

# Operational semantics for Prolog with Cut in Rocq and its application to determinacy analysis

Jane Open Access   

Dummy University Computing Laboratory, [optional: Address], Country

My second affiliation, Country

Joan R. Public<sup>1</sup>  

Department of Informatics, Dummy College, [optional: Address], Country

---

## Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent convallis orci arcu, eu mollis dolor. Aliquam eleifend suscipit lacinia. Maecenas quam mi, porta ut lacinia sed, convallis ac dui. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse potenti.

**2012 ACM Subject Classification** Replace ccsdesc macro with valid one

**Keywords and phrases** Dummy keyword

**Digital Object Identifier** 10.4230/LIPIcs.CVIT.2016.23

**Funding** *Jane Open Access:* (Optional) author-specific funding acknowledgements

*Joan R. Public:* [funding]

**Acknowledgements** I want to thank ...

## 1 Introduction

ELPI is a dialect of  $\lambda$ PROLOG (see [14, 15, 7, 12]) used as an extension language for the ROCQ prover (formerly the COQ proof assistant). ELPI has become an important infrastructure component: several projects and libraries depend on it [13, 3, 4, 19, 8, 9]. Examples include the Hierarchy-Builder library-structuring tool [5] and Derive [17, 18, 11], a program-and-proof synthesis framework with industrial applications at SkyLabs AI.

Starting with version 3, ELPI gained a static analysis for determinacy [10] to help users tame backtracking. ROCQ users are familiar with functional programming but not necessarily with logic programming and uncontrolled backtracking is a common source of inefficiency and makes debugging harder. The determinacy checkers identifies predicates that behave like functions, i.e., predicates that commit to their first solution and leave no *choice points* (places where backtracking could resume).

This paper reports our first steps towards a mechanization, in the ROCQ prover, of the determinacy analysis from [10]. We focus on the control operator *cut*, which is useful to restrict backtracking but makes the semantic depart from a pure logical reading.

We formalize two operational semantics for PROLOG with cut. The first is a stack-based semantics that closely models ELPI's implementation and is similar to the semantics mechanized by Pusch in ISABELLE/HOL [16] and to the model of Debray and Mishra [6, Sec. 4.3]. This stack-based semantics is a good starting point to study further optimizations used by standard PROLOG abstract machines [20, 1], but it makes reasoning about the scope of *cut* difficult. To address that limitation we introduce a tree-based semantics in which the branches pruned by *cut* are explicit and we prove the two semantics equivalent. Using the

---

<sup>1</sup> Optional footnote, e.g. to mark corresponding author



```

Inductive P := IP of nat. Inductive D := ID of nat. Inductive V := IV of nat.

Inductive Tm :=
  | Tm_P of P
  | Tm_D of D
  | Tm_V of V
  | Tm_App of Tm & Tm.
Inductive Callable :=
  | Callable_P of P
  | Callable_App of Callable & Tm.

```

■ **Figure 1** Tm and Callable types

tree-based semantics we then show that if every rule of a predicate passes the determinacy analysis, the call to a deterministic predicate does not leave any choice points.

## 2 Common code: the language

put unif and pro  
gram in variable  
hides from types

Before going to the two semantics, we show the piece of data structure that are shared by the them. The smallest unit of code that we can use in the language is an atom. The atom inductive (see Type 1) is either a cut or a call. A call carries a callable term (see Figure 1). A term (Tm) is either a predicate, a datum, a variable or the binary application of a term to another. A Callable is a term accepting predicates only predicates as functors.

**Inductive** A := cut | call : Callable → A. (1)

**Record** R := mkR { head : Callable; premises : list A }. (2)

**Record** P := { rules : seq R; sig : sigT }. (3)

**Definition** Σ := {fmap V → Tm}. (4)

**Definition** bc : Unif → P →  $\mathcal{F}$  → Callable →  
Σ →  $\mathcal{F}$  \* seq (Σ \* seq A) := (5)

!!!: controllare il  
tipo di bc nel  
testo

A rule (see Type 2) is made a head of type term and a list of premises, the premises are atoms. A program (see Type 3) is made by a list of rules and a mapping from predicates to their signatures. The type sigT is the classic type from the simply typed lambda calculus, i.e. it is either a base type or an arrow. We decorate arrows to know the mode of the lhs type.

A substitution (see Type 4) is a mapping from variables to terms. It is the output of a successful query and is often called the output of a query.

```

Record Unif := {
  unify : Tm → Tm → Σ → option Σ;
  matching : Tm → Tm → Σ → option Σ;
}.

```

The backchain function (bc, see Type 5) filters the rules in the program that can be used on a given query. It takes: a unificator  $U$  which explains how to unify terms up to standard unification (for output terms) or matching (for input terms); a program  $P$  to explore and filter; a set  $S$  of free variable (fvS) allowing to fresh the program  $P$  by renaming the its variables; a query  $q$ ; and the substitution  $\sigma$  in which the query  $q$  lives. The result of a backchain operation is couple made of an extension of  $S$  containing the new variables that have been allocated during the unification phase and a list of filtered rules  $r$  accompagnate by their a substitution. This substitution is the result of the unification of  $q$  with the head of each rule in  $r$ .

