \))

In this section we present a declarative diagnosis method for CFLP(\( \mathcal{D} \)) and prove its logical correctness. In what follows, we assume that a constraint domain \( \mathcal{D} \) and a CFLP(\( \mathcal{D} \))-program \( \mathcal{P} \) are given.

### 4.1 Wrong Answers and Intended Interpretations

Declarative diagnosis techniques rely on a declarative description of the intended program semantics. We will assume that the user knows (at least to the extent needed for answering queries during the debugging session) a so-called intended
model I, which is a c-interpretation expected to satisfy $I \models_{D} P$, unless $P$ is incorrect. For instance, $\text{rect} (X, Y) \land X \leq Y \rightarrow \text{false} \iff A < X$ could belong to the intended model $I$ for the program fragment shown in Example 1. As explained in Subsection 3.4, the c-facts belonging to c-interpretations can be non-ground. Nevertheless, the model notion $I \models_{D} P$ used here (see Definition 2 above) corresponds to the so-called weak semantics from [12], which depends just on the ground c-facts belonging to $I$. Therefore, different presentations of the intended model will be equivalent for the purposes of this report, as long as they include the same ground c-facts.

The aim of declarative diagnosis is to start with an observed symptom of erroneous program behavior, and detect some error in the program. The proper notions of symptom and error in our setting are as follows:

**Definition 3 (symptoms and errors).** Assume $I$ is the intended interpretation for program $P$, and consider a solved form $S$ produced as computed answer for the initial goal $G$ by some goal solving system. We define:

1. $S$ is a wrong answer w.r.t $I$ (serving as symptom) iff $\text{Sol}_{D}(S) \not\subseteq \text{Sol}_{I}(G)$.
2. $P$ is incorrect w.r.t. $I$ iff there exists some program rule $(f t \leftarrow r \leftarrow \Delta) \in P$ (manifesting an error) that is not valid in $I$ (in the sense of Definition 2).

For instance, the computed answer shown in Example 1 is wrong w.r.t. the intended model for the program assumed in that example, for the reasons already discussed in Section 2. As illustrated by this example, computed answers typically include constraints on the variables occurring in the initial goal. However, goal solving systems for CFLP($D$) programs also maintain internal information on constraints related to variables used in intermediate computation steps, but not occurring in the initial goal. Such information is relevant for declarative debugging purposes. Therefore, in the rest of this section we will assume that computed answers $S$ include also constraints related to intermediate variables.

### 4.2 A Logical Calculus for Witnessing Computed Answers

Assuming that $S$ is a computed answer for an initial goal $G$ using program $P$, declarative diagnosis needs a suitable CT representing the computation. In our setting we will obtain the CT from a logical proof $P \vdash_{\text{CPPC}(D)} G \leftarrow S$ which derives the statement $G \leftarrow S$ from the program $P$ in the Constraint Positive Proof Calculus (shortly CPPC($D$)) given by the inference rules in Fig. 1. We will say that the CPPC($D$)-proof witnesses the computed answer.

Most of these rules have been borrowed from the proof theory of CRW$L(D)$, a Constraint ReWriting Logic which characterizes the semantics of CFLP($D$) programs [12]. The main novelties in CPPC($D$) are the addition of rule EX (to deal with the existential quantifiers in computed answers) and a reformulation of rule DF$_P$, which is presented as the consecutive application of two inference steps named AR$_f$ and FA$_f$, which cannot be applied separately. The purpose of this composite inference is to introduce the c-facts $f t \leftarrow t \leftarrow \Pi$ at the conclusion of inference FA$_f$, called boxed c-facts in the sequel. As we will see,
only boxed c-facts will appear at the nodes of CTs obtained from $CPPC(D)$-proofs. Therefore, all the queries asked to the user during a declarative debugging session will be about the validity of c-facts in the intended model of the program, which is itself represented as a set of c-facts. We also agree that the premises $Gσ \models \Pi$ in rule $EX$ (resp. $Δ \models \Pi$ in rule $DF_p$) must be understood as a shorthand for several premises $α \models \Pi$, one for each atomic $ϕ$ in $Gσ$ (resp. $Δ$).

Any $CPPC(D)$-derivation $P \vdash_{CPPC(D)} G \models S$ can be depicted in the form of a Positive Proof Tree over $D$ (shortly, $PPT(D)$) with $G \models S$ at the root and
c-statements at the internal nodes, and such that the statement at any node is inferred from the statements at its children using some $CPPC(D)$ inference rule. In particular, the statement at the root must be inferred using rule $\text{EX}$, which is then applied nowhere else in the proof tree. Fig. 2. shows a $PPT(R)$ representing a $CPPC(R)$-derivation which witnesses the computed answer from Example 1, which is wrong w.r.t. the intended model of the program.

