Iris: Higher-Order Concurrent Separation Logic

Lecture 2: Basic Logic of Resources

Lars Birkedal

Aarhus University, Denmark

September 15, 2020
Overview

Earlier:
- Operational Semantics of $\lambda_{\text{ref,conc}}$
  - $e, (h, e) \leadsto (h, e')$, and $(h, E) \rightarrow (h', E')$

Today:
- Basic Logic of Resources
  - $l \leftrightarrow v$, $P \ast Q$, $P \not\ast Q$, $\Gamma \vdash P \vdash Q$
A higher-order separation logic over a simple type theory with new base types and base terms defined in signature $S$.

Terms and types are as in simply typed lambda calculus, types include a type Prop of propositions.

Do not confuse the lambda calculus of Iris with the programming language lambda abstractions in $\lambda_{\text{ref,conc}}$.

- The lambda calculus of Iris is an equational theory of functions, no operational semantics (think standard mathematical functions)
- In $\lambda_{\text{ref,conc}}$ one can define functions whose behaviour is defined by the operational semantics of $\lambda_{\text{ref,conc}}$
Syntax: Types

\[ \tau ::= T | \mathbb{Z} | Val | Exp | Prop | 1 | \tau + \tau | \tau \times \tau | \tau \rightarrow \tau \]

where

- \( T \) stands for additional base types which we will add later
- \( Val \) and \( Exp \) are types of values and expressions in \( \lambda_{\text{ref,conc}} \)
- Prop is the type of Iris propositions.
Syntax: Terms

\[ t, P ::= x | n | v | e | F(t_1, \ldots, t_n) | (\cdot) | (t, t) | \pi_i \cdot t | \lambda x : \tau. t | t(t) | \text{inl} \cdot t | \text{inr} \cdot t | \text{case}(t, x.t, y.t) | \text{False} | \text{True} | t =_\tau t | P \Rightarrow P | P \land P | P \lor P | P \ast P | P \rightarrow P | \exists x : \tau. P | \forall x : \tau. P | \square P | \blacklozenge P | \{P\} t \{P\} | t \hookrightarrow t \]

where

- \( x \) are variables
- \( n \) are integers
- \( v \) and \( e \) range over values of the language, i.e., they are primitive terms of types \( \text{Val} \) and \( \text{Exp} \)
- \( F \) ranges over the function symbols in the signature \( S \).
Well-typed Terms ($\Gamma \vdash_S t : \tau$)

- Typing relation 
  \[ \Gamma \vdash_S t : \tau \]
  
  defined inductively by inference rules.

- Here $\Gamma = x_1 : \tau_1, x_2 : \tau_2, \ldots, x_n : \tau_n$ is a context, assigning types to variables

- Selected rules:
  \[ \Gamma, x : \tau \vdash t : \tau' \]
  \[ \frac{\Gamma \vdash t : \tau \rightarrow \tau' \quad u : \tau}{\Gamma \vdash t(u) : \tau'} \]
  \[ \frac{\Gamma \vdash \lambda x. t : \tau \rightarrow \tau'}{\Gamma \vdash \text{True} : \text{Prop}} \]
  \[ \frac{\Gamma \vdash t : \tau \quad \Gamma \vdash u : \tau}{\Gamma \vdash t =_\tau u : \text{Prop}} \]
  \[ \frac{\Gamma \vdash P : \text{Prop} \quad \Gamma \vdash Q : \text{Prop}}{\Gamma \vdash P \Rightarrow Q : \text{Prop}} \]
  \[ \frac{\Gamma \vdash \forall x : \tau. P : \text{Prop}}{\Gamma, x : \tau \vdash P : \text{Prop}} \]
Entailment \((\Gamma \vdash P \vdash Q)\)

- Entailment relation
  \[
  \Gamma \vdash P \vdash Q
  \]
  for \(\Gamma \vdash P : \text{Prop}\) and \(\Gamma \vdash Q : \text{Prop}\).

- The relation is defined by induction, using standard rules from intuitionistic higher-order logic extended with new rules for the new connectives.

- We only have one proposition \(P\) on the left of the turnstile.
  - You may be used to seeing a list of assumptions separated by commas
  - Instead we extend the context by using \(\wedge\)
  - This choice makes it easy to extend the context also with \(*\).

- To understand the entailment rules for the new connectives, we need to have an intuitive understanding of the semantics of the logical connectives.