In Figure 2, we have an example of a simple ELPI program which will be used in the following section of the paper as an example to show how backtracking and the cut operator works in the semantics we propose. The translation of these rules in the ROCQ representation is straightforward.

```

f 1 2.    f 2 3.    r 2 4.    r 2 8.
g X X.                                % r1
g X Z :- r X Z, !.                    % r2
g X Z :- f X Y, f Y Z.                % r3

```

■ **Figure 2** Small ELPI program example

## 2.1 The cut operator

The semantics of the cut operator adopted in the ELPI language corresponds to the *hard cut* operator of standard SWI-PROLOG. This operator has two primary purposes. First, it eliminates all alternatives that are created either simultaneously with, or after, the introduction of the cut into the execution state.

To illustrate this high-level description, consider the program shown in Figure 2 and the query  $q = g \ 2 \ Z$ . All three rules for  $g$  can be used on the query  $q$ . They are tried according to their order of appearance in the program: rule  $r_1$  is tried first, followed by  $r_2$ , and  $r_3$ .

The first rule has no premises and immediately returns the assignment  $Z = 2$ . However, the computation does not terminate at this point, since two additional unexplored alternatives remain, corresponding to the premises of rules  $r_2$  and  $r_3$ .

The premises of rule  $r_2$  are  $r \ 2 \ Z, !$ . At this stage, the role of the cut becomes apparent. If the premise  $r \ 2 \ Z$  succeeds, the cut commits to this choice and removes the premises of rule  $r_3$  from the alternative list, as they were generated at the same point as the cut. Moreover, if the call  $r \ 2 \ Z$  itself produces multiple alternatives, only the first one is committed, while the remaining alternatives are discarded. This is because such alternatives have been created at a deeper depth in the search tree than the cut.

Concretely, the call  $r \ 2 \ Z$  yields two solutions, assigning  $Z$  the values 4 and 8, respectively. The second solution is eliminated by the cut, and only the first assignment is preserved.

## 3 Semantics intro

We propose two operational semantics for a logic program with cut. The two semantics are based on different syntaxes, the first syntax (called *tree*) exploits a tree-like structure and is ideal both to have a graphical view of its evolution while the state is being interpreted and to prove lemmas over it. The second syntax, called *elpi*, is the ELPI's syntax and has the advantage of reducing the computational cost of cutting and backtracking alternatives by using shared pointers. We aim to prove the equivalence of the two semantics together with some interesting lemmas of the cut behavior.

## 4 Tree semantics

```

Inductive tree :=
| KO | OK | TA of A
| Or of option tree & Σ & tree
| And of tree & seq A & tree.

```

In the tree we distinguish 5 main cases:  $KO$ ,  $OK$ , and are special meta-symbols representing, respectively, the failed and a successful terminal. These symbols are considered meta because they are internal intermediate symbols used to give structure to the tree.

The  $TA$  constructor (acronym for tree-atom) is the constructor of atoms in the tree.

se metti  $r1 = g \ A$   
 $B :- f \ A \ B$ . allora  
 $g \ e \ f$  sono fun-  
 zioni, e puoi spie-  
 gare anche l'idea  
 del detcheck qui

$TA = \text{Todo/-}$   
 Goal?

```

Fixpoint get_end s A :  $\Sigma$  * tree :=
  match A with
  | TA _ | KO | OK  $\Rightarrow$  (s, A)
  | Or None s1 B  $\Rightarrow$  get_end s1 B
  | Or (Some A) _  $\Rightarrow$  get_end s A
  | And A _ B  $\Rightarrow$ 
    let (s', pA) := get_end s A in
    if pA == OK then get_end s' B
    else (s', pA)
  end.

Definition get_subst s A := (get_end s A).1.
Definition path_end A := (get_end  $\epsilon$  A).2. (*~ $\epsilon$ ~ is the ~ $\epsilon$ ~ subst*)
Definition success A := path_end A == OK.
Definition failed A := path_end A == KO.
Definition path_atom A := if path_end A is TA _ then true else

```

■ Figure 3 Definition of *get\_end*

The two recursive cases of a tree are the *Or* and *And* non-terminals. The *Or* non-terminal  $A \vee B_\sigma$  denotes a disjunction between two trees  $A$  and  $B$ . The first branch is optional, if absent it represents a dead tree, i.e. a tree that has been entirely explored. The second branch is annotated with a suspended substitution  $\sigma$  so that, upon backtracking to  $B$ ,  $\sigma$  is used as the initial substitution for the execution of  $B$ .

The *And* non-terminal  $A \wedge_{B_0} B$  represents a conjunction of two trees  $A$  and  $B$ . We call  $B_0$  the reset point for  $B$ ; it is used to restore the state of  $B$  to its initial form if a backtracking operation occurs on  $A$ . Intuitively, let  $t2l$  be the function flattening a tree in a list of sequents disjunction, in PROLOG-like syntax the tree  $A \wedge_{B_0} B$  becomes  $(A_1, t2l B); (A_2, B_0); \dots; (A_n, B_0)$  where  $t2l(A) = A_1, \dots, A_n$ .

A graphical representation of a tree is shown in Figure 4a. To make the graph more compact, the *And* and *Or* non-terminals are n-ary rather than binary, with right-binding priority. The *KO* terminal act as the neutral elements in the *Or* list, while *OK* is the neutral element of the *And* list.

The interpretation of a tree is performed by two main routines: *step* and *next\_alt* that traverse the tree depth-first, left-to-right. Then, then *run* inductive makes the transitive closure of step *step* and *next\_alt*: it iterates the calls to its auxiliary functions. In Types 7–9 we give the types contrats of these symbols where *fvS* is a set of variable names.