We say that a goal solving system is called $CPPC(D)$-sound iff for any computed answer $S$ obtained for an initial goal $G$ using program $P$ there is...
some witnessing $\text{CPPC}(\mathcal{D})$-proof $\mathcal{P} \vdash_{\text{CPPC}(\mathcal{D})} G \Leftarrow S$. The next result shows that $\text{CPPC}(\mathcal{D})$-sound goal solving systems exist:

**Theorem 1 (existence of $\text{CPPC}(\mathcal{D})$-sound goal solving systems).** The goal solving calculus $\text{CDNC}(\mathcal{D})$ given in [19] is $\text{CPPC}(\mathcal{D})$-sound.

**Proof.** Straightforward adaptation of the soundness theorem for $\text{CDNC}(\mathcal{D})$ presented in [19].

In addition to $\text{CDNC}(\mathcal{D})$, other formal goal solving calculi known for $\text{CFLP}(\mathcal{D})$ are also $\text{CPPC}(\mathcal{D})$-sound. Moreover, it is also reasonable to assume $\text{CPPC}(\mathcal{D})$-soundness for implemented goal solving systems such as $\text{Curry}$ [10] and $\text{TOY}$ [13] whose computation model is based on constrained lazy narrowing. Moreover, any $\text{CPPC}(\mathcal{D})$-sound goal solving system is semantically sound in the sense of item 2 in Definition 2:

**Theorem 2 (Semantic correctness of the $\text{CPPC}(\mathcal{D})$ calculus).** If $G$ is an initial goal for $\mathcal{P}$ and $S$ is a solved goal such that $\mathcal{P} \vdash_{\text{CPPC}(\mathcal{D})} G \Leftarrow S$ then $\mathcal{P} \models_{\mathcal{D}} G \Leftarrow S$.

**Proof.** It is sufficient to assume an arbitrarily given model $\mathcal{I} \models_{\mathcal{D}} \mathcal{P}$ and to prove that any $\text{CPPC}(\mathcal{D})$ inference rule whose premises are valid in $\mathcal{I}$ has a conclusion that is also valid in $\mathcal{I}$. Details are given in the Appendix.

### 4.3 Declarative Diagnosis using Proof Trees

Now we are ready to present a declarative diagnosis method and to prove its correctness. Our results apply to any $\text{CPPC}(\mathcal{D})$-sound goal solving system. First we prove that the observation of an error symptom implies the existence of some error in the program:

**Theorem 3 (Wrong answers are caused by erroneous program rules).** Assume that a $\text{CPPC}(\mathcal{D})$-sound goal solving system computes $S$ as answer for the initial goal $G$ using program $\mathcal{P}$. If $S$ is wrong w.r.t. the user’s intended interpretation $\mathcal{I}$ then some program rule belonging to $\mathcal{P}$ is incorrect w.r.t. $\mathcal{I}$. 

**Proof.** Because of $\text{CPPC}(\mathcal{D})$-soundness of the goal solving system, we know that $\mathcal{P} \vdash_{\text{CPPC}(\mathcal{D})} G \Leftarrow S$. Then, from Theorem 2 we obtain $\mathcal{P} \models_{\mathcal{D}} G \Leftarrow S$, i.e. $\text{Sol}_{\mathcal{D}}(S) \subseteq \text{Sol}_{\mathcal{J}}(G)$ for each model $\mathcal{J} \models_{\mathcal{D}} \mathcal{P}$. Since $S$ is wrong w.r.t. the user’s intended model $\mathcal{I}$, it must be the case that $\text{Sol}_{\mathcal{D}}(S) \nsubseteq \text{Sol}_{\mathcal{I}}(G)$ because of Definition 3. Therefore, we can conclude that the intended model $\mathcal{I}$ is not a model of $\mathcal{P}$. Then, by Definition 2, some program rule belonging to $\mathcal{P}$ is not valid in $\mathcal{I}$. 

The previous theorem does not yet provide a practical method for finding an erroneous program rule. As explained in the Introduction, a declarative diagnosis method is expected to find the erroneous program rule by inspecting a CT. We propose to use abbreviated $\text{CPPC}(\mathcal{D})$ proof trees as CTs. Since $\text{DF}_{\mathcal{P}}$ is the
only inference rule in the \textit{CPPC} calculus that depends on the program, abbreviated proof trees will omit the inference steps related to all the other \textit{CPPC} rules. More precisely, given a \textit{PPT(D)} \(T\), its associated \textit{Abbrivated Positive Proof Tree} over \(D\) (shortly, \textit{APPT(D)}) \(AT\) is defined as follows:

- The root of \(AT\) is the root of \(T\).
- The children of a node \(N\) in \(AT\) are the closest descendants of \(N\) in \(T\) corresponding to boxed c-facts introduced by \textit{DFP} inference steps.