- Note: in this course, we do not present a formal semantics of the logic and formally prove the logic sound (for that, see “Iris from the Ground Up: A Modular Foundation for Higher-Order Concurrent Separation Logic” on iris-project.org).
Let us do some exercises in standard Intuitionistic Higher-Order Logic before moving on to the new connectives.
\( \land \) is commutative

\[
\begin{align*}
P \land Q & \vdash P \land Q \\
P \land Q & \vdash Q \\
P \land Q & \vdash P \\
P \land Q & \vdash Q \land P
\end{align*}
\]
Weakening for $\wedge$

First observe:

$$\frac{P \land R \vdash P \land R}{P \land R \vdash P}$$

Then use transitivity to show:

by above

$$\frac{P \land R \vdash P \quad P \vdash Q}{P \land R \vdash Q}$$

Thus we have:

$$\frac{P \vdash Q}{P \land R \vdash Q}$$

i.e., we can weaken on the left (thinking bottom-up).
∧ is associative

Use weakening on the left from above:

\[
\begin{align*}
(P \land Q) \land R &\vdash P \\
(P \land Q) \land R &\vdash Q \\
(P \land Q) \land R &\vdash R
\end{align*}
\]
Adjoint Rules for $\land$ and $\Rightarrow$

Double rule (applicable from top to bottom and from bottom to top):

\[
\frac{R \land P \vdash Q}{R \vdash P \Rightarrow Q}
\]

Proof from top to bottom: directly by $\Rightarrow$I.

Proof from bottom to top:

\[
\frac{P \Rightarrow Q \vdash P \Rightarrow Q}{(P \Rightarrow Q) \land P \vdash P \Rightarrow Q} \quad \frac{(P \Rightarrow Q) \land P \vdash P \Rightarrow Q}{(P \Rightarrow Q) \land P \vdash P} \quad \frac{P \vdash P}{\Rightarrow E}
\]

\[
\frac{R \vdash P \Rightarrow Q \quad P \vdash P}{R \land P \vdash (P \Rightarrow Q) \land P} \quad \frac{(P \Rightarrow Q) \land P \vdash P \Rightarrow Q}{(P \Rightarrow Q) \land P \vdash P} \quad \frac{(P \Rightarrow Q) \land P \vdash P}{\text{TRANS}}
\]

\[
R \land P \vdash Q
\]
\( \land \) is greatest lower bound wrt. entailment

The \( \land I \) and \( \land E \) rules immediately give the following double rule:

\[
\begin{array}{c}
R \vdash P & R \vdash Q \\
\hline
R \vdash P \land Q
\end{array}
\]
\( \lor \) is least upper bound wrt. entailment

We can also show that \( \lor \) is least upper bound wrt. entailment, i.e., claim:

\[
\begin{align*}
P & \vdash R \\
Q & \vdash R
\end{align*}
\]

\[P \lor Q \vdash R\]

Proof from top to bottom:

\[
\begin{array}{c}
P \lor Q \vdash P \lor Q \\
\hline
P \vdash R \\
(P \lor Q) \land P \vdash R \\
\hline
Q \vdash R \\
(P \lor Q) \land Q \vdash R \\
\hline
\hline
P \lor Q \vdash R
\end{array}
\]

\( \lor\text{E} \)

From bottom to top:

\[
\begin{array}{c}
P \vdash P \\
\hline
P \vdash P \lor Q \\
P \lor Q \vdash R \\
\hline
P \vdash R
\end{array}
\]

(likewise to conclude \( Q \vdash R \)).
\( \land \) distributes over / preserves \( \lor \): \( P \land (Q \lor R) \vdash (P \land Q) \lor (P \land R) \)

Proof idea: use the adjoint rules for \( \land \) and \( \Rightarrow \) from above. (In the proof we also use the least upper bound rule for \( \lor \) from above). Proof left-to-right:

\[
\begin{align*}
  P \land Q & \vdash P \land Q \\
  P \land Q & \vdash (P \land Q) \lor (P \land R) \\
  Q & \vdash P \Rightarrow (P \land Q) \lor (P \land R) \\
  P \land R & \vdash P \land R \\
  P \land R & \vdash (P \land Q) \lor (P \land R) \\
  R & \vdash P \Rightarrow (P \land Q) \lor (P \land R) \\
  Q \lor R & \vdash P \Rightarrow (P \land Q) \lor (P \land R) \\
  P \land (Q \lor R) & \vdash (P \land Q) \lor (P \land R)
\end{align*}
\]

Proof right-to-left:

\[
\begin{align*}
  P & \vdash P \\
  P \land Q & \vdash P \\
  (P \land Q) \lor (P \land R) & \vdash P \\
  Q & \vdash Q \lor R \\
  Q \land Q & \vdash Q \lor R \\
  R & \vdash Q \lor R \\
  R \land R & \vdash Q \lor R \\
  (P \land Q) \lor (P \land R) & \vdash Q \lor R \\
  (P \land Q) \lor (P \land R) & \vdash P \land (Q \lor R)
\end{align*}
\]
Negation

Define $\neg P = P \Rightarrow \text{False}$.

