

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. Public¹  

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

Abstract

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

12 **2012 ACM Subject Classification** Replace ccsdesc macro with valid one

13 **Keywords and phrases** Dummy keyword

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

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

16 **Joan R. Public:** [funding]

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

1 Introduction

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

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

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

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

¹ Optional footnote, e.g. to mark corresponding author



© Jane Open Access and Joan R. Public;
licensed under Creative Commons License CC-BY 4.0

42nd Conference on Very Important Topics (CVIT 2016).

Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:10

 Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

23:2 Operational semantics for Prolog with Cut in Rocq and its application to determinacy analysis

```

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

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

2 Common code: the language

put unif and progs
gram in variables
hides from types
46 Before going to the two semanticcs, we show the piece of data structure that are shared by
the them. The smallest unit of code that we can use in the langauge 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.

```

48 Inductive A := cut | call : Callable -> A.                               (1)
49 Record R := mkR { head : Callable; premises : list A }.                  (2)
50 Record program := { rules : seq R; sig : sigT }.                         (3)
51 Definition Sigma := {fmap V -> Tm}.                                       (4)
52 Definition bc : Unif -> program -> fvS -> Callable ->
      Sigma -> fvS * seq (Sigma * R) :=                                         (5)

```

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

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

```

Record Unif := {
  unify : Tm -> Tm -> Sigma -> option Sigma;
  matching : Tm -> Tm -> Sigma -> option Sigma;
}.

```

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

68 In Figure 2, we have an example of a simple ELPI program which will be used in the
69 following section of the paper as an example to show how backtracking and the cut operator
70 works in the semantcis we propose. The translation of these rules in the ROCQ representation
71 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

72 2.1 The cut operator

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

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

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

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

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

91 3 Semantics intro

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

99 3.1 Tree semantics

```
Inductive tree :=
| KO | OK | TA : A -> tree
| Or : option tree -> Sigma -> tree -> tree
| And : tree -> seq A -> tree -> tree.
```

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

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

23:4 Operational semantics for Prolog with Cut in Rocq and its application to determinacy analysis

```

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

```

(a) Defintion of *get_end*

104 The two recursive cases of a tree are the *Or* and *And* non-terminals. The *Or* non-terminal
 105 $A \vee B_\sigma$ denotes a disjunction between two trees A and B . The first branch is optional, if
 106 absent it represents a dead tree, i.e. a tree that has been entirely explored. The second
 107 branch is annotated with a suspended substitution σ so that, upon backtracking to B , σ is
 108 used as the initial substitution for the execution of B .

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

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

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

```

122 Inductive step_tag := Expanded | CutBrothers | Failed | Success. (6)
123 Definition step : program -> fvS -> Sigma -> tree -> (fvS * step_tag * tree) := (7)
124 Definition next_alt : bool -> tree -> option tree := (8)
125 Inductive run (u:Unif) (p : program) : fvS -> Sigma -> tree -> (9)
                  Sigma -> option tree -> Prop :=

```

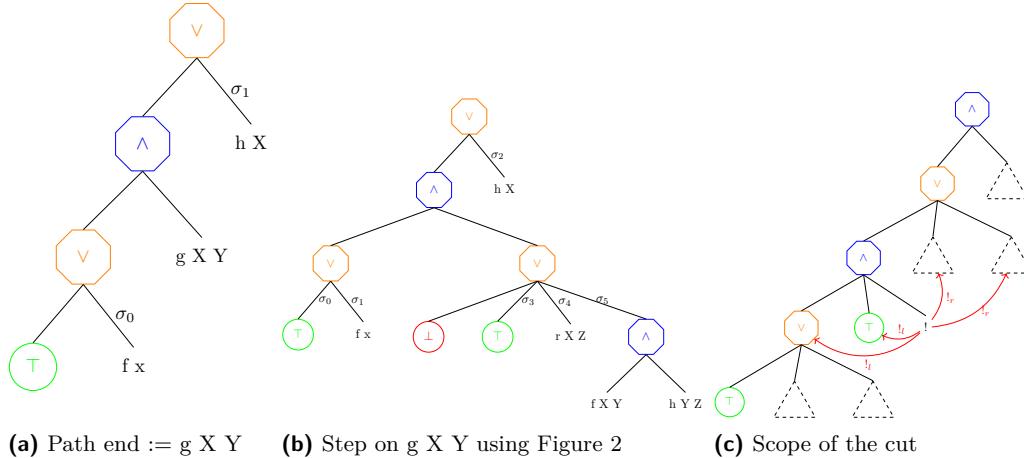
126 The tree interpreter, as in prolog, explores the state in DFS strategy, to discover the
 127 substitution and the leaf of the tree that should be interpreted. The *get_end* routine, shown
 128 in Figure 3a, accomplishes to this task. The *get_end* returns its inputs if the tree is a
 129 leaf. Otherwise,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

135 We derive the following two functions from *get_end*:

```

136 Definition get_subst s A := (get_end s A).1. (1)
137 Definition path_end A := (get_end empty A).2. (*empty is the empty 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** `success A := path_end A == OK.` (3)

141 **Definition** `failed A := path_end A == KO.` (4)

142 **Definition** `path_atom A := if path_end A is TA _ then true else false.` (5)

143 The latter definition identifies path ending in an atom.

144 3.1.1 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, otherwsise, it returns the identity.