A node in an \textit{APPT(D)} is called a \textit{buggy node} iff the c-statement at the node is not valid in the intended interpretation \(I\), while all the c-statements at the children nodes are valid in \(I\). Our last theorem guarantees that declarative diagnosis with \textit{APPT(D)s} used as \(CTs\) leads to the correct detection of program errors. A proof is given in the Appendix.

**Theorem 4 (Declarative diagnosis of wrong answers).** Under the assumptions of Theorem 3, any \textit{APPT(D)} witnessing \(P \vdash_{\text{CPPC}(D)} G \Leftarrow S\) (which must exist due to \textit{CPPC(D)-soundness} of the goal solving system) has some buggy node. Moreover, each buggy node points to a program rule belonging to \(P\) which is incorrect in the user’s intended interpretation.

5 A Practical Debugging Tool for \textit{CFLP(R)}

Fig. 3 shows the \textit{APPT(R)} associated to the \textit{PPT(R)} of Fig. 2, as displayed by \textit{DDT}, the debugger tool included in the system \textit{TOY}. Although in theory all the c-facts in a \textit{PPT(R)} should include the same constraint \(\Pi\), in practice the tool simplifies \(\Pi\) at each c-fact \(f \bar{T}_n \rightarrow t \Leftarrow \Pi\), keeping only those atomic constraints related to the variables occurring on \(f \bar{T}_n \rightarrow t\). It can be checked that such a simplification does not affect to the intended meaning of c-facts.

![Fig. 3. The APPT(R) corresponding to the PPT(R) of Fig. 2.](image-url)
Before starting a debugging session the user may inspect and simplify the tree using several facilities. For instance the user could mark any node corresponding to the infix function && as trusted, indicating that the definition of && is surely not erroneous. This makes all the nodes corresponding to && automatically valid. Valid nodes can be removed from the tree safely (the set of buggy nodes doesn’t change) by using a suitable menu option.

Next, the user can start a debugging session by selecting one of the two possible strategies included in DDT: the top-down or the divide and query strategy (see [5] for a comparative between both strategies in an older version of DDT which did not yet support constraints). After selecting the divide and query strategy, which usually leads to shorter sessions, DDT asks about the validity of the following node:

<table>
<thead>
<tr>
<th>Divide &amp; Query Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Fact</td>
</tr>
<tr>
<td>intersect (rect (0, 20).50, 20.50) (rect (5, 5).50, 40.0) -&gt; true &lt;= X &lt;= 20, X &gt;= 20, Y &lt;= 5</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The intended program model corresponds to the intuitions explained in Section 2. Therefore, the question must be understood as: Is \((X, Y)\) a point in the intersection of the two rectangles for all possible values of \(X\), \(Y\) satisfying \(X \leq 35\), \(X \geq 20\), \(Y \leq 5\) is \((X, Y)\)? The answer is no, because with these constraints \(Y\) can take any value less than 5 and some of these values would yield a pair \((X, Y)\) out of the intersection for every \(X\). Therefore the user marks the cross meaning that the c-fact is non-valid. The next question is:

<table>
<thead>
<tr>
<th>Divide &amp; Query Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Fact</td>
</tr>
<tr>
<td>intersect (rect (0, 20).50, 20.50) (rect (5, 5).50, 40.0) -&gt; true &lt;= X &lt;= 20, X &gt;= 20, Y &lt;= 5</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

which is also reported as non-valid by the user. At this point a buggy node is found by the tool, pointing out to the incorrect program rule and ending the debugging session:

<table>
<thead>
<tr>
<th>Buggy Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>BuggyNodeFound!</td>
</tr>
<tr>
<td>Node intersect (rect (0, 20).50, 20.50) (rect (5, 5).50, 40.0) -&gt; true &lt;= X &lt;= 20, X &gt;= 20, Y &lt;= 5</td>
</tr>
<tr>
<td>Programme: rect 5</td>
</tr>
</tbody>
</table>

The current version of the debugger supports programs using the constraint domain \(\mathcal{R}\), which provides arithmetic constraints over the real numbers as well as strict equality and disequality constraints over data values of any type; see Example 2 and [12] for details. The tool is as an extension of older versions which did not yet support constraints over the domain \(\mathcal{R}\) [5,3], and it is part of the public distribution of the functional logic programming system TOY, available at http://toy.sourceforge.net. The APPT associated to a wrong answer is constructed by means of a suitable program transformation. The yielded tree is then displayed through a graphical debugging interface implemented in Java. More detailed explanations on the practical use of DDT can be found in [5,3].
6 Conclusions and Future Work