Then $\neg P \vdash \forall Q : \text{Prop}. P \Rightarrow Q$.

Proof:

\[
\frac{
\frac{
\frac{
\text{False} \vdash \text{False}
}{\text{False} \vdash Q}
}{\text{False} \vdash Q}
}{\text{False} \Rightarrow \text{False} \land P \vdash Q}
\]

\[
\frac{
\frac{
\frac{
\frac{
\frac{
\text{False} \vdash \text{False}
}{\text{False} \vdash Q}
}{\text{False} \vdash Q}
}{\text{False} \Rightarrow \text{False} \land P \vdash Q}
}{\text{False} \Rightarrow \text{False} \land P \vdash Q}
}{\neg P \vdash P \Rightarrow Q}
\]

\[
\frac{
\frac{
\frac{
\frac{
\frac{
\frac{
\text{False} \vdash \text{False}
}{\text{False} \vdash Q}
}{\text{False} \vdash Q}
}{\text{False} \Rightarrow \text{False} \land P \vdash Q}
}{\text{False} \Rightarrow \text{False} \land P \vdash Q}
}{\neg P \vdash P \Rightarrow Q}
}{\neg P \vdash \forall Q : \text{Prop}. P \Rightarrow Q}
\]
Adjoint Rule for ∀

\[ \frac{\Gamma | Q \vdash \forall x : \tau. P}{\Gamma, x : \tau | Q \vdash P} \]

(here it is assumed that \( x \not\in \text{FV}(Q) \) so that \( Q \) is well-formed in \( \Gamma \)).

Proof from bottom to top: directly by ∀I.

Proof from top to bottom:

\[ \frac{\Gamma | Q \vdash \forall x : \tau. P}{\Gamma, x : \tau | Q \vdash \forall x : \tau. P} \]
\[ \frac{\Gamma, x : \tau | \vdash x : \tau}{\text{∀E}} \]
\[ \frac{\Gamma, x : \tau | Q \vdash P[x/x]}{\Gamma, x : \tau | Q \vdash P} \text{ since } P[x/x] = P \]

(note: we use weakening for the variable context on the left)
Adjoint Rule for $\exists$

$$\Gamma \mid \exists x : \tau. P \vdash Q$$

$$\frac{}{\Gamma, x : \tau \mid P \vdash Q}$$

(here it is assumed that $x \notin \text{FV}(Q)$ so that $Q$ is well-formed in $\Gamma$).

Proof from bottom to top:

$$\frac{}{\Gamma \mid \exists x : \tau. P \vdash \exists x : \tau. P}$$

$$\frac{}{\Gamma, x : \tau \mid \exists x : \tau. P \vdash Q}$$

$$\frac{\Gamma, x : \tau \mid \exists x : \tau. P \vdash Q}{\Gamma \mid \exists x : \tau. P \vdash Q}$$

Proof from top to bottom:

$$\frac{\Gamma, x : \tau \vdash x : \tau}{\Gamma, x : \tau \mid P \vdash P[x/x]}$$

$$\frac{\Gamma, x : \tau \mid P \vdash \exists x : \tau. P}{\Gamma, x : \tau \mid P \vdash Q}$$

$$\frac{\Gamma, x : \tau \mid \exists x : \tau. P \vdash Q}{\Gamma, x : \tau \mid \exists x : \tau. P \vdash Q}$$

$$\frac{\Gamma, x : \tau \mid \exists x : \tau. P \vdash Q}{\Gamma \mid \exists x : \tau. P \vdash Q}$$
∧ distributes over \( \exists \): \( P \land \exists x : \tau. Q \vdash \exists x : \tau. P \land Q \)

Proof idea: the same as for \( \land \) distributes over \( \lor \) (think: \( \lor \) is binary disjunction, \( \exists \) is finite or infinite disjunction (depending on type \( \tau \)), the distribution over arbitrary disjunctions follows from the adjoint rule for \( \land \) and \( \Rightarrow \) earlier.)

In the proof we use the adjoint rules for \( \exists \) described above.