**Inductive** tag := Expanded | CutBrothers | Failed | Success. (6)

**Definition** step :  $\mathbb{P} \rightarrow \mathcal{F} \rightarrow \Sigma \rightarrow \text{tree} \rightarrow (\mathcal{F} * \text{tag} * \text{tree}) :=$  (7)

**Definition** next\_alt :  $\mathbb{B} \rightarrow \text{tree} \rightarrow \text{option tree} :=$  (8)

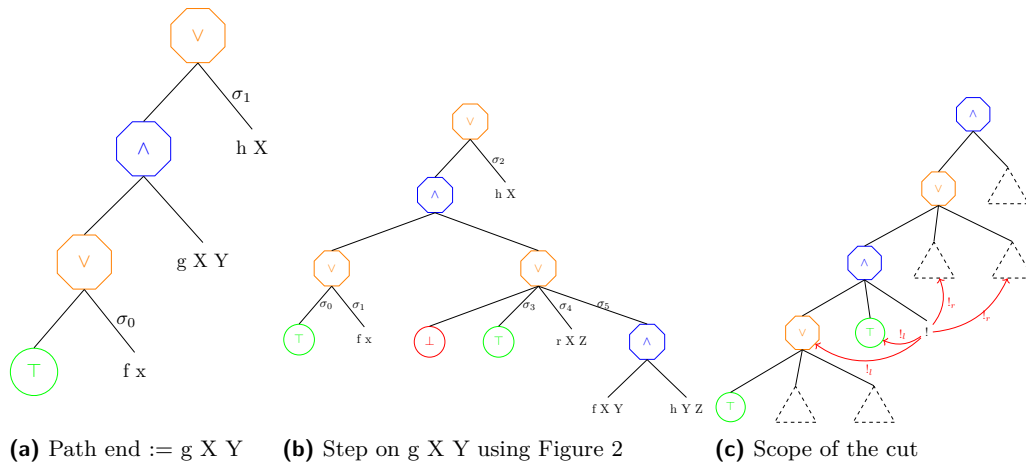
**Inductive** run (u:Unif) (p :  $\mathbb{P}$ ):  $\mathcal{F} \rightarrow \Sigma \rightarrow \text{tree} \rightarrow \Sigma \rightarrow \text{option tree} \rightarrow \text{Prop} :=$  (9)

The tree interpreter, as in prolog, explores the state in DFS strategy, to discover the substitution and the leaf of the tree that should be interpreted. The *get\_end* routine, shown in Figure 3, accomplishes to this task. The *get\_end* returns its inputs if the tree is a leaf. Otherwise, if the tree is a disjunction, the path continues on the left subtree, if it exists, otherwise it recursively retrieves the wanted piece of information in the rhs using the substitution stored in the *Or* branch: the current substitution when we cross the rhs of a *Or* is the one store in the *Or* node itself. In the case of a conjunction, if the to-be-explored leaf in the lhs is *OK*, then we look for the *get\_end* in the rhs, otherwise we return the result of the lhs.

We derive the following two functions from *get\_end*:

**Definition** get\_subst s A := (get\_end s A).1. (1)

**Definition** path\_end A := (get\_end  $\epsilon$  A).2. (\*~ $\epsilon$ ~ is the ~ $\epsilon$ ~ subst\*) (2)



■ **Figure 4** Some tree representations

138 In Figure 4a the *path\_end* of the tree is *g X Y*.

139 Below we define three special kinds of trees depending on their *path\_end*.

140 **Definition**  $\text{success } A := \text{path\_end } A == \text{OK}.$  (3)

141 **Definition**  $\text{failed } A := \text{path\_end } A == \text{KO}.$  (4)

142 **Definition**  $\text{path\_atom } A := \text{if path\_end } A \text{ is TA } \_ \text{ then true else false}.$  (5)

143 The latter definition identifies path ending in an atom.

#### 144 4.1 The *step* procedure

145 The *step* procedure takes as input a program, a set of free variables (fv), a substitution, and  
146 a tree, and returns an updated set of free variables, a *step\_tag*, and an updated tree.

147 Free variables are those variables that appear in a tree; they are used and updated when  
148 a backchaining operation takes place.

149 The *step\_tag* (see Type 6) indicates the kind of an internal tree step: **CutBrothers** denotes  
150 the interpretation of a superficial cut, i.e., a cut whose parent nodes are all *And*-nodes.  
151 **Expanded** denotes the interpretation of non-superficial cuts or predicate calls. **Failure** and  
152 **Success** are returned for, respectively, *failed* and *success* trees.

153 The step procedure is intended to interpretate atoms, that is, it transforms the tree iff its  
154 *path\_end* is an atom, otherwise, it returns the identity.

155 **Lemma**  $\text{succ\_step\_iff } u \text{ p fv s } A: \text{success } A \leftrightarrow \text{step } u \text{ p fv s } A = (\text{fv}, \text{Success}, A).$  (1)

156 **Lemma**  $\text{fail\_step\_iff } u \text{ p fv s } A: \text{failed } A \leftrightarrow \text{step } u \text{ p fv s } A = (\text{fv}, \text{Failed}, A).$  (2)

157 *Call step* The interpretation of a call *c* starts by calling the *bc* function on *c*. The output  
158 list *l* is taken to represent build the new subtree. If *l* is empty then *KO* tree is returned,  
159 otherwise the subtree is a right-skewed tree made of *n* inner *Or* nodes, where *n* is the length  
160 of *l*. The root has *KO* as left child. The lhs of the other nodes is a right-skewed tree of *And*  
161 nodes. The *And* nodes are again a right-seked tree containing premises of the selected rule.