We have presented a declarative technique for diagnosing wrong computed answers in \( \text{CFLP}(\mathcal{D}) \), a generic scheme for constraint functional logic programming over a given constraint domain \( \mathcal{D} \). Our diagnosis technique represents the computation which has produced a wrong computed answer by means of an abridged proof tree whose inspection leads to the discovery of at some erroneous program rule responsible for the wrong answer. The logical correctness of the method can be formally proved thanks to the connection between abridged proof trees and program semantics.

A debugging tool called \( \text{DDT} \) which implements the proposed technique over the domain \( \mathcal{R} \) of arithmetic constraints over the real numbers has been implemented as a non-trivial extension of previously existing debugging tools. \( \text{DDT} \) provides several practical facilities for reducing the number and the complexity of the questions that are presented to the user during a debugging session.

As future work, we plan to develop a formal framework for the declarative diagnosis of missing answers in \( \text{CFLP}(\mathcal{D}) \), using a suitable kind of abridged proof trees as computation trees. On the practical level we plan several improvements of \( \text{DDT} \), such as enabling the diagnosis of missing answers, supporting finite domain constraints, and providing new facilities for simplifying the presentation of queries to the user.

References


Appendix

In this Appendix, intended for the reviewers, we give the proofs of the main results omitted in the report. Within these proofs, we will use the following definition for the useful information ordering $\sqsubseteq$ introduced in [12] over partial expressions: $\bot \sqsubseteq e$ for all $e \in \text{Exp}_\bot(\mathcal{U})$ and $(e e_1) \sqsubseteq (e' e_2')$ whenever $e \sqsubseteq e'$ and $e_1 \sqsubseteq e_2'$. Moreover, we will use the notation $\eta =_X \eta'$ to indicate that $\eta |_X = \eta' |_X$ for all $\eta, \eta' \in \text{Sub}_\bot(\mathcal{U})$ and $X \subseteq \mathcal{V}$, and we abbreviate $\eta =_{\mathcal{V}\setminus X} \eta'$ as $\eta =_{\mathcal{V}\setminus X} \eta'$.

The first result proves that productions $X \rightarrow t$ or $s \rightarrow Y$ occurring in a solved form can be interpreted as the variable bindings of an idempotent substitution $\sigma$, because of the following proposition:

**Proposition 1.** For any solved form $S$ as presented above, $\text{Sol}_D(\exists \mathcal{U}. \overline{X_n \rightarrow t_n \land \overline{s_m \rightarrow Y_m \square \square II}}) = \text{Sol}_D(\exists \mathcal{U}. \overline{X_n = t_n \land \overline{s_m = Y_m \square \square II}})$.

**Proof.** Let $\eta \in \text{Val}_\bot(D)$ be any valuation. We prove that (a) $\eta \in \text{Sol}_D(\exists \mathcal{U}. \overline{X_n \rightarrow t_n \land \overline{s_m \rightarrow Y_m \square \square II}}) \Leftrightarrow$ (b) $\eta \in \text{Sol}_D(\exists \mathcal{U}. \overline{X_n = t_n \land \overline{s_m = Y_m \square \square II}})$. In this proof, the symbol $\rightarrow$ is interpreted as the symbol $\sqsubseteq$. (b) $\Rightarrow$ (a) holds trivially because "$u = v$" $\Rightarrow$ "$u \sqsubseteq v$". We prove now (a) $\Rightarrow$ (b). If $\eta \in \text{Sol}_D(\exists \mathcal{U}. \overline{X_n \rightarrow t_n \land \overline{s_m \rightarrow Y_m \square \square II}})$ then there exists $\eta' \in \text{Val}_\bot(D)$ such that $\eta' =_{\mathcal{V}} \eta$ and $\eta' \in \text{Sol}_D(\overline{X_n \rightarrow t_n \land \overline{s_m = Y_m \square \square II}})$, i.e. $X_i \eta' \sqsubseteq t_i \eta'$ (1 $\leq$ i $\leq$ n), $s_i \eta' \sqsubseteq Y_i \eta'$ (1 $\leq$ j $\leq$ m) and $\eta' \in \text{Sol}_D(\square II)$. By the admissibility conditions of goals, the sequence of patterns $t_1 \ldots t_n Y_1 \ldots Y_m$ is lineal and it has only occurrences of variables in $\mathcal{U}$. Therefore, we can take another $\eta'' \in \text{Val}_\bot(D)$ such that $\eta'' \sqsubseteq \eta'$, $\eta'' =_{\mathcal{V}} \eta'$, $X_i \eta'' = t_i \eta''$ (1 $\leq$ i $\leq$ n) and $s_i \eta'' = Y_i \eta''$ (1 $\leq$ j $\leq$ m). Since $\eta'' =_{\mathcal{V}} \eta'' =_{\mathcal{V}} \eta$, we conclude that $\eta'' =_{\mathcal{V}} \eta$ such that $\eta'' \in \text{Sol}_D(\overline{X_n = t_n \land \overline{s_m = Y_m \square \square II}})$ and then $\eta \in \text{Sol}_D(\exists \mathcal{U}. \overline{X_n = t_n \land \overline{s_m = Y_m \square \square II}})$.

