Master thesis
Computing Science

Radboud University

Extending Iris with Inductive predicates using Elpi

Author:
Luko van der Maas
luko.vandermaas@ru.nl
s1010320

Supervisor:
dr. Robbert Krebbers
robbert@cs.ru.nl

Assessor:
...
...

March 5, 2024

Abstract

Field, current gap, direction of solution, Results, Genererailzation of results and where else to apply it.

This is an abstract. It is very abstract. And now a funny pun about Iris from github copilot: "Why did the mathematician bring Iris to the formal methods conference? Because they wanted to be a 'proof-essional' with the most 'Irisistible' Coq proofs!"

Contents

Chapter 1

Introduction

Korte beschrijving van state of the art, er is seperatie logica met ... Het probleem met voorbeeld Oplossing uitleggen Lijstje van je contributies, ik heb x y en z gedaan en verwijzen naar hoofdstuk - ze moeten nieuw zijn - Meetbaar zijn - Doelvol zijn

Iris is a separation logic [Jun+15; Jun+16; Kre+17; Jun+18]. Propositions can be seen as predicates over resources, *e.g.,* heaps. Thus, there are a number of extra logical connectives such as `P * Q`, which represents that `P` and `Q` split up the resources into two disjoints in which they respectively hold. Moreover, hypotheses in our logic can often be used only once when proving something, they represent resources that we consume when used. To be able to reason in this logic in Coq a tactics' language has been added to Coq called the Iris Proof Mode (IPM) [KTB17; Kre+18].

```
EI.ind
Inductive is_MLL : val → list val → iProp :=
  | empty_is_MLL : is_MLL NONEV []
  | link_is_MLL v vs l tl : l ↦ (v, #true, tl) -∗
    is_MLL tl vs -∗ is_MLL (SOMEV #l) vs
  | cons_is_MLL v vs tl l : l ↦ (v, #false, tl) -∗
    is_MLL tl vs -∗ is_MLL (SOMEV #l) (v :: vs).
```

Chapter 2

Background on separation logic

In this chapter we give a background on separation logic by specifying and proving the correctness of a program on marked linked lists (MLLs), as seen in chapter 1. First we will setup the example we will discuss in this chapter in section 2.1. Next, we will be looking at separation logic as we will use it in the rest of this thesis in section 2.2. Then, we show how to give specifications using Hoare triples and weakest preconditions in section 2.3. Next, we will show how we can create a predicate used to represent a datastructure for our example in section 2.4. Lastly, we will finish the specification and proof of a program manipulating marked linked lists in section 2.5.

2.1 Setup

We will be defining a program that deletes an element at an index in a MLL as our example for this chapter. This program is written in HeapLang, a higher order, untyped, ML-like language. HeapLang supports many concepts around both concurrency and higher-order heaps (storing closures on the heap), however, we won't need any of these features. It can thus be treated as a basic ML-like language. The syntax together with any syntactic sugar can be found in figure 2.1. For more information about HeapLang one can reference the Iris technical reference [Iri23].

The program we will be using as an example will delete an index out of

$$
\begin{array}{rcll}
v, w \in \mathit{Val} & ::= & z \mid \mathbf{true} \mid \mathbf{false} \mid () \mid \lightning \mid \ell \mid & (z \in \mathbb{Z}, \ell \in \mathit{Loc}) \\
& & (v, w)_{\mathbf{v}} \mid \mathbf{inl}_{\mathbf{v}}(v) \mid \mathbf{inr}_{\mathbf{v}}(v) & \\
e \in \mathit{Expr} & ::= & v \mid x \mid e_1(e_2) \mid \circledcirc_1\, e \mid e_1 \circledcirc_2 e_2 \mid & \\
& & \mathbf{if}\, e\, \mathbf{then}\, e_1\, \mathbf{else}\, e_2 \mid & \\
& & (e_1, e_2)_{\mathbf{e}} \mid \mathbf{fst}(e) \mid \mathbf{snd}(e) \mid & \\
& & \mathbf{inl}_{\mathbf{e}}(e) \mid \mathbf{inr}_{\mathbf{e}}(e) \mid & \\
& & \mathbf{match}\, e\, \mathbf{with}\, \mathbf{inl}(x) \Rightarrow e_1 \mid \mathbf{inr}(y) \Rightarrow e_2\, \mathbf{end} \mid & \\
& & \mathbf{ref}(e_1, e_2) \mid !\, e \mid e_1 \leftarrow e_2 & \\
\circledcirc_1 & ::= & - \mid \ldots \quad \text{(list incomplete)} & \\
\circledcirc_2 & ::= & + \mid - \mid +_{\mathbf{L}} \mid = \mid \ldots \quad \text{(list incomplete)} &
\end{array}
$$

$$
\begin{array}{rcl}
\mathbf{let}\, x = e\, \mathbf{in}\, e' & \triangleq & (\lambda x.\, e')(e) \\
\mathbf{none} & \triangleq & \mathbf{inl}_{\mathbf{v}}(()) \\
\mathbf{some}\, v & \triangleq & \mathbf{inr}_{\mathbf{v}}(v) \\
e; e' & \triangleq & \mathbf{let}\, \_ = e\, \mathbf{in}\, e'
\end{array}
$$

Figure 2.1: Fragment of the syntax of HeapLang as used in the examples with at the bottom syntactic sugar being used

the list by marking that node, thus logically deleting it.

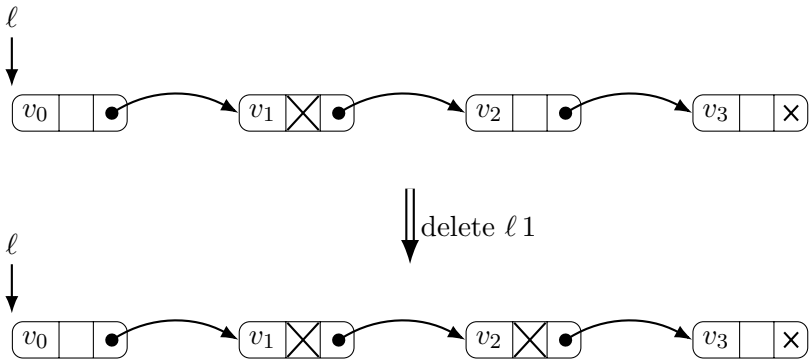
$$
\begin{array}{l}
\text{delete}\ \ell\, i := \mathbf{match}\, \ell\, \mathbf{with} \\
\quad \mathbf{none} \quad \Rightarrow () \\
\quad \mid \mathbf{some}\, \mathit{hd} \Rightarrow \mathbf{let}\, (x, \mathit{mark}, \mathit{tl}) = !\, \mathit{hd}\, \mathbf{in} \\
\qquad\qquad \mathbf{if}\, \mathit{mark} = \mathbf{false}\ \&\&\ i = 0\, \mathbf{then} \\
\qquad\qquad\quad \mathit{hd} \leftarrow (x, \mathbf{true}, \mathit{tl}) \\
\qquad\qquad \mathbf{else\ if}\, \mathit{mark} = \mathbf{false}\, \mathbf{then} \\
\qquad\qquad\quad \text{delete}\ \mathit{tl}\ (i - 1) \\
\qquad\qquad \mathbf{else} \\
\qquad\qquad\quad \text{delete}\ \mathit{tl}\ i \\
\quad \mathbf{end}
\end{array}
$$

The program is a function called delete, the function has two arguments. The first argument ℓ is either **none**, for the empty list, or **some** hd where hd is a pointer to a MLL. HeapLang has no null pointers, thus we use **none** as the null pointer. The second argument is the index in the MLL to delete. The first step this recursive function does in check whether the list we are

deleting from is empty or not. We thus match ℓ on either **none**, the MLL is empty, or on **some** *hd*, where *hd* becomes the pointer to the MLL and the MLL contains some nodes. If the list is empty, we are done and return unit. If the list is not empty, we load the first node and save it in the three variables *x*, *mark* and *tl*. Now, *x* contains the first element of the list, *mark* tells us whether the element is marked, thus logically deleted, and *tl* contains the reference to the tail of the list. We now have three different options for our list.

- If our index is zero and the element is not marked, thus logically deleted, we want to delete it. We write to the *hd* pointer our node, but with the mark bit set to **true**, thus logically deleting it.
- If the mark bit is **false**, but the index to delete, *i*, is not zero. The current node has not been deleted, and thus we we want to decrease *i* by one and recursively call our function f on the tail of the list.
- Lastly if the mark bit is set to **true**, we want to ignore this node and continue to the next one. We thus call our recursive function f without decreasing *i*.

delete $\ell\,1$ will thus apply the transformation below.