155 **Lemma** `succ_step_iff u p fv s A: success A <-> step u p fv s A = (fv, Success, A)`. (1)

156 **Lemma** `fail_step_iff u p fv s A: failed A <-> step u p fv s A = (fv, Failed, A)`. (2)

157 *Call step* The interpretation of a call *c* stars 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 aroung 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

CVIT 2016

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 successfull 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 throgh 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 3.1.2 The *next_alt* procedure

187 It is evident that the *step* alone is not sufficient to reproduce entirely the behavior of the
 188 full ELPI solver. In particular, *step* does not perform any backtracking nor it cleans success.
 189 From Lemmas 1 and 2, *step* returns the identity. In order to continue the computation on
 190 these particular trees, we need the *next_alt* procedure: its signature is provided in Type 8
 191 and its implementation in Figure 5.

192 The *next_alt* procedure takes a boolean and a tree and return a new tree if it still contains
 193 an alternative. The idea behind *next_alt* is to clean recursively remove every subtree in DFS
 194 order if its *path_end* is a failure. Moreover, if the boolean passed to *next_alt* is true, then it
 195 erases the first successful path in the tree.

196 An interesting property of *next_alt* is the following, allowing to see how *next_alt* complements *step*.

198 **Lemma** `path_atom_next_alt_id b A: path_atom A -> next_alt b A = Some A.` (3)

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

205 3.1.3 The *run* inductive

206 The run inductive is nothing but the transitive closure of the *step* and *next_alt*

$$207 \quad \frac{\text{success}A}{\text{run } fv s_1 A (\text{get_subst } s_1 A) (\text{next_alt } \top A)} \text{ run_done}$$

```

Definition next_alt : bool -> tree -> option tree :=
fix next_alt b A :=
match A with
| KO => None
| OK => if b then None else Some OK
| TA _ => Some A
| And A BO B =>
  let build_BO A := And A BO (big_and BO) in
  if success A then
    match next_alt b B with
    | None => omap build_BO (next_alt true A)
    | Some B => Some (And A BO B)
    end
  else if failed A then omap build_BO (next_alt false A)
  else Some (And A BO B)
| Or None sB B => omap (fun x => Or None sB x) (next_alt b B)
| Or (Some A) sB B =>
  match next_alt b A with
  | None => omap (fun x => Or None sB x) (next_alt false B)
  | Some nA => Some (Or (Some nA) sB B)
  end
end.

```

■ **Figure 5** *next_alt* implementation

$$\begin{array}{c}
\frac{\text{path_atom } A \quad step \ u \ p \ fv_0 \ s_1 \ A = (fv_1, \ st, \ B) \quad run \ fv_1 \ s_1 \ B \ s_2 \ r}{run \ fv_0 \ s_1 \ A \ s_2 \ r} \ run_step \\
\\
\frac{\text{failed } A \quad next_alt \bot \ A = \text{Some } B \quad run \ fv_0 \ s_1 \ B \ s_2 \ r}{run \ fv_0 \ s_1 \ A \ s_2 \ r} \ run_fail
\end{array}$$

210 3.1.4 Valid tree

211 Reasoning on a the tree semantics allows to identify an invariant that

212 3.2 Elpi semantics

213 TODO: dire che la semantica ad albero è più facile per le prove

214 The ELPI interpreter is based on an operational semantics close to the one picked by
 215 Pusch in [16], in turn closely related to the one given by Debray and Mishra in [6, Section
 216 4.3]. Push mechanized the semantics in Isabelle/HOL together with some optimizations that
 217 are present in the Warren Abstract Machine [20, 1].

218 In these operational semantics we need to decorate the cut atom with a list of alternative,
 219 morally a pointer to a sub-list of the overall alternatives. An atom in the elpi semantics is
 220 defined as follows:

```

Inductive alts :=
| no_alt
| more_alt : (Sigma * goals) -> alts -> alts
with goals :=
| no_goals
| more_goals : (A * alts) -> goals -> goals .