The two following auxiliary lemmas used in the proof of Theorem 2 can be proved by simple (albeit tedious) inductive reasoning:

**Lemma 1 (Substitution Lemma).**
Assume a given c-interpretation $\mathcal{I}$ over $D$, an admissible goal $G$, a valuation $\eta \in \text{Val}_\bot(D)$ and an idempotent substitution $\sigma \in \text{Sub}_\bot(\mathcal{U})$ such that $\eta \in \text{Sol}_D(\sigma)$ (i.e. $X_\eta = X_{\sigma \eta}$ for all $X \in \text{dom}(\sigma)$) and $\eta \in \text{Sol}_D(G\sigma)$. Then $\eta \in \text{Sol}_D(G)$.

**Lemma 2 (Coincidence Lemma).**
Assume a given c-interpretation $\mathcal{I}$ over $D$, an admissible goal $G$, and two valuations $\eta, \eta' \in \text{Val}_\bot(D)$ such that $\eta =_{\text{false}(G)} \eta'$. Then $\eta \in \text{Sol}_D(G)$ iff $\eta' \in \text{Sol}_D(G)$. 

Proof of Theorem 2 (Semantic correctness of the CPPC(D) calculus):

Proof. The proof of this result is based on the inductive proof for the semantic correctness of the CRWL(D) calculus presented in [12]. We have only to prove that the new rules EX, ARI and FAI introduced in the CPPC(D) calculus are semantically correct in the inductive part of this proof with respect to the declarative semantics introduced in Subsection 3.4:

– The rule EX is semantically correct. We suppose by induction hypothesis that \( \mathcal{P} \models_D G \sigma \Leftarrow I \) and we prove that also \( \mathcal{P} \models_D G \Longleftrightarrow \exists \mathcal{U}. \ (\sigma \circ I) \). Let \( \mathcal{I} \) be an arbitrary model of \( \mathcal{P} \) such that \( \mathcal{I} \models_D G \sigma \Leftarrow I \), i.e. \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(G) \). We prove that \( \mathcal{I} \models_D G \Longleftrightarrow \exists \mathcal{U}. \ (\sigma \circ I), \text{Sol}_D(\exists \mathcal{U}. \ (\sigma \circ I)) \subseteq \text{Sol}_D(G) \). Let \( \eta \in \text{Sol}_D(\exists \mathcal{U}. \ (\sigma \circ I)) \). By the syntactic form of solved goals, \( \eta \in \text{Sol}_D(\exists \mathcal{U}. \ (X_n = t_n \wedge s_m = m \circ I)) \). From Proposition 1, \( \eta \in \text{Sol}_D(\exists \mathcal{U}. \ (X_n = t_n \wedge Y_m = m \circ I)) \). By applying Definition 1, there exists \( \eta' \in Val_\lambda(D) \) such that \( \eta' = \eta \eta' \in \text{Sol}_D(X_n = t_n \wedge Y_m = m \circ I) \), and therefore, \( \eta' \in \text{Sol}_D(X_n = t_n \wedge Y_m = m) \) (i.e., \( \eta' \in \text{Sol}_D(\sigma) \)) and \( \eta' \in \text{Sol}_D(\mathcal{I}) \). Since by induction hypothesis \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(G) \), it follows that \( \eta' \in \text{Sol}_D(G) \). Moreover, since \( \eta \in \text{Sol}_D(\mathcal{I}) \), using Lemma 1, we obtain \( \eta' \in \text{Sol}_D(G) \). In consequence, there exists \( \eta' \in Val_\lambda(D) \) such that \( \eta' = \eta \eta' \in \text{Sol}_D(X_n = t_n \wedge Y_m = m \circ I) \). Finally, using the condition of applicability \( \text{fvar}(G) \cap \mathcal{U} = \emptyset \) associated to the rule EX and the Lemma 2, we can conclude that \( \eta \in \text{Sol}_D(G) \).