A tuple is shown here as three boxes next to each other, the first box contains a value. The second box is a boolean, it is true, thus marked, if it is crossed out. The third box is a pointer, denoted by either a cross, a null pointer, or a circle with an arrow pointing to the next node.

When thinking about it in terms of lists, delete $\ell\,1$ deletes from the list $[v_0, v_2, v_3]$ the element v_2, thus resulting in the list $[v_0, v_3]$. In the next section we will show how separation logic can be used to reason about sections of memory, such as shown above.

2.2 Separation logic

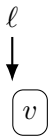
- Separation logic is a logic that allows us to represent the state of memory in a higher order predicate logic

- The syntax is

TODO: What are e and v

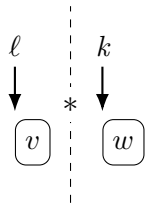
$$P \in \mathit{iProp} ::= \mathsf{False} \mid \mathsf{True} \mid P \wedge P \mid P \vee P \mid P \Rightarrow P \mid \exists x : \tau.\, P \mid \forall x : \tau.\, P \mid \\ \ell \mapsto v \mid P * P \mid P \mathrel{-\!\!*} P \mid \Box P \mid \mathsf{wp}\, e\, [\Phi]$$

- We will sometimes write $\mathsf{wp}\, e\, [\Phi]$ as $\mathsf{wp}\, e\, [v.\, P]$ where Φ is a predicate that takes a value
- It contains the normal higher order predicate logic connectives on the first line
- The first two connectives on the second line will be discussed in this section
- The last three connectives on the second line will be discussed in section 2.3
- We start with points to, $\mapsto$



$\ell \mapsto v$

- Picture of memory with $\ell \mapsto v$ next to it
- $\ell \mapsto v$ means we own a location in memory, l, and it has value v
- $\wedge$ now no longer works as expected
- introduce $*$



$\ell \mapsto v * k \mapsto w$

- Describe rules of $*$

$$\begin{aligned} \mathsf{True} * P &\dashv\vdash P \\ P * Q &\vdash Q * P \\ (P * Q) * R &\vdash P * (Q * R) \end{aligned}$$

$$\frac{P_1 \vdash Q_1 \qquad P_2 \vdash Q_2}{P_1 * P_2 \vdash Q_1 * Q_2}\ {*\text{-MONO}}$$

- This does not include $P \vdash P * P$

2.3 Writing specifications of programs

- We will discuss how to specify the actions of a program
- delete will be the example
- The goal will be total correctness
- Guarantee that given some preconditions in separation logic hold, the program will terminate and some postconditions in separation logic hold and e is safe
- Typically use Hoare triples

$$[P]\, e\, [\Phi]$$

- Given that P holds
- e terminates
- returns v
- $\Phi(v)$ now holds
- We often write $[P]\, e\, [v.\, Q]$, thus leaving out a λ
- We can also write a value for v to express that the returned value is that value
- Thus the specification of $\ell \leftarrow w$ becomes

$$[\ell \mapsto v]\, \ell \leftarrow w\, [().\ \ell \mapsto w]$$

- The precondition of our specification is that there is a location ℓ that has value v
- Then, $\ell \leftarrow w$ return unit
- New state of memory is $\ell \mapsto w$
- The Hoare triple of delete is

$$[\mathsf{isMLL}\ hd\ \vec{v}]\ \text{delete}\ hd\ i\ [().\ \mathsf{isMLL}\ hd\ (\mathsf{remove}\ i\ \vec{v})]$$

- This uses a predicate we will talk more about in section 2.4
- It tells is that the MLL in memory at hd is represented by the list of value $\vec{v}$
- remove is the function on mathematical lists that removes the element at index i from the list $\vec{v}$

WP

TODO: better title

- There is a second way to specify programs
- We use weakest preconditions, $\mathsf{wp}\ e\ [\Phi]$
- The weakest precondition states that expression e is safe to execute, terminates with value v and afterwards $\Phi(v)$ holds.
- We use the same way of writing predicates in the weakest precondition as with Hoare triples
- There is precondition in the weakest preconditions, instead we add that using the magic wand
- We add that using the magic wand, $P \mathrel{-\!\!*} \mathsf{wp}\ e\ [\Phi]$
- Magic wand is implication that reasons about resources
- $Q \mathrel{-\!\!*} R$ describes resources where if we add Q we get R
- as can bee seen in the below law

$$\frac{P * Q \vdash R}{P \vdash Q \mathrel{-\!\!*} R} \mathrel{-\!\!*}\text{I-E}$$

- This law works both ways.
- Thus, using the magic wand we add that if we have P then $\mathsf{wp}\ e\ [\Phi]$ holds.
- Thus, if we want to specify $\ell \leftarrow v$ using weakest precondition we use the rule WP-STORE in figure 2.2
- To prove, $\mathsf{wp}\ (\ell \leftarrow w)\ [\Phi]$, we have to prove that $\ell \mapsto v$ holds and $\ell \mapsto w \mathrel{-\!\!*} \Phi()$. In other words, if we add that $\ell \mapsto w$ holds, $\Phi()$ should hold.
- Besides rules about specific expression we also have general rules about the weakest precondition
- WP-VALUE is used when a program is finished
- WP-MONO allows us to transfrom the postcondition of wp
- WP-FRAME allows us to ???

Question: what does this again

- WP-BIND can extract the expression that is to be executed inside of the whole expression using the possible contexts

Structural rules.

$$\text{WP-VALUE}\quad \Phi(v) \vdash \mathsf{wp}\ v\ [\Phi] \qquad \text{WP-MONO}\quad \frac{\forall v.\Phi(v) \vdash \Psi(v)}{\mathsf{wp}\ e\ [\Phi] \vdash \mathsf{wp}\ e\ [\Psi]}$$

$$\text{WP-FRAME}\quad Q * \mathsf{wp}\ e\ [x.\ P] \vdash \mathsf{wp}\ e\ [x.\ Q * P] \qquad \text{WP-BIND}\quad \mathsf{wp}\ e\ [x.\ \mathsf{wp}\ K[x]\ [\Phi]] \vdash \mathsf{wp}\ K[e]\ [\Phi]$$

Rules for basic language constructs.

$$\text{WP-ALLOC}\quad \forall \ell.\ \ell \mapsto v \mathrel{-\!\!*} \Phi(\ell) \vdash \mathsf{wp}\ \mathbf{ref}(v)\ [\Phi] \qquad \text{WP-LOAD}\quad \ell \mapsto v * \ell \mapsto v \mathrel{-\!\!*} \Phi(v) \vdash \mathsf{wp}\ !\ell\ [\Phi]$$

$$\text{WP-STORE}\quad \ell \mapsto v * (\ell \mapsto w \mathrel{-\!\!*} \Phi()) \vdash \mathsf{wp}\ (\ell \leftarrow w)\ [\Phi] \qquad \text{WP-PURE}\quad \frac{e \longrightarrow_{\text{pure}} e' \qquad \mathsf{wp}\ e'\ [\Phi]}{\mathsf{wp}\ e\ [\Phi]}$$

Pure reductions.

$$(\mathsf{f}\,x := e)v \longrightarrow_{\text{pure}} e[v/x][\mathsf{f}\,x := e/\mathsf{f}] \qquad \mathbf{if}\ \mathbf{true}\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2 \longrightarrow_{\text{pure}} e_1$$

$$\mathbf{if}\ \mathbf{false}\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2 \longrightarrow_{\text{pure}} e_2 \qquad \mathbf{fst}(v_1, v_2) \longrightarrow_{\text{pure}} v_1$$

$$\mathbf{snd}(v_1, v_2) \longrightarrow_{\text{pure}} v_2 \qquad \frac{\circledcirc_1 v = w}{\circledcirc_1 v \longrightarrow_{\text{pure}} w} \qquad \frac{v_1 \circledcirc_2 v_2 = v_3}{v_1 \circledcirc_2 v_2 \longrightarrow_{\text{pure}} v_3}$$

$$\mathbf{match}\ \mathbf{inl_v}\ v\ \mathbf{with}\ \mathbf{inl}\ x \Rightarrow e_1 \mid \mathbf{inr}\ x \Rightarrow e_2\ \mathbf{end} \longrightarrow_{\text{pure}} e_1[v/x]$$

$$\mathbf{match}\ \mathbf{inr_v}\ v\ \mathbf{with}\ \mathbf{inl}\ x \Rightarrow e_1 \mid \mathbf{inr}\ x \Rightarrow e_2\ \mathbf{end} \longrightarrow_{\text{pure}} e_2[v/x]$$