```

23:8 Operational semantics for Prolog with Cut in Rocq and its application to determinacy analysis

221 We are completely loosing the tree structure. There are no clean reset points. The
 222 backtracking operation is simpler: it is the tail function. The cutr and cutm operations
 223 disappears: the alternatives are stored directly in the cutE terminal.

224 The elpi interpreter is as follows:

```
(*TODO: add system of rules*)
Inductive nur : Sigma -> goals -> alts -> Sigma -> alts -> Type :=
| StopE s a : nur s nilC a s a
| CutE s s1 a ca r gl : nur s gl ca s1 r -> nur s ((cutE ca) :: g1) a s1 r
| CallE p s s1 a b bs gl r t :
  F u p t s = [:: b & bs ] ->
    nur b.1 (save_goals a gl (a2gs1 p b)) (save_alts a gl ((aa2gs p) bs) ++ a) s1 r ->
    nur s ((callE p t) :: g1) a s1 r
| FailE p s s1 s2 t gl a al r :
  F u p t s = [::] -> nur s1 a al s2 r -> nur s ((callE p t) :: g1) ((s1, a) :: al) s2 r.
```

225 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 1B := t2l B s1 [::] in
    let 1A := t2l A s 1B in
    add_ca_deep bt (1A ++ 1B)
  | And A B0 B   =>
    let 1B0 := r2l B0 in
    let 1A := t2l A s bt in
    if 1A is [:: (s1A, x) & xs] then
      let xz := add_deepG bt 1B0 x in
      let xs := add_deep bt 1B0 xs in
      let xs := map (catr 1B0) xs in
      let 1B := t2l B s1A (xs ++ bt) in
      (map (catl xz) 1B) ++ xs
    else [::]
  end.
```

► **Theorem 5** (tree_to_elpi).

226 $\forall A \sigma_1 B \sigma_2 b \sigma_0, vt A \rightarrow$
 227 $\text{run}_u \sigma_1 A (\text{Some } \sigma_2) B b \rightarrow$
 228 $\exists x xs, t2l A \sigma_1 \emptyset = x :: xs \wedge \text{nur}_u x.1 x.2 xs \sigma_2 (t2l B \sigma_0 \emptyset).$

► **Theorem 6** (elpi_to_tree).

229 $\forall \sigma_1 \sigma_2 a na g,$
 230 $\text{nur}_u \sigma_1 g a \sigma_2 na \rightarrow$
 231 $\forall \sigma_0 t, vt t \rightarrow (t2l t \sigma_0 \emptyset) = ((\sigma_1, g) :: a) \rightarrow$
 232 $\exists t' n, \text{run}_u \sigma_0 t (\text{Some } \sigma_2) t' n \wedge t2l t' \sigma_0 \emptyset = na.$

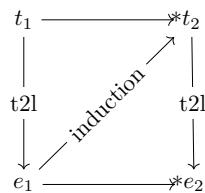


Figure 6 Induction scheme for Theorem 6

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

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

244 We have 4 case to analyse:

245 References

- 246 1 Hassan Aït-Kaci. *Warren's Abstract Machine: A Tutorial Reconstruction*. The MIT Press, 08
 247 1991. doi:10.7551/mitpress/7160.001.0001.
- 248 2 Yves Bertot. A certified compiler for an imperative language. Technical Report RR-3488,
 249 INRIA, September 1998. URL: <https://inria.hal.science/inria-00073199v1>.
- 250 3 Valentin Blot, Denis Cousineau, Enzo Crance, Louise Dubois de Prisque, Chantal Keller,
 251 Assia Mahboubi, and Pierre Vial. Compositional pre-processing for automated reasoning in
 252 dependent type theory. In Robbert Krebbers, Dmitriy Traytel, Brigitte Pientka, and Steve
 253 Zdancewic, editors, *Proceedings of the 12th ACM SIGPLAN International Conference on
 254 Certified Programs and Proofs, CPP 2023, Boston, MA, USA, January 16-17, 2023*, pages
 255 63–77. ACM, 2023. doi:10.1145/3573105.3575676.
- 256 4 Cyril Cohen, Enzo Crance, and Assia Mahboubi. Trocq: Proof transfer for free, with or
 257 without univalence. In Stephanie Weirich, editor, *Programming Languages and Systems*, pages
 258 239–268, Cham, 2024. Springer Nature Switzerland.
- 259 5 Cyril Cohen, Kazuhiko Sakaguchi, and Enrico Tassi. Hierarchy Builder: Algebraic hierarchies
 260 Made Easy in Coq with Elpi. In *Proceedings of FSCD*, volume 167 of *LIPICS*, pages 34:1–34:21,
 261 2020. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.FSCD.2020.34>.
 262 doi:10.4230/LIPIcs.FSCD.2020.34.
- 263 6 Saumya K. Debray and Prateek Mishra. Denotational and operational semantics for prolog. *J.
 264 Log. Program.*, 5(1):61–91, March 1988. doi:10.1016/0743-1066(88)90007-6.