– The rule ARI is semantically correct. We suppose by induction hypothesis that \( \mathcal{P} \models_D e_i \rightarrow t_i \Leftarrow I \) for each \( 1 \leq i \leq n \), \( \mathcal{P} \models_D \bar{s}_k \rightarrow t \Leftarrow I \) and we prove that also \( \mathcal{P} \models_D \bar{f}_n \bar{s}_k \rightarrow t \Leftarrow I \). Let \( \mathcal{I} \) be an arbitrary model of \( \mathcal{P} \) such that \( \mathcal{I} \models_D e_i \rightarrow t_i \Leftarrow I \) for each \( 1 \leq i \leq n \) (i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(e_i \rightarrow t_i) \) for each \( 1 \leq i \leq n \)), \( \mathcal{I} \models_D \bar{f}_n \rightarrow s \Leftarrow I \) (i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(\bar{f}_n \rightarrow s) \)) and \( \mathcal{I} \models_D \bar{s}_k \rightarrow s \Leftarrow I \) (i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(\bar{s}_k \rightarrow t) \)). We prove that \( \mathcal{I} \models_D \bar{f}_n \bar{s}_k \rightarrow t \Leftarrow I \), i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(\bar{f}_n \bar{s}_k \rightarrow t) \). Let \( \eta \in \text{Sol}_D(\mathcal{I}) \). We have then \( \eta \in \text{Sol}_D(e_i \rightarrow t_i) \) for each \( 1 \leq i \leq n \), and by Definition 1, \( \mathcal{I} \models_D e_i \eta \rightarrow t_i \eta \) for each \( 1 \leq i \leq n \). Analogously, \( \eta \in \text{Sol}_D(\bar{f}_n \rightarrow s) \), by Definition 1, \( \mathcal{I} \models_D \bar{f}_n \eta \rightarrow s \eta \), and by the Conservation Property (see [12] for details), \( (f \eta_n \rightarrow s) \in I \). Analogously, \( \eta \in \text{Sol}_D(\bar{s}_k \rightarrow t) \) and by Definition 1, \( \mathcal{I} \models_D (s) \eta \rightarrow t \eta \). But then, by applying of the rule DF (see [12] for details), we have that \( \mathcal{I} \models_D (\bar{f}_n \eta) (\bar{s}_k \eta) \rightarrow t \eta \). From Definition 1, we obtain finally \( \eta \in \text{Sol}_D(\bar{f}_n \bar{s}_k \rightarrow t) \).

– The rule FAI is semantically correct. We suppose by induction hypothesis that \( \mathcal{P} \models_D \Delta \Leftarrow I \), \( \mathcal{P} \models_D r \rightarrow s \Leftarrow I \) and we prove \( \mathcal{P} \models_D \bar{f}_n \rightarrow s \Leftarrow I \) where \( (f \bar{t}_n \rightarrow r \Leftarrow \Delta) \in \mathcal{P} \). By definition of \( [\mathcal{P}]_\perp \), there are \( (f \bar{t}_n \rightarrow r' \Leftarrow \Delta') \in \mathcal{P} \) and \( \theta \in \text{Sub}_\perp(\mathcal{U}) \) such that \( (f \bar{t}_n \rightarrow r' \Leftarrow \Delta') \theta \equiv (f \bar{t}_n \rightarrow r \Leftarrow \Delta) \). Let \( \mathcal{I} \) be an arbitrary model of \( \mathcal{P} \) such that \( \mathcal{I} \models_D \Delta \Leftarrow I \) (i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(\Delta) \)) and \( \mathcal{P} \models_D r \rightarrow s \Leftarrow I \) (i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(r \rightarrow s) \)). We prove that \( \mathcal{I} \models_D \bar{f}_n \rightarrow s \Leftarrow I \), i.e., \( \text{Sol}_D(\mathcal{I}) \subseteq \text{Sol}_D(\bar{f}_n \rightarrow s) \). Let \( \eta \in \text{Sol}_D(\mathcal{I}) \). Then we have \( \eta \in \text{Sol}_D(\Delta) \), and by Definition 1, \( \mathcal{I} \models_D \Delta \eta \), and
also, \( I \models_{\mathcal{D}} \Delta' \theta \eta \). Analogously, \( \eta \in \text{Sol}_I(r \rightarrow s) \), and by Definition 1, \( I \models_{\mathcal{D}} r \eta \rightarrow s \eta \), and also, \( I \models_{\mathcal{D}} r' \theta \eta \rightarrow s \eta \). We have then \( (fI_n \rightarrow r') \in \mathcal{P}, \theta \eta \in \text{Sub}_1(U) \) ground substitution and \( s \eta \in \text{Pat}_1(U) \) ground such that \( (fI_n \rightarrow r') \theta \eta \equiv (fI_n \rightarrow r) \eta \) is ground, \( I \models_{\mathcal{D}} \Delta \theta \eta \) and \( I \models_{\mathcal{D}} r' \theta \eta \rightarrow s \eta \). Since \( I \) is a model of \( \mathcal{P} \), by applying Definition 2, we obtain \( ((fI_n) \theta \eta \rightarrow s \eta) \in I \), i.e., \( ((fI_n) \eta \rightarrow s \eta) \in I \), or also, \( (fI_n \rightarrow s) \eta \in I \). Finally, by applying the Conservation Property (see [12] for details), it is equivalent to \( I \models_{\mathcal{D}} (fI_n \rightarrow s) \eta \), and by Definition 1, we can conclude that \( \eta \in \text{Sol}_I(fI_n \rightarrow s) \).