Context rules

$$\begin{aligned} K \in Ctx ::= {} & \bullet \mid e\,K \mid K\,v \mid \circledcirc_1 K \mid e \circledcirc_2 K \mid K \circledcirc_2 v \mid \mathbf{if}\ K\ \mathbf{then}\ e_1\ \mathbf{else}\ e_2 \mid \\ & (e, K) \mid (K, v) \mid \mathbf{fst}(K) \mid \mathbf{snd}(K) \mid \\ & \mathbf{inl}(K) \mid \mathbf{inr}(K) \mid \mathbf{match}\ K\ \mathbf{with}\ \mathbf{inl} \Rightarrow e_1 \mid \mathbf{inr} \Rightarrow e_2\ \mathbf{end} \mid \\ & \mathbf{AllocN}(e, K) \mid \mathbf{AllocN}(K, v) \mid \mathbf{Free}(K) \mid !\,K \mid e \leftarrow K \mid K \leftarrow v \mid \end{aligned}$$

Figure 2.2: Rules for the weakest precondition assertion.

TODO: Explain why Hoare does not work, but wp does

- Thus we define the hoare triple as a weakest precondition
- Only use weakest pre-conditions in our proofs

$$[P]\ e\ [\Phi] \triangleq \square(P \mathrel{-\!\!*} \mathsf{wp}\ e\ [\Phi])$$

- We make use of new connective, $\Box$
- Our weakest precondition with its precondition are wrapped in a box, making the proposition persistent
- Any persistent proposition has the property that once we know it holds, it always holds
- As can be seen by the rule $\Box$-DUP below
- We are allowed to duplicate any persistent proposition
- We do have to prove that it is persistent
- To prove a proposition persistent we can only use persistent proposition in our assumptions as can be seen in the rule $\Box$-MONO below
- Other rules about persistent proposition can be seen below

$\Box$-DUP
$\Box P \dashv\vdash \Box P * \Box P$

$\Box$-SEP
$\Box P * Q \dashv\vdash \Box P * \Box Q$

$\Box$-MONO
$$\frac{P \vdash Q}{\Box P \vdash \Box Q}$$

$\Box$-E
$\Box P \vdash P$

$\Box$-DISTR
$\Box P \wedge Q \vdash \Box P * Q$

$$\Box P \vdash \Box \Box P$$
$$\forall x.\ \Box P \vdash \Box \forall x.\ P$$
$$\Box \exists x.\ P \vdash \exists x.\ \Box P$$

- From the definition of a hoare triple we now know it is persistent
- This is needed since we have a higher order heap, we can store closures
- Take the following function with its specification below

$$\begin{aligned}&\text{refadd } n \ :=\ \lambda \ell.\, \ell \leftarrow\, !\,\ell + n\\ &[\mathsf{True}]\ \text{refadd } n\, [f.\, \forall \ell.\ [\ell \mapsto m]\, f\, \ell\, [().\, \ell \mapsto n]]\end{aligned}$$

- The program takes a value n and then returns a closure which we can call with a pointer to add n to the value of that pointer
- We can now use this function in a program like below

$$\begin{aligned}&\textbf{let}\ f = \text{refadd } 10\ \textbf{in}\\ &\textbf{let}\ \ell = \textbf{ref}\, 0\ \textbf{in}\\ &f\,\ell; f\,\ell\\ &!\,\ell\end{aligned}$$

- Now since we can't duplicate resources and resources are used up once use, once we gain from the specification of addref that f has specification $[\ell \mapsto m]\, f\, \ell\, [().\, \ell \mapsto n]$
- If a hoare triple was not persistent, we could only use this specification once
- Thus we could not verify what would happen the second time we call f.
- But since they are we can use $\square$-DUP to duplicate the specification of f and use it twice
- Thus we can prove that the above program returns 20

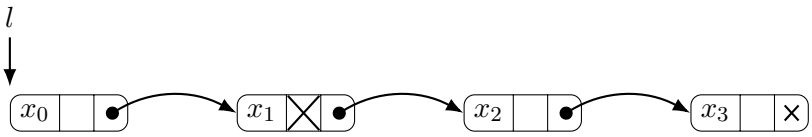
2.4 Representation predicates

The goal in specifying programs is to connect the world in which the program lives to the mathematical world. In the mathematical world we are able to create proves and by linking the program world to the mathematical world we can prove properties of the program.

TODO: Maybe move the first part of this section to an earlier section

We have shown in the previous two sections how one can represent simple states of memory in a logic and reason about it together with the program. However, this does not easily scale to more complicated data types, especially recursive datatypes. One such datatype is the MLL. We want to connect a MLL in memory to a mathematical list. In section 2.3 we used the predicate $\mathsf{isMLL}\, hd\, \vec{v}$, which tells us that the in the memory starting at hd we can find a MLL that represents the list $\vec{v}$. In this section we will show how such a predicate can be used.

- We need an inductive predicate to reason about a recursive structure
- For $\mathsf{isMLL}\, (\mathbf{some}\, \ell)\, [x_0, x_2, x_3]$ look below



- Our end goal should work like below
- this does not work because it is not necessarily finite?

Question: This is correct right, and is Coq the reason why it has to be finite?

$$\mathsf{isMLL}\, hd\, \vec{v} = \begin{array}{ll} & hd = \mathbf{none} * \vec{v} = [] \\ \vee & hd = \mathbf{some}\, l * l \mapsto (v, \mathbf{true}, tl) * \mathsf{isMLL}\, tl\, \vec{v} \\ \vee & hd = \mathbf{some}\, l * l \mapsto (v, \mathbf{false}, tl) * \mathsf{isMLL}\, tl\, ([v] + \vec{v}) \end{array}$$

- We first turn our desired predicate into a functor
- It transforms a predicate Φ into a predicate that applies Φ to the tail of the MLL if it exists

TODO: write more correct

$$\mathsf{isMLLPre}\,\Phi\,hd\,\vec{v} \triangleq \begin{array}{ll} & hd = \mathbf{none} * \vec{v} = [] \\ \vee & hd = \mathbf{some}\,l * l \mapsto (v, \mathbf{true}, tl) * \Phi\,tl\,\vec{v} \\ \vee & hd = \mathbf{some}\,l * l \mapsto (v, \mathbf{false}, tl) * \Phi\,tl\,([v] + \vec{v}) \end{array}$$

- This gets rid of the possible infinite nature of the statement
- but not strong enough
- we want to find a Φ such that

$$\forall hd\,\vec{v}.\ \mathsf{isMLLPre}\,\Phi\,hd\,\vec{v} \mathrel{-\!\!*\!\!*} \Phi\,hd\,\vec{v}$$

- This is the fixpoint of isMLLPre
- Use Knaster-Tarski Fixpoint Theorem to find this fixpoint [Tar55]
- Specialized to the lattice on predicates

Theorem 2.1 (*Knaster-Tarski Fixpoint Theorem*)

Let $\mathsf{F}\colon (A \to iProp) \to (A \to iProp)$ *be a monotone predicate, then*

$$\mathsf{lfp}\,\mathsf{F}\,x \triangleq \forall \Phi.\ (\forall x.\ \mathsf{F}\,\Phi\,x \mathrel{-\!\!*} \Phi\,x) \mathrel{-\!\!*} \Phi\,x$$

defines the least fixpoint of F

Question: Where to introduce *iProp*?