162 A step in the tree of Figure 4a makes a backchain operation over the query *g X Y* and, in  
163 the program defined in Figure 2, the new tree would be the one in Figure 4b. We have put a  
164 red border around the new generated subtree. It is a disjunction of four subtrees: the first  
165 node is the *KO* node (by default), the second is *OK*, since *r1* has no premises, the third and  
166 the fourth contains the premises of respectively *r2* and *r3*.

dire dei reset  
point

dire che le  
sostituzioni del  
backchain sono  
importanti e

167 *Cut step* The cut case is delicate, since interpreting a cut in a tree has three main impacts:  
 168 at first the cut is replaced by the *OK* node, then some special subtrees, in the scope of the  
 169 *Cut*, are cut away: in particular we need to soft-kill the left-siblings of the *Cut* and hard-kill  
 170 the right-uncles of the the *Cut*.

171 ► **Definition 1** (Left-siblings (resp. right-sibling)). *Given a node  $A$ , the left-siblings (resp.*  
 172 *right-sibling) of  $A$  are the list of subtrees sharing the same parent of  $A$  and that appear on*  
 173 *its left (resp. right).*

174 ► **Definition 2** (Right-uncles). *Given a node  $A$ , the right-uncles of  $A$  are the list of right-sibling*  
 175 *of the father of  $A$ .*

176 ► **Definition 3** (Hard-kill,  $!_r$ ). *Given a tree  $t$ , hard-kill replaces the given subtree with the*  
 177 *KO node*

178 ► **Definition 4** (Soft-kill,  $!_l$ ). *Given a successful tree  $t$ , soft-kill replaces with KO all subtrees*  
 179 *that are not part of the path in  $t$  leading to the OK node.*

180 An example of the impact of the cut is show in Figure 4c, the dashed triangles represent  
 181 generic trees. The step routine interprets the cut since it is the node in its path-end: we pass  
 182 through a and and all trees on the left of the cut are successful. In the example we have 4  
 183 arrow tagged with the  $!_l$  or  $!_r$  symbols. The  $!_l$  arrows go left and soft-kill the pointed subtree,  
 184 it keeps *OK* nodes since they are part of the tree leading to the cut, and replaces the other  
 185 subtrees with *KO*. The  $!_r$  procedure replaces the nodes pointed by the arrows with *KO*.

## 186 4.2 The *next\_alt* procedure

187 It is evident that the *step* alone is not sufficient to reproduce entirely the behavior of the full  
 188 expected prolog interpreter. In particular, we need to bracktrack on failures. Moreover, in  
 189 case of success, we should return a state where the state is cleaned of the success itself, this  
 190 is essential to, non deterministically, find all the solution of a given query. By Lemmas 1  
 191 and 2, we know that *step* returns the identity on successful and failed states. In order to  
 192 continue the computation on these particular trees, we need the *next\_alt* procedure aiming  
 193 to expecially work with failed and successful trees: and its implementation in Figure 5.

194 The *next\_alt* procedure takes a boolean and a tree, clean it from failures or success and  
 195 returns a new tree if this tree still contains a non explored path. The idea behind *next\_alt* is  
 196 to clean recursively every subtree in DFS order if its *path\_end* is a failure. Moreover, if the  
 197 boolean passed to *next\_alt* is true, then it erases the first successful path in the tree.

198 The base cases of *next\_alt* are immediate. The *Or* case is rather intuitive: if the lhs  
 199 of the *Or* does not exist we look for the *next\_alt* in the rhs. Otherwise, we look for the  
 200 *next\_alt* in the lhs, if this *next\_alt* does not exists, we look for the *next\_alt* in the rhs.

201 We want to spend few words about the *And* case, since the reset point  $B0$  for  $B$  plays an  
 202 important role. The *next\_alt* in an *And* tree should consider two cases: if the lhs succeeds,  
 203 then the *next\_alt* should be retrived in the rhs. If this alternative does not exists it means  
 204 that the rhs has entirely been explored. We need to erase the success in the lhs and try to  
 205 find if a non-explored alternative exists. If so, we return a new tree with the new lhs and the  
 206 rhs is built from the reset point. **big\_and** is a trivial function build a right-skewed tree of  
 207 and nodes where the leaves are the atoms written in the reset point. We need to reuse the  
 208 reset point since, the step procedure in *And* trees evaluates the rhs of a *And* tree if the lhs  
 209 succeeds. This evaluation is dependent on the substitution in the lhs tree. Therefore, if we  
 210 need to backtrack in the lhs, we need to reset the rhs.

```

Definition next_alt :  $\mathbb{B} \rightarrow \text{tree} \rightarrow \text{option tree} :=
  \text{fix next\_alt } b \ A :=
    \text{match } A \text{ with}
    | KO \Rightarrow \text{None}
    | OK \Rightarrow \text{if } b \text{ then None else Some OK}
    | TA _ \Rightarrow \text{Some } A
    | And A BO B \Rightarrow
      \text{let build\_BO } A := \text{And } A \text{ BO } (\text{big\_and } BO) \text{ in}
      \text{if success } A \text{ then}
        \text{match next\_alt } b \ B \text{ with}
        | None \Rightarrow \text{omap build\_BO } (\text{next\_alt true } A)
        | Some B' \Rightarrow \text{Some } (\text{And } A \text{ BO } B')
      \text{end}
      \text{else if failed } A \text{ then omap build\_BO } (\text{next\_alt false } A)
      \text{else Some } (\text{And } A \text{ BO } B)
    | Or None sB B \Rightarrow \text{omap } (\text{fun } x \Rightarrow \text{Or None sB } x) (\text{next\_alt } b \ B)
    | Or (Some A) sB B \Rightarrow
      \text{match next\_alt } b \ A \text{ with}
      | None \Rightarrow \text{omap } (\text{fun } x \Rightarrow \text{Or None sB } x) (\text{next\_alt false } B)
      | Some A' \Rightarrow \text{Some } (\text{Or } (\text{Some } A') \text{ sB } B)
    \text{end}
  \text{end.}$ 
```