Proof left-to-right:

\[
\begin{align*}
\Gamma & \vdash \exists x : \tau. P \land Q \vdash \exists x : \tau. P \land Q \\
\Gamma, x : \tau & \vdash P \land Q \vdash \exists x : \tau. P \land Q \\
\Gamma, x : \tau & \vdash Q \vdash P \Rightarrow \exists x : \tau. P \land Q \\
\Gamma & \vdash \exists x : \tau. Q \vdash P \Rightarrow \exists x : \tau. P \land Q \\
\Gamma & \vdash P \land \exists x : \tau. Q \vdash \exists x : \tau. P \land Q
\end{align*}
\]

Proof right-to-left:

\[
\begin{align*}
\Gamma, x : \tau & \vdash P \vdash P \\
\Gamma, x : \tau & \vdash P \land Q \vdash P \land \exists x : \tau. Q \\
\Gamma, x : \tau & \vdash \exists x : \tau. P \vdash P \land \exists x : \tau. Q
\end{align*}
\]
$\vdash \forall P, Q : \text{Prop.} \ (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

With the context of variables explicit:

$\vdash \forall P, Q : \text{Prop.} \ (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$
$P : \text{Prop} \mid P \vdash \neg
\neg P$

In English: Suppose $P$ holds. To show $\neg
\neg P$, so assume $\neg P$ and show False. But now we have assume both $P$ and $\neg P$ and hence we get False, as desired. Done.
∃ commuting with \( \lor \): \( \exists x : \tau. P \lor Q \vdash \exists x : \tau. P \lor \exists x : \tau. Q \)

Proof of left-to-right:

| \( x : \tau | P \vdash P \) | \( x : \tau \vdash x : \tau \) |
| \hline
| \( x : \tau | P \vdash \exists x : \tau. P \) | \( x : \tau | Q \vdash Q \) |
| \hline
| \( x : \tau | P \vdash \exists x : \tau. P \lor \exists x : \tau. Q \) | \( x : \tau | Q \vdash \exists x : \tau. Q \) |
| \hline
| \( x : \tau | P \lor Q \vdash \exists x : \tau. P \lor \exists x : \tau. Q \) | \( \exists x : \tau. P \lor Q \vdash \exists x : \tau. P \lor \exists x : \tau. Q \) |
Proof of right-to-left:

\[
\begin{align*}
 P & \vdash P \\
 P & \vdash P \lor Q \\
 \exists x. P & \vdash \exists x. P \lor Q \\
 Q & \vdash Q \\
 Q & \vdash P \lor Q \\
 \exists x. Q & \vdash \exists x. P \lor Q \\
 \exists x. P \lor \exists x. Q & \vdash \exists x. P \lor Q
\end{align*}
\]

Here we have used monotonicity of \( \exists x \):

\[
\Gamma, x : \tau \mid P \vdash Q \\
\Gamma \mid \exists x : \tau.P \vdash \exists x : \tau.Q
\]

which holds because:

\[
\begin{align*}
 \Gamma, x : \tau \mid P \vdash Q & \quad \Gamma, x : \tau \vdash x : \tau \\
 \Gamma, x : \tau \mid P \vdash \exists x : \tau.Q & \\
 \Gamma, x : \tau \mid P \vdash \exists x : \tau.Q & \\
 \Gamma \mid \exists x : \tau.P \vdash \exists x : \tau.Q
\end{align*}
\]
Intuition for Iris Propositions

- **Intuition**: A proposition $P$ describes a set of resources.
- Write $\mathcal{R}$ for the set of resources, and write $r_1$, $r_2$, etc., for elements in $\mathcal{R}$.
- We assume that
  - there is an empty resource
  - there is a way to compose (or combine) resources $r_1$ and $r_2$, denoted $r_1 \cdot r_2$
  - the composition is defined for resources that are suitably disjoint, denoted $r_1 \# r_2$.
- Later on we will formalize such notions of resources using certain commutative monoids. For now, it suffices to think about the example of $\mathcal{R} = \text{Heap}$.
Intuition for Iris Propositions

- Canonical example: $R = Heap$, the set of heaps from $\lambda_{\text{ref,conc}}$.
- Recall: $Heap = \text{Loc} \xrightarrow{\text{fin}} Val$, the set of partial functions from locations to values.
- The empty resource is the empty heap, denoted $[]$.
- Two heaps $h_1$ and $h_2$ are disjoint, denoted $h_1 \not\# h_2$, if their domains do not overlap ($i.e.$, $\text{dom}(h_1) \cap \text{dom}(h_2) = \emptyset$).
- The composition of two disjoint heaps $h_1$ and $h_2$ is the heap $h = h_1 \cdot h_2$ defined by

$$h(x) = \begin{cases} h_1(x) & \text{if } x \in \text{dom}(h_1) \\ h_2(x) & \text{if } x \in \text{dom}(h_2) \end{cases}$$
Intuition for Iris Propositions