- Monotone is defined as

Definition 2.2 (*Monotone predicate*)

Any F is monotone when for any $\Phi, \Psi\colon A \to iProp$, it holds that

$$\square(\forall x.\ \Phi x \mathrel{-\!\!*} \Psi x) \mathrel{-\!\!*} \forall x.\ \mathsf{F}\Phi x \mathrel{-\!\!*} \mathsf{F}\Phi x$$

- In general F is monotone if all occurrences of its Φ are positive
- This is the case for isMLL
- We can expand theorem 2.1 to predicates of type $\mathsf{F}\colon (A \to B \to iProp) \to (A \to B \to iProp)$
- Thus the fixpoint exists and is

$$\mathsf{lfp}\,\mathsf{isMLLPre}\,hd\,\vec{v} = \forall \Phi.\,(\forall hd'\,\vec{v}'.\,\mathsf{isMLLPre}\,\Phi\,hd'\,\vec{v}' \mathrel{-\!\!*} \Phi\,hd'\,\vec{v}') \mathrel{-\!\!*} \Phi\,hd\,\vec{v}$$

- We can now redefine isMLL as

$$\mathsf{isMLL}\,hd\,\vec{v} \triangleq \mathsf{lfp}\,\mathsf{isMLLPre}\,hd\,\vec{v}$$

- Using the least fixpoint we can now define some additional lemmas

Lemma 2.3 (lfp F *is the least fixpoint on* F)

Given a monotone $\mathsf{F} : (A \to iProp) \to (A \to iProp)$*, it holds that*

$$\forall x.\,\mathsf{F}\,(\mathsf{lfp}\,\mathsf{F})\,x \mathrel{-\!\!*\!\!*} \mathsf{lfp}\,\mathsf{F}\,x$$

Lemma 2.4 (*least fixpoint induction principle*)

Given a monotone $\mathsf{F} : (A \to iProp) \to (A \to iProp)$*, it holds that*

$$\square(\forall x.\,\mathsf{F}\,\Phi\,x \mathrel{-\!\!*} \Phi\,x) \mathrel{-\!\!*} \forall x.\,\mathsf{lfp}\,\mathsf{F}\,x \mathrel{-\!\!*} \Phi\,x$$

Lemma 2.5 (*least fixpoint strong induction principle*)

Given a monotone $\mathsf{F} : (A \to iProp) \to (A \to iProp)$*, it holds that*

$$\square(\forall x.\,\mathsf{F}\,(\lambda y.\,\Phi\,y \wedge \mathsf{lfp}\,\mathsf{F}\,y)\,x \mathrel{-\!\!*} \Phi\,x) \mathrel{-\!\!*} \forall x.\,\mathsf{lfp}\,\mathsf{F}\,x \mathrel{-\!\!*} \Phi\,x$$

TODO: Maybe on isMLL example

2.5 Proof of delete in MLL

In this section we will proof the specification of delete. First we recap the definition and then give the proof. Recall the definition of delete.

```
delete ℓ i := match ℓ with
                none    ⇒ ()
              | some hd ⇒ let (x, mark, tl) = ! hd in
                          if mark = false && i = 0 then
                            hd ← (x, true, tl)
                          else if mark = false then
                            delete tl (i − 1)
                          else
                            delete tl i
              end
```

Lemma 2.6

For any list $\vec{v}$

Chapter 3

Fixpoints

Chapter 4

Implementing an Iris tactic in Elpi

In this chapter we will show how Elpi together with Coq-Elpi can be used to create new tactics. We will do this by giving a tutorial on how to implement the `iIntros` tactic from Iris.

4.1 `iIntros` example

`iIntros` is based on the Coq **`intros`** tactic. The Coq **`intros`** tactic makes use of a domain specific language (DSL) for quickly introducing different logical connective. In Iris this concept was adopted for the `iIntros` tactic, but adopted to the Iris contexts. Also, a few expansions, as inspired by ssreflect [HKP97; GMT16], were added to perform other common initial proof steps such as **`simpl`**, **`done`** and others. We will show a few examples of how `iIntros` can be used to help prove lemmas.

We begin with a lemma about the magic wand. The magic wand can be seen as the implication of separation logic which also takes into account the separation of resources.

$$\frac{P * Q \vdash R}{P \vdash Q \mathrel{-\!\!*} R} \mathrel{-\!\!*}\text{-Intro} \qquad \frac{P \land Q \vdash R}{P \vdash Q \to R} \to\text{-Intro}$$

Thus, where a normal implication introduction adds the left-hand side to the Coq context, the magic wand adds the left-hand side to the spatial resource context.

TODO: Rewrite when I have a solid explanation of the Iris contexts

```
1 P, R: iProp
2 ============
3 ------------*
4 P -* R -* P
```

When using `iIntros "HP HR"`, the proof state is transformed into the following state.

```
P, R: iProp
============
"HP" : P
"HR" : R
------------*
P
```

We have introduced the two separation logic propositions into the spatial context. This does not only work on the magic wand, we can also use this to introduce more complicated statements. Take the following proof state,

```
P: nat → iProp
============================================
--------------------------------------------*
∀ x : nat, (∃ y : nat, P x * P y) ∨ P 0 -* P 1
```

It consists of a universal quantification, an existential quantification, a conjunction and a disjunction. We can again use one application of `iIntros` to introduce and eliminate the premise. `iIntros "%x [[%y [Hx Hy]] | H0]"` takes the proof to the following state of two goals

```
(1/2)
P: nat → iProp
x, y: nat
==================
"Hx" : P x
"Hy" : P y
------------------*
P 1

(2/2)
P: nat → iProp
x: nat
==================
"H0" : P 0
------------------*
P 1
```

The intro pattern consists of multiple sub intro patterns. Each sub intro pattern starts with a forall introduction or wand introduction. We then interpret the intro pattern for the introduced hypothesis. They can have the following interpretations:

- `"H"` represents renaming a hypothesis. The name given is used as the name of the hypothesis in the spatial context.

- `"%H"` represents pure elimination. The introduced hypothesis is interpreted as a Coq hypothesis, and added to the Coq context.
- `"[IPL | IPR]"` represents disjunction elimination. We perform a disjunction elimination on the introduced hypothesis. Then, we apply the two included intro patterns two the two cases created by the disjunction elimination.
- `"[IPL IPR]"` represents separating conjunction elimination. We perform a separating conjunction elimination. Then, we apply the two included intro patterns two the two hypotheses by the separating conjunction elimination.
- `"[%x IP]"` represents existential elimination. If first element of a separating conjunction pattern is a pure elimination we first try to eliminate an exists in the hypothesis and apply the included intro pattern on the resulting hypothesis. If that does not succeed we do a conjunction elimination.

Thus, we can break down `iIntros "%x [[%y [Hx Hy]] | H0]"` into its components. We first forall introduce or first sub intro pattern `"%x"` and then perform the second case, introduce a pure Coq variable for the `∀ x : nat`. Next we wand introduce for the second sub intro pattern, `"[[%y [Hx Hy]] | H0]"` and interpret the outer pattern. it is the third case and eliminates the disjunction, resulting in two goals. The left patterns of the seperating conjunction pattern eliminates the exists and adds the `y` to the Coq context. Lastly, `"[Hx Hy]"` is the fourth case and eliminates the seperating conjunction in the Iris context by splitting it into two assumptions `"Hx"` and `"Hy"`.

There are more patterns available to introduce more complicated goals, these can be found in a paper written by Krebbers, Timany, and Birkedal [KTB17].

4.2 Contexts

- Iris uses a named context instead of the entailment
- `env A` is a list of pairs from identifiers to `A`.

```
1  Inductive ident :=
2    | IAnon : positive → ident
3    | INamed :> string → ident.
4
5  Record envs (PROP : bi) := Envs {
```

```
  env_persistent : env PROP;
  env_spatial : env PROP;
  env_counter : positive;
}.
```

TODO: Explain *Prop*somewhere or just use *iProp*

TODO: I am simplifying the environments here, should I do that?

- Identifiers are either anonymous or named
- Environments are maps from identifiers to values
- The final context is two environments of propositions and a counter
- The first environment is the persistent context
- The second environment is the spatial context
- The two environments can't have overlapping identifiers
- The counter is used to always be able to generate a fresh anonymous identifier
- Semantics of the contexts is

```
Definition of_envs {PROP : bi}
    (Γp Γs : env PROP) : PROP :=
  (□ [∧] Γp ∧ [∗] Γs)%I.
```

Question: Should I differentiate between □ and <pers>

- The persistent environment is combined with $\wedge$ and surrounded by a $\Box$.
- The spatial environment is combined with $*$
- We can now write our entailment as

```
Definition envs_entails {PROP : bi}
    (Δ : envs PROP) (Q : PROP) : Prop :=
  of_envs (env_intuitionistic Δ) (env_spatial Δ) ⊢ Q.
```

- This is represented in the proof state as

```
P, Q, R: iProp
============
"HP" : P
------------□
"HR" : Q
------------*
R
```

- P is a persistent proposition
- Q is a spatial proposition
- We need to proof R

4.3 Tactics

- The proof rules are hard to use with the context
- Define Lemma's that work with the context
- These allow us to define our tactics easily

```
Lemma tac_wand_intro Δ i P Q :
  match envs_app false (Esnoc Enil i P) Δ with
  | None => False
  | Some Δ' => envs_entails Δ' Q
  end →
  envs_entails Δ (P -* Q).
```

- Introduces a magic wand
- Add introduced proposition to the spatial context
- The condition we need to satisfy is a Coq function that resolves to Q with P added to the context
- If `i` already exists in the context, we have to proof False
- Tactics now just process the arguments and call necessary Lemma's

The tactics the IPM adds are build to replicate many of the behaviors of the Coq tactics while manipulating the Iris contexts. In the next section we will show how the Iris variant of the **`intros`** tactic works.