■ **Figure 5** *next\_alt* implementation

Some interesting property of *next\_alt* are shown below and allow to see how *next\_alt* complements *step*.

**Lemma** *path\_atom\_next\_alt\_id*  $b \ A$ :  $\text{path\_atom } A \rightarrow \text{next\_alt } b \ A = \text{Some } A$ . (3)

**Lemma** *next\_alt\_failedF*  $b \ A \ A'$ :  $\text{next\_alt } b \ A = \text{Some } A' \rightarrow \text{failed } A' = \text{false}$ . (4)

For example, in Figure 4b the step procedure has created a failed state: its path-end ends in *KO*. The expected behavior of *next\_alt* is to take this *KO* node and make it a .... This allows *step* to continue the exploration of the tree. In particular, the path-end of this new state end in *OK*. The step leaves the state unchanged producing the new substitution. This solution however is not unique, we should be able to backtrack on this successful state. To do so we can call *next\_alt* and it will deadify the *OK* node allowing *step* to proceed on  $r \ X \ Z$ .

subst taken from  
the or

### 4.3 The *run* inductive

The inductive procedure *run* is modeled as a function: it takes as input a program, a set of free variables, an initial substitution  $\sigma_0$ , and a tree  $t_0$ , and returns a substitution  $\sigma_1$  together with an optional updated tree  $t_1$ . The substitution  $\sigma_1$  represents the most-general unificator that makes the execution of the tree  $t_0$  succeed starting from the initial substitution  $\sigma_0$ ,  $\sigma_1$  is an extension of  $\sigma_0$ . The tree  $t_1$  is the updated tree containing the alternatives that have not yet been explored. If the tree contains no solution, then *None* is returned.

The procedure *run* is based on three main derivation rules, shown in Figure 6. If the *path\_end* of the tree  $t$  is a success, the input substitution is returned and the input tree is cleaned of its successful path. If the *path\_end* of the tree is an atom, then *step* is invoked to evaluate this atom, and *run* is recursively called on the new tree. Finally, if the *path\_end* of the tree is a failure, *next\_alt* is called to clear the failed path; if the resulting cleaned tree exists, *run* is recursively called on it.

$$\begin{array}{c}
\frac{}{\text{success } A \rightarrow \text{get\_subst } s1 \ A = s2 \rightarrow (\text{next\_alt true } A) = B \rightarrow \text{run } fv \ s1 \ A \ s2 \ B} \text{RUN\_DONE} \\
\\
\frac{}{\text{path\_atom } A \rightarrow \text{step } u \ p \ fv0 \ s1 \ A = (fv1, st, B) \rightarrow \text{run } fv1 \ s1 \ B \ s2 \ r \rightarrow \text{run } fv0 \ s1 \ A \ s2 \ r} \text{RUN\_STEP} \\
\\
\frac{}{\text{failed } A \rightarrow \text{next\_alt false } A = \text{Some } B \rightarrow \text{run } fv0 \ s1 \ B \ s2 \ r \rightarrow \text{run } fv0 \ s1 \ A \ s2 \ r.} \text{RUN\_FAIL} \\
\\
\frac{\text{success } A}{\text{run } fv \ s1 \ A \ (\text{get\_subst } s1 \ A) \ (\text{next\_alt } \top \ A)} \text{run\_done} \\
\\
\frac{\text{path\_atom } A \quad \text{step } u \ p \ fv0 \ s1 \ A = (fv1, st, B) \quad \text{run } fv1 \ s1 \ B \ s2 \ r}{\text{run } fv0 \ s1 \ A \ s2 \ r} \text{run\_step} \\
\\
\frac{\text{failed } A \quad \text{next\_alt } \perp \ A = \text{Some } B \quad \text{run } fv0 \ s1 \ B \ s2 \ r}{\text{run } fv0 \ s1 \ A \ s2 \ r} \text{run\_fail}
\end{array}$$

■ **Figure 6** Rule system for *run*

#### 234 4.4 Valid trees

235 The inductive tree allows one to generate a large number of trees, some of which are not  
 236 valid, in the sense that they cannot be produced starting from a given query. The class of  
 237 valid trees is characterized by the following function.

```

238 Fixpoint valid_tree s :=
239   match s with
240     | TA _ | OK | KO => true
241     | Or None _ B => valid_tree B
242     | Or (Some A) _ B => valid_tree A && ((B == KO) || B.base_or B)
243     | And A B0 B => valid_tree A &&
244       if success A then valid_tree B
245       else B == big_and B0
246   end.