- We said: “A proposition $P$ describes a set of resources.”
- Also say: “$P$ is a set of resources.”
- Also say: “$P$ denotes a set of resources.”
- $P \in P(\mathcal{R})$.
- When $r$ is a resource described by $P$, we also say that $r$ satisfies $P$, or that $r$ is in $P$.
- The intuition for $P \vdash Q$ is then that all resources in $P$ are also in $Q$ (i.e., $\forall r \in \mathcal{R}. \ r \in P \Rightarrow r \in Q$).
Describing Resources in the Logic

▶ Primitive: the points-to predicate $x \leftrightarrow v$.
▶ It is a formula, i.e., a term of type Prop

\[
\Gamma \vdash \ell : Val \quad \Gamma \vdash v : Val \\
\Gamma \vdash \ell \leftrightarrow v : Prop
\]

▶ It describes the set of heap fragments that map location $x$ to value $v$

\[
x \leftrightarrow v = \{h \mid x \in \text{dom}(h) \land h(x) = v\}
\]

▶ Ownership reading: if I assert $\ell \leftrightarrow v$, then I express that I have the ownership of $\ell$ and hence I may modify what $\ell$ points to, without invalidating invariants of other parts of the program.
Intuition for $\star$ and $\rightsquigarrow$

- $P \star Q = \{ r \mid \exists r_1, r_2. r = r_1 \cdot r_2 \land r_1 \in P \land r_2 \in Q\}$
- For example, $x \mapsto u \star y \mapsto v$ describes the set of heaps with two disjoint locations $x$ and $y$, the first stores $u$ and the second $v$.
- Note: $x \mapsto v \star x \mapsto u \vdash \text{False}$.
- $P \rightsquigarrow Q = \{ r \mid \forall r_1. r_1 \# r \land r_1 \in P \Rightarrow r \cdot r_1 \in Q\}$
- For example, the proposition

$$x \mapsto u \rightsquigarrow (x \mapsto u \star y \mapsto v)$$

describes those heap fragments that map $y$ to $v$, because when we combine it with a heap fragment mapping $x$ to $u$, then we get a heap fragment mapping $x$ to $u$ and $y$ to $v$. 
Weakening Rule

Weakening rule:

\[ \text{*-WEAK} \]

\[ P_1 * P_2 \vdash P_1 \]

- Thus Iris is an **affine** separation logic.
- Example:
  \[ x \leftrightarrow u \star y \leftrightarrow v \vdash x \leftrightarrow u \]
  
  - Suppose \( h \in (x \leftrightarrow u \star y \leftrightarrow v) \).
  - Then \( h(x) = u \) and \( h(y) = v \).
  - Therefore \( h \in (x \leftrightarrow u) \).
  - Generally, if \( h \in P \) and \( h' \geq h \), then also \( h' \in P \).
Weakening Rule

In a bit more detail:

- **Intuitively**, the fact that this rule is sound means that propositions are interpreted by upwards closed sets of resources:
  - We say that $r_1 \geq r_2$ iff $r_1 = r_2 \cdot r_3$, for some $r_3$.
  - Suppose $r_1 \in P_1$ and that $r \geq r_1$. Then there is $r_2$ such that $r = r_1 \cdot r_2$.
  - Let $P_2$ be $\{r_2\}$.
  - Then $r_1 \cdot r_2 \in P_1 \ast P_2$.
  - By the weakening rule, we then also have that $r = r_1 \cdot r_2 \in P_1$.
  - Hence $P_1$ is upwards closed.
- The above is not a formal proof, hence the stress on “intuitively”.

Associativity and Commutativity of $\ast$

Basic structural rules:

\[
\frac{\ast}{\text{\textsc{*-assoc}}} P_1 \ast (P_2 \ast P_3) \vdash (P_1 \ast P_2) \ast P_3
\]

\[
\frac{}{\text{\textsc{*-comm}}} P_1 \ast P_2 \vdash P_2 \ast P_1
\]

Sound because composition of resources, $\cdot$, is commutative and associative.
Separating Conjunction Introduction

To show a separating conjunction $Q_1 \ast Q_2$, we need to split the assumption and decide which resources to use to prove $Q_1$ and which ones to use to prove $Q_2$.

Example: $P \vdash P \ast P$ is not provable in general
Introduction rule intuitively sound because

- Suppose $r \in R$. TS $r \in P \rightarrow Q$.
- Thus let $r_1 \in P$ and suppose $r_1 \neq r$. TS $r \cdot r_1 \in Q$.
- We have $r \cdot r_1 \in R \cdot P$.
- Hence, by antecedent, $r \cdot r_1 \in Q$, as required.

Elimination rule intuitively sound because

- ...