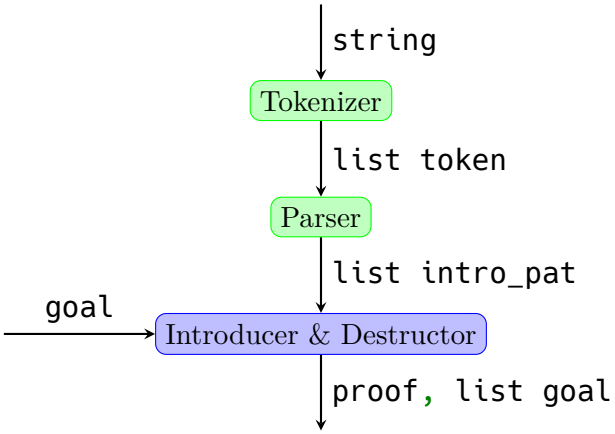


Figure 4.1: Structure of `eiIntros` with the input and output types on the edges.

4.4 Elpi

We implement our tactic in the λProlog language Elpi [Dun+15; GCT19]. Elpi implements λprolog [MN86; Mil+91; BBR99; MN12] and adds constraint handling rules to it [Mon11]. constraint handling will be explained in Section ?.

TODO: Defer constraint handling to later

To use Elpi as a Coq meta programming language, there exists the Elpi Coq connector, Coq-Elpi [Tas18]. We will use Coq-Elpi to implement the Elpi variant of `iIntros`, named above as `eiIntros`.

Our Elpi implementation `eiIntros` consists of three parts as seen in figure 4.1. The first two parts will interpret the DSL used to describe what we want to introduce. Then, the last part will apply the interpreted DSL. In section 4.5 we describe how a string is tokenized by the tokenizer. In section 4.6 we describe how a list of tokens is parsed into a list of intro patterns. In section 4.7 we describe how we use an intro pattern to introduce and eliminate the needed connectives. In every section we describe more parts of the Elpi programming language and the Coq-Elpi connector starting with the base concepts of the language and working up to the mayor concepts of Elpi and Coq-Elpi.

4.5 Tokenizer

The tokenizer takes as input a string. We will interpret every symbol in the string and produce a list of tokens from this string. Thus, the first step is to define our tokens. Next we show how to define a predicate that transform our string into the tokens we defined.

4.5.1 Data types

We have separated the introduction patterns into several distinct tokens. Most tokens just represent one or two characters, but some tokens also contain some data associated with that token. For example `"H1"` is tokenized as the name token containing the string "H1".

```
kind token type.

type tAnon, tFrame, tBar, tBracketL, tBracketR, tAmp,
     tParenL, tParenR, tBraceL, tBraceR, tSimpl,
     tDone, tForall, tAll token.
type tName string -> token.
type tNat int -> token.
type tPure option string -> token.
type tArrow direction -> token.

kind direction type.
type left, right direction.
```

We first define a new type called token using the `kind` keyword, where `type` specifies the kind of our new type. Then we define several constructors for the token type. These constructors are defined using the `type` keyword, we specify a list of names for the constructors and then the type of those constructors. The first set of constructors do not take any arguments, thus have type `token`, and just represent one or more constant characters. The next few constructors take an argument and produce a token, thus allowing us to store data in the tokens. For example, `tName` has type `string -> token`, thus containing a string. Besides `string`, there are a few more basic types in Elpi such as `int`, `float` and `bool`. We also have higher order types, like `option A`, and later on `list A`.

```
kind option type -> type.
type none option A.
type some A -> option A.
```

Creating types of kind `type -> type` can be done using the `kind` directive and passing in a more complicated kind.

We can now represent a string as a list of these tokens. Given the string `"[H %H']"` we can represent it as the following list of type `token`:

```
[tBracketL, tName "H", tPure (some "H'"), tBracketR]
```

4.5.2 Predicates

Programs in Elpi consist of predicates. Every predicate can have several rules to describe the relation between its inputs and outputs.

```
1 pred tokenize i:string, o:list token.
2 tokenize S O :-
3   rex.split "" S SS,
4   tokenize.rec SS O.
```

Line 1 describes the type of the predicate. The keyword `pred` starts the definition of a predicate. Next we give the name of the predicate, "tokenize". Lastly, we give a list of arguments of our predicate. Each argument is marked as either `i:`, they act as an input or `o:`, they act as an output, in section 4.5.3 a more precise definition is given. In the only rule of our predicate, defined on line 2, we assign a variable to both of the arguments. `S` has type `string` and is bound to the first argument. `O` has type `list token` and is bound to the second argument. By calling predicates after the `:-` symbol we can define the relation between the arguments. The first predicate we call, `rex.split`, has the following type:

```
1 pred rex.split i:string, i:string, o:list string.
```

When we call it, we assign the empty string to its first argument, the string we want to tokenize to the second argument, and we store the output list of string in the new variable `SS`. This predicate allows us to split a string at a certain delimiter. We take as delimiter the empty string, thus splitting the string up in a list of strings of one character each. Strings in Elpi are based on OCaml strings and are not lists of characters. Since Elpi does not support pattern matching on partial strings, we need this workaround.

The next line, line 4, calls the recursive tokenizer, `tokenizer.rec`[1], on the list of split string and assigns the output to the output variable `O`.

The reason predicates in Elpi are called predicates and not functions, is that they don't always have to take an input and give an output. They can sometimes better be seen as predicates defining for which values of their arguments they hold. Each rule defines a list of predicates that need to hold for their premise to hold. Thus, a predicate can have multiple values for its output, as long as they hold for all contained rules. These multiple possible values can be reached by backtracking, which we will discuss in section 4.5.5. To execute a predicate, we thus find the first rule for which its premise is sufficient for the arguments we supply. We then check if each of the predicates in the conclusion hold starting at the top. If they hold, and we

[1] Names in Elpi can have special characters in them like `.`, `-` and `>`, thus, `tokenize` and `tokenize.rec` are fully separate predicates. It is just a convention that when creating a helper predicate we name it by adding a dot and a short name for the helper.

get a value for every output argument, we are done executing our predicate. How we determine when arguments are sufficient and what happens when a rule does not hold, we will discuss in the next two sections.

4.5.3 Matching and unification

The arguments of a predicate can be more than just a variable. We can supply a value containing variables and depending on the argument mode, input or output, we match or unify the input with the premise respectively.

`tokenize.rec` uses matching and unification to solve most cases.

```
1 pred tokenize.rec i:list string, o:list token.
2 tokenize.rec [] [] :- !.
3 tokenize.rec [" " | SL] TS :- !, tokenize.rec SL TS.
4 tokenize.rec ["$" | SL] [tFrame | TS] :- !,
5   tokenize.rec SL TS.
6 tokenize.rec ["/", "/", "=" | SL] [tSimpl, tDone | TS] :- !,
7   tokenize.rec SL TS.
8 tokenize.rec ["/", "/" | SL] [tDone | TS] :- !,
9   tokenize.rec SL TS.
```

This predicate has several rules, we chose a few to highlight here. The first rule, on line 2, has a premise and a cut as its conclusion, we will discuss cuts in section 4.5.5, for now they can be ignored. This rule can be used when the first argument matches `[]` and if the second argument unifies with `[]`. The difference is that, for two values to match they must have the exact same constructors and can only contain variables in the same places in the value. Thus, the only valid value for the first argument of the first rule is `[]`. When unifying two values we allow a variable to be unified with a constructor, when this happens the variable will get assigned the value of the constructor. Thus, we can either pass `[]` to the second argument, or some variable `V`. After the execution of the rule the variable `V` will have the value `[]`.

The next four rules use the same principle. They use the list pattern `[E1, ..., En | TL]`, where `E1` to `En` are the first n values and `TL` is the rest of the list, to match on the first few elements of the list. We unify the output with a list starting with the token that corresponds to the string we match on. The tails of the input and output we pass to the recursive call of the predicate to solve.