\[ \square \]

**Proposition 2** (Weak completeness of declarative debugging).

*Every finite computation tree with an erroneous root contains at least one buggy node.*

**Proof.** Induction on the depth of the computation tree \( \mathcal{T} \):

- **Basis.** In this case \( \mathcal{T} \) only contains one node, which is trivially a buggy node.
- **Inductive case.** We consider again the root of \( \mathcal{T} \). Two possible cases:
  - If there is no incorrect child, the root is a buggy node.
  - If some child \( N \) is incorrect we consider its associated subtree \( \mathcal{T}_N \). The depth of \( \mathcal{T}_n \) is less of the depth of \( \mathcal{T} \). Therefore, by induction hypotheses \( \mathcal{T}_N \) contains a buggy node.

**Proposition 3.** Let \( \mathcal{T} \) be any PPT(\( \mathcal{D} \)) and \( \mathcal{A} \mathcal{T} \) the corresponding APPT(\( \mathcal{D} \)). Any buggy node \( N \) of \( \mathcal{A} \mathcal{T} \) corresponds to a boxed node of \( \mathcal{T} \) introduced by an application of the CPPC(\( \mathcal{D} \))-inference \( \mathbf{DF} \). Moreover, \( N \) is also a buggy node in \( \mathcal{T} \).

**Proof.** Let \( N \) be any buggy node of \( \mathcal{A} \mathcal{T} \), and let \( N'_1, \ldots, N'_p \) be the children of \( N \) in \( \mathcal{A} \mathcal{T} \), and let \( \varphi, \varphi'_j \) (\( 1 \leq j \leq p \)) be the answer collection statements labelling \( N \) and the \( N'_j \). Since \( N \) is a buggy node, all the \( \varphi'_j \) are valid in \( I \) while \( \varphi \) is invalid in \( I \). Due to the construction of \( \mathcal{A} \mathcal{T} \) from \( \mathcal{T} \), there are two possible cases for the relationship between \( N \) and the \( N'_j \) in \( \mathcal{T} \):

- **Case 1:** \( N \) is the root of \( \mathcal{T} \) and \( N'_j \) are the closest independent descendants of \( N \) in \( \mathcal{T} \) which are boxed nodes.
- **Case 2:** \( N \) is a boxed node of \( \mathcal{T} \) and \( N'_j \) are the closest independent descendants of \( N \) in \( \mathcal{T} \) which are boxed nodes.

In Case 1, all the inference steps going from \( \varphi'_1, \ldots, \varphi'_m \) to \( \varphi \) in \( \mathcal{T} \) would use a CPPC(\( \mathcal{D} \))-inference other than \( \mathbf{DF} \). As shown by the proof of Theorem 2, all the inference rules in CPPC(\( \mathcal{D} \)) with the single exception of \( \mathbf{DF} \) preserve validity in arbitrary interpretations. Since all the \( \varphi'_j \) are valid in \( I \) but \( \varphi \) is not, this case is impossible. In Case 2, each of the children \( N_i \) (\( 1 \leq i \leq m \)) of \( N \) in \( \mathcal{T} \) is labelled by some answer collection statement \( \varphi_i \) which follows from \( \varphi'_1, \ldots, \varphi'_j \)
by means of $CPPC(D)$-inferences other than $DF_P$, preserving validity in arbitrary interpretations. Therefore, $\varphi_i$ is valid in $\mathcal{I}$ for all $1 \leq i \leq m$, and $N$ is a buggy node in $T$. \hfill \Box