- 265 7 Cvetan Dunchev, Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. ELPI: fast,
 266 embeddable, λ Prolog interpreter. In *Proceedings of LPAR*, volume 9450 of *LNCS*, pages
 267 460–468. Springer, 2015. URL: <https://inria.hal.science/hal-01176856v1>, doi:10.1007/
 268 978-3-662-48899-7_32.
- 269 8 Davide Fissore and Enrico Tassi. A new Type-Class solver for Coq in Elpi. In *The Coq
 270 Workshop*, July 2023. URL: <https://inria.hal.science/hal-04467855>.

23:10 Operational semantics for Prolog with Cut in Rocq and its application to determinacy analysis

- 271 9 Davide Fissore and Enrico Tassi. Higher-order unification for free!: Reusing the meta-
272 language unification for the object language. In *Proceedings of PPDP*, pages 1–13. ACM, 2024.
273 doi:10.1145/3678232.3678233.
- 274 10 Davide Fissore and Enrico Tassi. Determinacy checking for elpi: an higher-order logic program-
275 ming language with cut. In *Practical Aspects of Declarative Languages: 28th International*
276 *Symposium, PADL 2026, Rennes, France, January 12–13, 2026, Proceedings*, pages 77–95,
277 Berlin, Heidelberg, 2026. Springer-Verlag. doi:10.1007/978-3-032-15981-6_5.
- 278 11 Benjamin Grégoire, Jean-Christophe Léchenet, and Enrico Tassi. Practical and sound equality
279 tests, automatically. In *Proceedings of CPP*, page 167–181. Association for Computing
280 Machinery, 2023. doi:10.1145/3573105.3575683.
- 281 12 Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. Implementing type theory
282 in higher order constraint logic programming. In *Mathematical Structures in Computer*
283 *Science*, volume 29, pages 1125–1150. Cambridge University Press, 2019. doi:10.1017/
284 S0960129518000427.
- 285 13 Robbert Krebbers, Luko van der Maas, and Enrico Tassi. Inductive Predicates via Least
286 Fixpoints in Higher-Order Separation Logic. In Yannick Forster and Chantal Keller, editors,
287 *16th International Conference on Interactive Theorem Proving (ITP 2025)*, volume 352 of *Leib-*
288 *niz International Proceedings in Informatics (LIPIcs)*, pages 27:1–27:21, Dagstuhl, Germany,
289 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITP.2025.27>. doi:10.4230/LIPIcs.ITP.2025.27.
- 290 14 Dale Miller. A logic programming language with lambda-abstraction, function variables, and
291 simple unification. In *Extensions of Logic Programming*, pages 253–281. Springer, 1991.
- 292 15 Dale Miller and Gopalan Nadathur. *Programming with Higher-Order Logic*. Cambridge
293 University Press, 2012.
- 294 16 Cornelia Pusch. Verification of compiler correctness for the wam. In Gerhard Goos, Juris
295 Hartmanis, Jan van Leeuwen, Joakim von Wright, Jim Grundy, and John Harrison, editors,
296 *Theorem Proving in Higher Order Logics*, pages 347–361, Berlin, Heidelberg, 1996. Springer
297 Berlin Heidelberg.
- 298 17 Enrico Tassi. Elpi: an extension language for Coq (Metaprogramming Coq in the Elpi λ Prolog
299 dialect). In *The Fourth International Workshop on Coq for Programming Languages*, January
300 2018. URL: <https://inria.hal.science/hal-01637063>.
- 301 18 Enrico Tassi. Deriving proved equality tests in Coq-Elpi. In *Proceedings of ITP*, volume 141 of
302 *LIPIcs*, pages 29:1–29:18, September 2019. URL: <https://inria.hal.science/hal-01897468>,
303 doi:10.4230/LIPIcs.CVIT.2016.23.
- 304 19 Luko van der Maas. Extending the Iris Proof Mode with inductive predicates using Elpi.
305 Master’s thesis, Radboud University Nijmegen, 2024. doi:10.5281/zenodo.12568604.
- 306 20 David H.D. Warren. An Abstract Prolog Instruction Set. Technical Report Technical Note 309,
307 SRI International, Artificial Intelligence Center, Computer Science and Technology Division,
308 Menlo Park, CA, USA, October 1983. URL: <https://www.sri.com/wp-content/uploads/2021/12/641.pdf>.