When we encounter multiple rules that all match the arguments of a rule we try the first one first. The rules on line 6 and 8 would both match the value `["/", "/", "="]` as first argument. But, we interpret this use the rule on line 6 since it is before the rule on line 8. This results in our list of strings being tokenized as `[tSimpl, tDone]`.

A fun side effect of output being just variables we pass to a predicate is that we can also easily create a function that is reversible. If we change the mode of our first argument to output and move rule 3 to the bottom, we can pass in a list of tokens and get back a list of strings representing this list of tokens.

Question: Don't know what to do with this, but is an interesting fact and shows the versatility, we might use it later.

4.5.4 Functional programming in Elpi

While our language is based on predicates we still often defer to a functional style of programming. The first language feature that is very useful for this goal is spilling. Spilling allows us to write the entry point of the tokenizer as defined in section 4.5.2 without the need of the temporary variable to pass the list of strings around.

```
1 pred tokenize i:string, o:list token.
2 tokenize S O :- tokenize.rec {rex.split "" S} O.
```

We spill the output of a predicate into the input of another predicate by using the `{ }` syntax. We don't specify the last argument of the predicate and only the last argument of a predicate can be spilled. It is mostly equal to the previous version, but just written shorter. There is one caveat, but it will be discussed in ?.

TODO: Refer to relevant section

The second useful feature is how lambda expressions are first class citizens of the language. A `pred` statement is a wrapper around a constructor definition using the keyword `type`, where all arguments are in output mode. The following predicate is equal to the type definition below it.

```
1 pred tokenize i:string, o:list token.
2 type tokenize string -> list token -> prop.
```

The `prop` type is the type of propositions, and with arguments they become predicates. We are thus able to write predicates that accept other predicates as arguments.

```
1 pred map i:list A, i:(A -> B -> prop), o:list B.
2 map [] _ [].
3 map [X|XS] F [Y|YS] :- F X Y, map XS F YS.
```

`map` takes as its second argument a predicate on `A` and `B`. On line 3 we map this predicate to the variable `F`, and we then use it to either find a `Y` such that `F X Y` holds, or check if for a given `Y`, `F X Y` holds. We can use the same strategy to implement many of the common functional programming higher order functions.

4.5.5 Backtracking

In this section we will finally describe what happens when a rule fails to complete halfway through. We start with a predicate which will be of much use for the last part of our tokenizer.

```
1 pred take-while-split i:list A, i:(A -> prop),
2                       o:list A, o:list A.
3 take-while-split [X|XS] Pred [X|YS] ZS :- Pred X,
4   take-while-split XS Pred YS ZS.
5 take-while-split XS _ [] XS.
```

`take-while-split` is a predicate that should take elements of its input list till its input predicate no longer holds and then output the first part of input in its third argument and the last part of the input in its fourth argument.

The predicate contains two rules. The first rule, defined on lines 2 and 3, recurses as long as the input predicate, `Pred` holds for the input list, `[X|XS]`. The second rule returns the last part of the list as soon as `Pred` no longer holds.

The first rule destructs the input in its head `X` and its tail `XS`. It then checks if `Pred` holds for `X`, if it does, we continue the rule and call `take-while-split` on the tail while assigning X as the first element of the first output list and the output of the recursive call as the tail of the first output and the second output. However, if `Pred X` does not succeed we backtrack to the previous rule in our conclusion. Since there is no previous rule in the conclusion we instead undo any unification that has happened and try the next possible rule. This will be the rule on line 4 and returns the input as the second output of the predicate.

We can use `take-while-split` to define the rule for the token `tName`

```
1 type tName string -> token.
2
3 tokenize.rec SL [tName S | TS] :-
4   take-while-split SL is-identifier S' SL',
5   { std.length S' } > 0, !,
6   std.string.concat "" S' S,
7   tokenize.rec SL' TS.
```

To tokenize a name we first call `take-while-split` with as predicate `is-identifier`, which checks if a string is valid identifier character, whether it is either a letter or one of a few symbols allowed in identifiers. It thus splits up the input string list into a list of string that is a valid identifier and the rest of the input. On line 5 we check if the length of the identifier is

larger than 0. We do this by spilling the length of `S'` into the `>` predicate. Next, on line 6, we concatenate the list of strings into one string, which will be our name. And on line 7, we call the tokenizer on the rest of the input, to create the rest of our tokens.

If our length check does not succeed we backtrack to next rule that matches, which is

```
1 tokenize.rec XS _ :- !,
2   coq.say "unrecognized tokens" XS, fail.
```

It prints an error messages saying that the input was not recognized as a valid token, after which it fails. The predicate thus does not succeed. There is one problem, if line 6 or 7 fails for some reason in the `tName` rule of the tokenizer, the current input starting at `X` is not unrecognized as we managed to find a token for the name at the start of the input. Thus, we don't want to backtrack to another rule of `tokenize.rec` when we have found a valid name token. This is where the cut symbol, `!`, comes in. It cuts the backtracking and makes certain that if we fail beyond that point we don't backtrack in this predicate.

If we take the following example

```
1 tokenize.rec ["H","^"] TS
2               ⇓ calls
3 tokenize.rec ["^"] TS'
```

When evaluating this predicate we would first apply the name rule of the `tokenize.rec` predicate. This would unify `TS` with `[tName "H" | TS']` and call line 3, `tokenize.rec ["^"] TS'`. Every rule of `tokenize.rec` fails including the last fail rule. This rule does first print `"unrecognized tokens ^"` but then also fails. Now when executing the rule of line 1, we have failed on the last predicate of the rule. If there was no cut before it, we would backtrack to the fail rule and also print `"unrecognized tokens [H, ^]"`. But, because there is a cut we don't print the faulty error message. Thus, we only print meaningful error message when we fail to tokenize an input.

4.6 Parser

Question: Ik twijfel over dit hele stuk aangezien er niet zo veel nieuws in wordt uitgelegt dat nuttig is voor later, behalve pas op met backtracking.

- Describe sections of parser

Alternative for this section

- Parser uses many of the same techniques as tokenizer for parsing
- Not much to explain

- Implements a reductive descent parsing
- Minimize backtracking
- Look at code for full details

4.6.1 Data structure

- structured to be easily read to apply the intro pattern.

```
kind ident type.
type iNamed string -> ident.
type iAnon term -> ident.

kind intro_pat type.
type iFresh, iSimpl, iDone intro_pat.
type iIdent ident -> intro_pat.
type iList list (list intro_pat) -> intro_pat.
```

- Tree structure?
- iList is combination of existential, disjunction and conjunction pattern

4.6.2 Reductive descent parsing

- We can translate a grammar directly into a parser
- Below, partial grammar for the intro patterns

$$
\begin{aligned}
\langle \textit{intropattern\_list} \rangle \quad &::= \epsilon \\
&\mid \langle \textit{intropattern} \rangle \ \langle \textit{intropattern\_list} \rangle
\end{aligned}
$$

$$
\begin{aligned}
\langle \textit{intropattern} \rangle \quad &::= \langle \textit{ident} \rangle \\
&\mid \text{`?'} \mid \text{`/='} \mid \text{`//'} \\
&\mid \text{`[' } \langle \textit{intropattern\_list} \rangle \text{ `]'} \\
&\mid \text{`(' } \langle \textit{intropattern\_conj\_list} \rangle \text{ `)'}
\end{aligned}
$$

$$
\begin{aligned}
\langle \textit{intropattern\_list} \rangle \quad &::= \epsilon \\
&\mid \langle \textit{intropattern} \rangle \text{ `|' } \langle \textit{intropattern\_list} \rangle \\
&\mid \langle \textit{intropattern} \rangle \ \langle \textit{intropattern\_list} \rangle
\end{aligned}
$$

$$
\begin{aligned}
\langle \textit{intropattern\_conj\_list} \rangle \quad &::= \epsilon \\
&\mid \langle \textit{intropattern} \rangle \text{ `\&' } \langle \textit{intropattern\_conj\_list} \rangle
\end{aligned}
$$

- Explain structure of parser
- give example of anon, simpl and done
- Using tokenizer name has become the same

```
pred parse_ip i:list token, o:list token, o:intro_pat.
parse_ip [tAnon | TS] TS (iFresh) :- !.
parse_ip [tSimpl | TS] TS (iSimpl) :- !.
parse_ip [tDone | TS] TS (iDone) :- !.
parse_ip [tName X | TS] TS (iIdent (iNamed X)) :- !.
```