```

238 Once again, the most interesting cases to analyze are *Or* and *And*.

239 For the *Or* constructor, we distinguish two cases depending on whether the left-hand  
 240 side (lhs) exists. If it does not exist, then the right-hand side (rhs) must be a valid tree.  
 241 Otherwise, the lhs must itself be a valid tree, and the rhs is either the *KO* tree, since it may  
 242 have been removed by the evaluation of a superficial cut in the lhs, or it has not yet been  
 243 explored. In the latter case, it is a *base\_or* tree, namely the right-skewed tree formed by a  
 244 disjunction of conjunctions.

245 For the *And* constructor, the lhs is required to be a valid tree. The shape of the rhs  
 246 depends on whether the lhs represents a success. If the lhs is not successful, then the rhs  
 247 has never been explored: the procedures *step* and *next\_alt* modify the rhs only when the  
 248 lhs succeeds. In this case, the lhs must be the right-skewed tree containing the conjunctions  
 249 of the atoms present in the reset point  $B_0$ . In other words, the rhs coincides with the reset  
 250 point. If the lhs is a success tree, then the rhs must be a valid tree.

**Definition**  $\text{stepE } \text{fv } t \text{ s } a \text{ gl} :=$   
 $\text{let } (\text{fv}', \text{rs}) := \text{bc up fv } t \text{ s } \text{ in}$   
 $\text{let } \text{rs\_ca} := \text{save\_alts } a \text{ gl } (\text{r2a rs}) \text{ in}$   
 $(\text{fv}', \text{rs\_ca}).$

**Inductive**  $\text{nur} : \mathcal{F}_v \rightarrow \Sigma \rightarrow \text{goals} \rightarrow \text{alts} \rightarrow \Sigma \rightarrow \text{alts} \rightarrow \text{Prop} :=$  (10)

$$\frac{}{\text{nur fv s } [::] \text{ a s a}} \text{STOPE}$$

$$\frac{}{\text{nur fv s gl ca s1 r} \rightarrow \text{nur fv s } [:: (\text{cut}, \text{ca}) \& \text{gl}] \text{ a s1 r}} \text{CUTE}$$

$$\frac{}{\text{stepE fv } t \text{ s } a \text{ gl} = (\text{fv}', [:: \text{b} \& \text{bs}]) \rightarrow \text{nur fv' b.1 b.2 (bs++al)} \text{ s1 r} \rightarrow \text{nur fv s } [:: (\text{call } t, \text{ca}) \& \text{gl}] \text{ al s1 r}} \text{CALLE}$$

$$\frac{}{\text{stepE fv } t \text{ s } a \text{ gl} = (\text{fv}', [::]) \rightarrow \text{nur fv' s1 a al s2 r} \rightarrow \text{nur fv s } [:: (\text{call } t, \text{ca}) \& \text{gl}] [:: (\text{s1}, \text{a}) \& \text{al}] \text{ s2 r.}} \text{FAILE}$$

■ **Figure 7** Rule system for *nur*

## 5 Elpi semantics

We now want to introduce the elpi semantics. The interpreter we show reflects the interpreter of the ELPI language and is an operational semantics close to the one picked by Pusch in [16], in turn closely related to the one given by Debray and Mishra in [6, Section 4.3]. Pusch mechanized the semantics in Isabelle/HOL together with some optimizations that are present in the Warren Abstract Machine [20, 1].

The inductive representing a state of the ELPI language is shown below.

**Inductive**  $\text{alts} := \text{no\_alt} \mid \text{more\_alt of } (\Sigma * \text{goals}) \& \text{alts}$   
**with**  $\text{goals} := \text{no\_goals} \mid \text{more\_goals of } (A * \text{alts}) \& \text{goals} .$

An elpi state is an enhanced two-dimension list. The outermost list represents the list of alternatives in disjunction accompagnate with the substitution that should be used to for their interpretation. The innermost list is a list of atom, representing a list of goals in conjunctions. These goals are decorated with a pointer to an elpi state, and are used to keep trace of the alternatives that should be kept when a cut is interpreted. We call these, special, alternatives the cut-to alternatives.

The idea of the ELPI interpreter is to receive a list of alternatives. The first alternative consists of a list of goals. Four cases must be taken into account; they are shown in Figure 7. In order to simplify goal retrieval, we split the head of the alternatives from the tail, so that it can be immediately matched in the inductive definition. Note that an empty list of alternatives represents, by definition, a failing state. If the goal list is empty (STOPE), then we have, by definition, a success, and the input solution together with the list of alternatives is returned. If the goal list starts with a cut (CUTE), then the current alternatives are erased in favour of the cut alternatives, and a recursive call is made on the remaining goal list.

Finally, we must consider the case in which the goal list starts with a call. The call can either fail (FAILE) or succeed (CALLE). We distinguish the two cases by looking if the backchaining operation returns zero or more rules. We have wrapped this task in the *stepE*

275 procedure, which also updates the goal and cut-alternative list. The fail case, is relatively  
 276 easy: the first goal does not succeed, we need to take the head of the alternatives, and make  
 277 it the new list of goals to be explored.

278 The case in which backchaining produces a non empty list, the *save\_alts* routine is in  
 279 cahrg of: taking the list of premises and add to each atom the the list of alternatives *a* as  
 280 their new cut-alternatives, then it append the list of goals *gl* to each of these new lists.

## 281 **6 Semantic equivalence**

282 The equivalence between the two semantics is possible under two conditions: we need to  
 283 work with "valid states", i.e. state that can be generated from a query of type call.