**Proof of Theorem 4 (Declarative diagnosis of wrong Answers):**

Proof. Let $T$ be a $PPT(D)$ witnessing $\mathcal{P} \vdash_{CPPC(D)} G \Leftarrow S$ and let $AT$ be the corresponding $APPT(D)$. Due to the weak completeness of declarative debugging (see [14] or Proposition 2), $AT$ has some buggy node. Due to Proposition 3, any buggy node $N$ of $AT$ corresponds to a boxed node introduced in $T$ by an application of the $CPPC(D)$-inference $DF_P$, which is also a buggy node in $T$. Therefore, looking to the boxed node $N$ in $T$ we find:

1. $N$ is labelled by $f\bar{t}_n \rightarrow s \Leftarrow \Pi$ invalid in $\mathcal{I}$. Therefore, $\mathcal{I} \not\models_{\mathcal{D}} f\bar{t}_n \rightarrow s \Leftarrow \Pi$ and then $Sol_{\mathcal{D}}(\Pi) \not\subseteq Sol_{\mathcal{I}}(f\bar{t}_n \rightarrow s)$.

2. $N$ has a children labelled by $\Delta \Leftarrow \Pi$ valid in $\mathcal{I}$. Therefore, $\mathcal{I} \models_{\mathcal{D}} \Delta \Leftarrow \Pi$ and then $Sol_{\mathcal{D}}(\Pi) \subseteq Sol_{\mathcal{I}}(\Delta)$.

3. $N$ has a children labelled by $r \rightarrow s \Leftarrow \Pi$ valid in $\mathcal{I}$. Therefore, $\mathcal{I} \models_{\mathcal{D}} r \rightarrow s \Leftarrow \Pi$ and then $Sol_{\mathcal{D}}(\Pi) \subseteq Sol_{\mathcal{I}}(r \rightarrow s)$.

4. $(f\bar{t}_n \rightarrow r \Leftarrow \Delta) \in [\mathcal{P}]_{\perp}$. Therefore, by definition of $[\mathcal{P}]_{\perp}$, there exists a constrained program rule $(f\bar{t}_n \rightarrow r' \Leftarrow \Delta') \in \mathcal{P}$ and a substitution $\theta \in Sub_{\perp}(U)$ such that $(f\bar{t}_n \rightarrow r' \Leftarrow \Delta') \theta \equiv (f\bar{t}_n \rightarrow r \Leftarrow \Delta) \in [\mathcal{P}]_{\perp}$. Let $\eta \in Sol_{\mathcal{I}}(\Pi)$. Then, according to items 2 and 3, $\eta \in Sol_{\mathcal{I}}(\Delta)$ (or equivalently by item 4, $\theta \eta \in Sol_{\mathcal{I}}(\Delta')$) and $\eta \in Sol_{\mathcal{I}}(r \rightarrow s)$ (or equivalently by item 4, $\eta \in Sol_{\mathcal{I}}(r' \theta \rightarrow s)$). By Definition 1, we have $\mathcal{I} \models_{\mathcal{D}} \Delta \eta$ (or equivalently by item 4, $\mathcal{I} \models_{\mathcal{D}} \Delta' \theta \eta$) and $\mathcal{I} \models_{\mathcal{D}} r \eta \rightarrow s \eta$ (or equivalently by item 4, $\mathcal{I} \models_{\mathcal{D}} r' \theta \eta \rightarrow s \eta$). Since $\eta$ is a valuation, $\theta \eta \in Sub_{\perp}(U)$ is a ground substitution, $s \eta \in Pat_{\perp}(U)$ is a ground pattern and $(f\bar{t}_n \rightarrow r' \Leftarrow \Delta') \theta \eta$ is ground. In this situation, if we suppose that the constrained program rule $(f\bar{t}_n \rightarrow r' \Leftarrow \Delta') \in \mathcal{P}$ is valid in $\mathcal{I}$, according to item 1 in Definition 2, we obtain $\mathcal{I} \models_{\mathcal{D}} (f\bar{t}_n \eta) \theta \eta \rightarrow s \eta$ (or equivalently by item 4, $\mathcal{I} \models_{\mathcal{D}} (f\bar{t}_n \eta) \theta \eta \rightarrow s \eta$), and then $\eta \in Sol_{\mathcal{I}}(f\bar{t}_n \rightarrow s \eta)$. But then, $Sol_{\mathcal{D}}(\Pi) \not\subseteq Sol_{\mathcal{I}}(f\bar{t}_n \rightarrow s)$ and we have a contradiction with item 1. So, the $f$’s constrained program rule $(f\bar{t}_n \rightarrow r' \Leftarrow \Delta')$ in $\mathcal{P}$ is incorrect in $\mathcal{I}$. \hfill \Box