- Check after calling new parser that conditions for values hold
- Post process conj parser result

```
parse_ip [tBracketL | TS] TS' (iList L) :- !,
parse_ilist TS [tBracketR | TS'] L.
parse_ip [tParenL | TS] TS' IP :- !,
parse_conj_ilist TS [tParenR | TS'] L',
{std.length L'} >= 2,
foldr {std.drop-last 2 L'} (iList [{std.take-last 2 L'}]) (x\ a\ r\ r =
```

- Recursive parser

```
pred parse_ilist i:list token, o:list token, o:list (list intro_pat).
parse_ilist [tBracketR | TS] [tBracketR | TS] [[]].
parse_ilist TS R [[IP] | LL'] :-
  parse_ip TS [tBar | RT] IP,
  parse_ilist RT R LL'.
parse_ilist TS R [[IP | L] | LL'] :-
  parse_ip TS RT IP,
  parse_ilist RT R [L | LL'].

pred parse_conj_ilist i:list token, o:list token, o:list intro_pat.
parse_conj_ilist TS [tParenR | R] [IP] :-
  parse_ip TS [tParenR | R] IP.
parse_conj_ilist TS R [IP | L'] :-
  parse_ip TS [tAmp | RT] IP,
  parse_conj_ilist RT R L'.
```

4.6.3 Danger of backtracking

- Show timing of current `parse_ilist` code on larger inputs
- Change backtracking
- Show new timings
- Explain why it is better

```
pred parse_ilist i:list token, o:list token, o:list (list intro_pat).
parse_ilist [tBracketR | TS] [tBracketR | TS] [[]].
parse_ilist TS R [IPS | LL'] :-
  parse_ip TS RT IP,
  (
    (
      RT = [tBar | RT'],
      parse_ilist RT' R LL',
      IPS = [IP]
    );
    (
      parse_ilist RT R [L | LL'],
      IPS = [IP | L]
    )
  ).
```

4.7 Applier

- Only used standard Elpi
- Now use Coq-Elpi
- What Coq-Elpi adds
- Section overview

4.7.1 Elpi coq HOAS

- First step, represent Coq terms in Elpi
- Names and function application are just constructors

```
1+1
```

```
app [global (const «Nat.add»),
    app [global (indc «S»), global (indc «0»)],
    app [global (indc «S»), global (indc «0»)]]
```

- Explain app, global, const, indc and «»
- Coq-Elpi uses higher-order abstract syntax (HOAS)
- functions in Coq are functions that produce terms in Coq-Elpi

```
fun (n: nat), n + 1
```

```
FUN = fun `n` (global (indt «nat»)) n \
        app [global (indt «sum»),
            n,
            app [global (indc «S»), global (indc «0»)]]
```

- fun constructor taking name, type and function producing term
- footnote about names all being convertible

```
type fun  name -> term -> (term -> term) -> term.
```

- prod, let, fix work the same

4.7.2 Coq context in Elpi

- Looking at terms in functions becomes hard as we need to give the function an input to get the term
- introduce fresh constant using `pi x\`

```
FUN = fun _ _ F,
pi x\ F x = app [_, _, P],
P = app [global (indc «S»), global (indc «0»)]
```

- Take function out of constructor
- Fill in function with existential variable to inspect contents
- Take out number we add
- We lose type and name information about x

```
pred decl i:term, o:name, o:term.
decl x `n` (global (indt «nat»)).
```

- decl rule describes types and names of variables
- Lookup type using `decl x N T`
- We have to add the rule when we define x

```
pi x\ decl x `n` (global (indt «nat»))
        => coq.typecheck (F x) Type ok.
```

- We add a rule to the top of the rules for the execution of the code after the **=>**
- During typechecking, `decl x N T` is executed resulting in ...
- `Type` becomes (global (indt «nat»))
- **=>** has many more uses later on

4.7.3 Quotation and anti-quotation

- Writing terms is a lot of work
- Coq-Elpi allows us to write Coq code that is translated immediately using imports in current file

```
{{ λ (n: nat), n + 1 }} =
  fun `n` (global (indt «nat»)) c0 \
      app [global (indt «sum»),
          c0,
          app [global (indc «S»), global (indc «O»)]]
```

- Coq-Elpi also allows putting Elpi vars in Coq terms (anti quotation)

```
{{ @envs_entails lp:PROP (@Envs lp:PROPE lp:CI lp:CS lp:N) lp:P }}
```

- Extract values from term
- Insert values in term, useful in proofs

```
{{ as_emp_valid_2 lp:Type _ (tac_start _ _) }}
```

- Lemma useful in next section
- Type is type of goal we want to proof
- Term becomes lemma we can apply to goal

4.7.4 Proofs in Elpi

- Proofs in Elpi built up proof term step by step
- Pass around Type of goal and variable to assign proof term to
- This is hole

```
kind hole type.
type hole term -> term -> hole. % hole Type Proof
```

- Proofs take a hole and often produce new holes
- Following proof step applies the ex-Falso proof step
- Replace type with False

```
pred do-iExFalso i:hole, o:hole.
do-iExFalso (hole Type Proof) (hole FalseType FalseProof) :-
  coq.elaborate-skeleton {{ tac_ex_falso _ _ _ }} Type Proof ok,
  Proof = {{ tac_ex_falso _ _ lp:FalseProof }},
  coq.typecheck FalseProof FalseType ok.
```

```
Lemma tac_ex_falso Δ Q : envs_entails Δ False → envs_entails Δ Q.
```

- Elaborate Lemma against type to generate proof term will be Lemma filled in with necessary values
- Next, extract New proof variable
- Get type of new proof variable

Iris context counter

- Iris can have anonymous hypotheses in context
- Keep track of number to assign to anon hypothesis
- Normally in Type
- Since we derive the type from the proof term we have to apply increases in this number in the proof term
- Instead we keep track of it separately

```
pred do-iStartProof i:hole, o:ihole.
do-iStartProof (hole Type Proof) (ihole N (hole NType NProof)) :-
  coq.elaborate-skeleton {{ as_emp_valid_2 lp:Type _ (tac_start _ _) }} T
  Proof = {{ as_emp_valid_2 _ _ (tac_start _ lp:NProof) }},
  coq.typecheck NProof NType ok,
  NType = {{ envs_entails (Envs _ _ lp:N) _}}.
```

- Start proof applies start proof lemma
- Next extracts current anon hypotheses count
- Stores it in hole using new type ihole

```
kind ihole type.
type ihole term -> hole -> ihole. % ihole iris hyp counter, (hole type pr
```

- Counter is Coq positive since increasing it is fairly easy

```
pred increase-ctx-count i:term, o:term.
increase-ctx-count N NS :-
  coq.reduction.vm.norm {{ Pos.succ lp:N }} _ NS.
```

- We can increase counter and put it in the resulting `ihole` when necessary.

4.7.5 Continuation Passing Style

- When introducing a forall we need to add the variable to our context
- Next steps in the proof thus need the new value in the context
- We have to use continuation passing style

```
pred do-intro-anon i:hole, i:(hole -> prop).
do-intro-anon (hole Type Proof) C :-
  coq.ltac.fresh-id "a" {{ False }} ID,
  coq.id->name ID N,
  coq.elaborate-skeleton (fun N _ _) Type Proof ok,
  Proof = (fun _ T IntroFProof),
  @pi-decl N T x\
    coq.typecheck (IntroFProof x) (F x) ok,
    C (hole (F x) (IntroFProof x)).
```

- This introduces a variable without needing a name
- first two steps create the name of the variable
- Next we use a function as the proof term
- We extract the (term -> term) proof variable and the type
- Add the new variable to the context with the name
- Get the type of the new hole
- Call the continuation function on the hole in the context
- In our eiIntros tactic we will be calling predicates like `do-intro-anon` and thus we get a similar type

```
pred do-iIntros i:(list intro_pat), i:ihole, i:(ihole -> prop).
do-iIntros [] IH C :- !, C IH.
do-iIntros [iPure (none) | IPS] (ihole N (hole Type Proof)) C :-
  coq.elaborate-skeleton {{ tac_forall_intro_nameless _ _ _ _ _ _ }} Type
  Proof = {{ tac_forall_intro_nameless _ _ _ _ _ lp:IProof }},
  coq.typecheck IProof IType ok, !,
  do-intro-anon (hole IType IProof) (h\ sigma IntroProof\ sigma IntroType
    h = hole IntroType IntroProof,
    coq.reduction.lazy.bi-norm IntroType NormType, !,
    do-iIntros IPS (ihole N (hole NormType IntroProof)) C
  ).
```