### 284 **6.1 From trees to lists**

285 The translation of a tree to a list is as follows:

```

Fixpoint t2l (A: tree) s (bt : alts) : alts :=
  match A with
  | OK          => [:: (s, [::])] ]
  | KO          => [::]
  | TA a        => [:: (s, [:: (a,[::]) ]) ]
  | Or None s1 B => add_ca_deep bt (t2l B s1 [::])
  | Or (Some A) s1 B =>
    let lB := t2l B s1 [::] in
    let lA := t2l A s lB in
    add_ca_deep bt (lA ++ lB)
  | And A B0 B =>
    let lA := t2l A s bt in
    if lA is [:: (slA, x) & xs] then
      let lB0 := a2g B0 in
      let xz := add_deepG bt lB0 x in
      let xs := add_deep bt lB0 xs in
      let xs := map (catr lB0) xs in
      let lB := t2l B slA (xs ++ bt) in
      (map (catl xz) lB) ++ xs
    else [::]
  end.

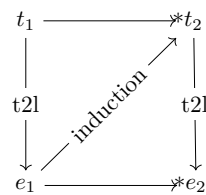
```

► **Theorem 5** (*tree\_to\_elpi*).

$$\begin{aligned}
 & \forall A \sigma_1 B \sigma_2 b \sigma_0, \text{vt } A \rightarrow \\
 & \text{run}_u \sigma_1 A (\text{Some } \sigma_2) B b \rightarrow \\
 & \exists x \text{ xs}, \text{t2l } A \sigma_1 \emptyset = x :: \text{xs} \wedge \text{nur}_u x.1 \text{ x.2 xs } \sigma_2 (\text{t2l } B \sigma_0 \emptyset).
 \end{aligned}$$

► **Theorem 6** (*elpi\_to\_tree*).

$$\begin{aligned}
 & \forall \sigma_1 \sigma_2 a \text{ na } g, \\
 & \text{nur}_u \sigma_1 g a \sigma_2 \text{ na} \rightarrow \\
 & \forall \sigma_0 t, \text{vt } t \rightarrow (\text{t2l } t \sigma_0 \emptyset) = ((\sigma_1, g) :: a) \rightarrow \\
 & \exists t' n, \text{run}_u \sigma_0 t (\text{Some } \sigma_2) t' n \wedge \text{t2l } t' \sigma_0 \emptyset = \text{na}.
 \end{aligned}$$



■ **Figure 8** Induction scheme for Theorem 6

The proof of Theorem 6 is based on the idea explained in [2, Section 3.3]. An ideal statement for this lemma would be: given a function  $12t$  transforming an elpi state to a tree, we would have that the execution of an elpi state  $e$  is the same as executing  $run$  on the tree resulting from  $12t(e)$ . However, it is difficult to retrieve the structure of an elpi state and create a tree from it. This is because, in an elpi state, we have no clear information about the scope of an atom inside the list and, therefore, no evident clue about where this atom should be placed in the tree.

Our theorem states that, starting from a valid state  $t$  which translates to a list of alternatives  $(\sigma_1, g) :: a$ . If we run in elpi the list of alternatives, then the execution of the tree  $t$  returns the same result as the execution in elpi. The proof is performed by induction on the derivations of the elpi execution. We have 4 derivations.

We have 4 cases to analyse:

## 7 Case study: determinacy analysis

we mechanize the first order part of xxx.

snippet det, main thm, invariant det tree (valid tree prev section?)

proof induction on exec, step/next alt preserving invariant proved by induction on the tree.

with list semantics cut and next alt requires to express a link between the ca or next alts and the current goal, which is non trivial without an intermediate data structure like the tree

## 8 Related work

prolog semantics, King lost

yves for the proof technique

## 9 Conclusion

### References

- 1 Hassan Ait-Kaci. *Warren's Abstract Machine: A Tutorial Reconstruction*. The MIT Press, 08 1991. doi:10.7551/mitpress/7160.001.0001.
- 2 Yves Bertot. A certified compiler for an imperative language. Technical Report RR-3488, INRIA, September 1998. URL: <https://inria.hal.science/inria-00073199v1>.
- 3 Valentin Blot, Denis Cousineau, Enzo Crance, Louise Dubois de Prisque, Chantal Keller, Assia Mahboubi, and Pierre Vial. Compositional pre-processing for automated reasoning in dependent type theory. In Robbert Krebbers, Dmitriy Traytel, Brigitte Pientka, and Steve Zdancewic, editors, *Proceedings of the 12th ACM SIGPLAN International Conference on*