- The predicate `do-iIntros` gets a list of intro patterns, an ihole and the continuation function
- Base case calls the cont. predicate
- Pure intro case

- First transform goal to put forall at the top of goal
- Then use `do-intro-anon` to introduce that variable
- Lastly normalize the type and call iIntros on the new hole
- No anon Iris hypotheses introduced thus counter stays the same

4.7.6 Backtracking in proofs

Question: We don't actually need to backtrack here, we can just look at the type and see which case we need

```
pred do-iIntro-ident i:ident, i:ihole, o:ihole.
do-iIntro-ident ID (ihole N (hole Type Proof))
                   (ihole N (hole IType IProof)) :-
  ident->term ID _ T,
  coq.elaborate-skeleton
    {{ tac_impl_intro _ lp:T _ _ _ _ _ _ _ }}
    Type Proof ok, !,
  Proof =
    {{ tac_impl_intro _ _ _ _ _ _ _ _ lp:IProof }},
  coq.typecheck IProof IType' ok,
  pm-reduce IType' IType,
  if (IType = {{ False }})
     (coq.error "eiIntro: " X " not fresh")
     (true).
do-iIntro-ident ID (ihole N (hole Type Proof))
                   (ihole N (hole IType IProof)) :-
  ident->term ID _ T,
  coq.elaborate-skeleton
    {{ tac_wand_intro _ lp:T _ _ _ _ _ }}
    Type Proof ok, !,
  Proof = {{ tac_wand_intro _ _ _ _ _ _ lp:IProof }},
  coq.typecheck IProof IType' ok,
  pm-reduce IType' IType,
  if (IType = {{ False }})
     (coq.error "eiIntro: " X " not fresh")
     (true).
do-iIntro-ident ID _ _ :-
  ident->term ID X _,
  coq.error "eiIntro: " X " could not introduce".
```

4.7.7 Starting the tactic

- Solve is the entry point

- Gets a goal with type proof and the arguments

```
solve (goal _ _ Type Proof [str Args]) GS :-
  tokenize Args T, !,
  parse_ipl T IPS, !,
  do-iStartProof (hole Type Proof) IH, !,
  do-iIntros IPS IH (ih\ set-ctx-count-proof ih _), !,
  coq.ltac.collect-goals Proof GL SG,
  all (open pm-reduce-goal) GL GL',
  std.append GL' SG GS.
```

- First we parse the arguments
- Ten start proof and get the ihole
- Then start do-iIntros where at the end we put the context counter in the proof
- ...
- ...

4.8 Writing commands

Chapter 5

Elpi implementation of Inductive

5.1 Functor

- We can also make commands
- What do we get as input for our commands
- What do we need to turn it in to
- Show example for isMLL

5.2 Monotone

5.2.1 Proper

- Write tactic for solving IProper proofs
- We write small tactics for different possible steps
- Simple steps, for respectful, point-wise, persistent
- Finishing steps for assumption and reflexive implication
- Apply other proper instance
- Find how many arguments to add to connective
- Lemma to get IProper instance from IProperTop instance
- Apply Lemma IProper
- Compose till all goals proven

5.2.2 Induction for proper

- Create Proper Type for fix-point
- Add point-wise for every constructor using fold-map
- Add this to left and right of respectful with a persistent around left-hand side
- Apply proper solver

5.3 Least fix-point

- The basic structure is this …
- We recurse over the type of the fix-point to introduce lambda's and existential quantification
- As the last step we add lambda's for any parameters we have

Bibliography

[BBR99] Catherine Belleannée, Pascal Brisset, and Olivier Ridoux. "A Pragmatic Reconstruction of λProlog". In: *The Journal of Logic Programming* 41.1 (Oct. 1, 1999), pp. 67–102. DOI: 10.1016/S0743-1066(98)10038-9.

[Dun+15] Cvetan Dunchev et al. "ELPI: Fast, Embeddable, λProlog Interpreter". In: *Log. Program. Artif. Intell. Reason.* Lecture Notes in Computer Science. 2015, pp. 460–468. DOI: 10.1007/978-3-662-48899-7_32.

[GCT19] Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. "Implementing Type Theory in Higher Order Constraint Logic Programming". In: *Math. Struct. Comput. Sci.* 29.8 (Sept. 2019), pp. 1125–1150. DOI: 10.1017/S0960129518000427.

[GMT16] Georges Gonthier, Assia Mahboubi, and Enrico Tassi. "A Small Scale Reflection Extension for the Coq System". PhD thesis. Inria Saclay Ile de France, 2016. URL: https://inria.hal.science/inria-00258384/document.

[HKP97] Gérard Huet, Gilles Kahn, and Christine Paulin-Mohring. "The Coq Proof Assistant a Tutorial". In: *Rapp. Tech.* 178 (1997). URL: http://www.itpro.titech.ac.jp/coq.8.2/Tutorial.pdf.

[Iri23] The Iris Team. "The Iris 4.1 Reference". In: (Oct. 11, 2023), pp. 51–56. URL: https://plv.mpi-sws.org/iris/appendix-4.1.pdf.

[Jun+15] Ralf Jung et al. "Iris: Monoids and Invariants as an Orthogonal Basis for Concurrent Reasoning". In: *Proc. 42nd Annu. ACM SIGPLAN-SIGACT Symp. Princ. Program. Lang.* POPL '15. Jan. 14, 2015, pp. 637–650. DOI: 10.1145/2676726.2676980.

[Jun+16] Ralf Jung et al. "Higher-Order Ghost State". In: *SIGPLAN Not.* 51.9 (Sept. 4, 2016), pp. 256–269. DOI: 10.1145/3022670.2951943.

[Jun+18] Ralf Jung et al. “Iris from the Ground up: A Modular Foundation for Higher-Order Concurrent Separation Logic”. In: *J. Funct. Program.* 28 (Jan. 2018), e20. DOI: 10.1017/S0956796818000151.

[Kre+17] Robbert Krebbers et al. “The Essence of Higher-Order Concurrent Separation Logic”. In: *Program. Lang. Syst.* Lecture Notes in Computer Science. 2017, pp. 696–723. DOI: 10.1007/978-3-662-54434-1_26.

[Kre+18] Robbert Krebbers et al. “MoSeL: A General, Extensible Modal Framework for Interactive Proofs in Separation Logic”. In: *Proc. ACM Program. Lang.* 2 (ICFP July 30, 2018), 77:1–77:30. DOI: 10.1145/3236772.

[KTB17] Robbert Krebbers, Amin Timany, and Lars Birkedal. “Interactive Proofs in Higher-Order Concurrent Separation Logic”. In: *SIGPLAN Not.* 52.1 (Jan. 1, 2017), pp. 205–217. DOI: 10.1145/3093333.3009855.

[Mil+91] Dale Miller et al. “Uniform Proofs as a Foundation for Logic Programming”. In: *Annals of Pure and Applied Logic* 51.1 (Mar. 14, 1991), pp. 125–157. DOI: 10.1016/0168-0072(91)90068-W.

[MN12] Dale Miller and Gopalan Nadathur. *Programming with Higher-Order Logic*. 2012. DOI: 10.1017/CBO9781139021326.

[MN86] Dale A. Miller and Gopalan Nadathur. “Higher-Order Logic Programming”. In: *Third Int. Conf. Log. Program.* Lecture Notes in Computer Science. 1986, pp. 448–462. DOI: 10.1007/3-540-16492-8_94.

[Mon11] Eric Monfroy. “Constraint Handling Rules by Thom Frühwirth, Cambridge University Press, 2009. Hard Cover: ISBN 978-0-521-87776-3.” In: *Theory Pract. Log. Program.* 11.1 (Jan. 2011), pp. 125–126. DOI: 10.1017/S1471068410000074.

[Tar55] Alfred Tarski. “A Lattice-Theoretical Fixpoint Theorem and Its Applications”. In: *Pac. J. Math.* 5.2 (June 1, 1955), pp. 285–309. URL: https://msp.org/pjm/1955/5-2/p11.xhtml.

[Tas18] Enrico Tassi. “Elpi: An Extension Language for Coq (Metaprogramming Coq in the Elpi λProlog Dialect)”. Jan. 2018. URL: https://inria.hal.science/hal-01637063.