- 325 *Certified Programs and Proofs, CPP 2023, Boston, MA, USA, January 16-17, 2023*, pages  
326 63–77. ACM, 2023. doi:10.1145/3573105.3575676.
- 327 **4** Cyril Cohen, Enzo Crance, and Assia Mahboubi. Trocq: Proof transfer for free, with or  
328 without univalence. In Stephanie Weirich, editor, *Programming Languages and Systems*, pages  
329 239–268, Cham, 2024. Springer Nature Switzerland.
- 330 **5** Cyril Cohen, Kazuhiko Sakaguchi, and Enrico Tassi. Hierarchy Builder: Algebraic hierarchies  
331 Made Easy in Coq with Elpi. In *Proceedings of FSCD*, volume 167 of *LIPICs*, pages 34:1–34:21,  
332 2020. URL: [https://drops.dagstuhl.de/entities/document/10.4230/LIPICs.FSCD.2020.](https://drops.dagstuhl.de/entities/document/10.4230/LIPICs.FSCD.2020.34)  
333 [34](https://drops.dagstuhl.de/entities/document/10.4230/LIPICs.FSCD.2020.34), doi:10.4230/LIPICs.FSCD.2020.34.
- 334 **6** Saumya K. Debray and Prateek Mishra. Denotational and operational semantics for prolog. *J.*  
335 *Log. Program.*, 5(1):61–91, March 1988. doi:10.1016/0743-1066(88)90007-6.
- 336 **7** Cvetan Dunchev, Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. ELPI: fast,  
337 embeddable,  $\lambda$ Prolog interpreter. In *Proceedings of LPAR*, volume 9450 of *LNCS*, pages  
338 460–468. Springer, 2015. URL: <https://inria.hal.science/hal-01176856v1>, doi:10.1007/  
339 978-3-662-48899-7\_32.
- 340 **8** Davide Fissore and Enrico Tassi. A new Type-Class solver for Coq in Elpi. In *The Coq*  
341 *Workshop*, July 2023. URL: <https://inria.hal.science/hal-04467855>.
- 342 **9** Davide Fissore and Enrico Tassi. Higher-order unification for free!: Reusing the meta-  
343 language unification for the object language. In *Proceedings of PPDP*, pages 1–13. ACM, 2024.  
344 doi:10.1145/3678232.3678233.
- 345 **10** Davide Fissore and Enrico Tassi. Determinacy checking for elpi: an higher-order logic program-  
346 ming language with cut. In *Practical Aspects of Declarative Languages: 28th International*  
347 *Symposium, PADL 2026, Rennes, France, January 12–13, 2026, Proceedings*, pages 77–95,  
348 Berlin, Heidelberg, 2026. Springer-Verlag. doi:10.1007/978-3-032-15981-6\_5.
- 349 **11** Benjamin Grégoire, Jean-Christophe L  chenet, and Enrico Tassi. Practical and sound equality  
350 tests, automatically. In *Proceedings of CPP*, page 167–181. Association for Computing  
351 Machinery, 2023. doi:10.1145/3573105.3575683.
- 352 **12** Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. Implementing type theory  
353 in higher order constraint logic programming. In *Mathematical Structures in Computer*  
354 *Science*, volume 29, pages 1125–1150. Cambridge University Press, 2019. doi:10.1017/  
355 S0960129518000427.
- 356 **13** Robbert Krebbers, Luko van der Maas, and Enrico Tassi. Inductive Predicates via Least  
357 Fixpoints in Higher-Order Separation Logic. In Yannick Forster and Chantal Keller, editors,  
358 *16th International Conference on Interactive Theorem Proving (ITP 2025)*, volume 352 of *Leib-*  
359 *niz International Proceedings in Informatics (LIPICs)*, pages 27:1–27:21, Dagstuhl, Germany,  
360 2025. Schloss Dagstuhl – Leibniz-Zentrum f  r Informatik. URL: [https://drops.dagstuhl.](https://drops.dagstuhl.de/entities/document/10.4230/LIPICs.ITP.2025.27)  
361 [de/entities/document/10.4230/LIPICs.ITP.2025.27](https://drops.dagstuhl.de/entities/document/10.4230/LIPICs.ITP.2025.27), doi:10.4230/LIPICs.ITP.2025.27.
- 362 **14** Dale Miller. A logic programming language with lambda-abstraction, function variables, and  
363 simple unification. In *Extensions of Logic Programming*, pages 253–281. Springer, 1991.
- 364 **15** Dale Miller and Gopalan Nadathur. *Programming with Higher-Order Logic*. Cambridge  
365 University Press, 2012.
- 366 **16** Cornelia Pusch. Verification of compiler correctness for the wam. In Gerhard Goos, Juris  
367 Hartmanis, Jan van Leeuwen, Joakim von Wright, Jim Grundy, and John Harrison, editors,  
368 *Theorem Proving in Higher Order Logics*, pages 347–361, Berlin, Heidelberg, 1996. Springer  
369 Berlin Heidelberg.
- 370 **17** Enrico Tassi. Elpi: an extension language for Coq (Metaprogramming Coq in the Elpi  $\lambda$ Prolog  
371 dialect). In *The Fourth International Workshop on Coq for Programming Languages*, January  
372 2018. URL: <https://inria.hal.science/hal-01637063>.
- 373 **18** Enrico Tassi. Deriving proved equality tests in Coq-Elpi. In *Proceedings of ITP*, volume 141 of  
374 *LIPICs*, pages 29:1–29:18, September 2019. URL: <https://inria.hal.science/hal-01897468>,  
375 doi:10.4230/LIPICs.CVIT.2016.23.

- 376 19 Luko van der Maas. Extending the Iris Proof Mode with inductive predicates using Elpi.  
377 Master's thesis, Radboud University Nijmegen, 2024. doi:10.5281/zenodo.12568604.
- 378 20 David H.D. Warren. An Abstract Prolog Instruction Set. Technical Report Technical Note 309,  
379 SRI International, Artificial Intelligence Center, Computer Science and Technology Division,  
380 Menlo Park, CA, USA, October 1983. URL: [https://www.sri.com/wp-content/uploads/](https://www.sri.com/wp-content/uploads/2021/12/641.pdf)  
381 2021/12/641.pdf.