Later Credits

Resourceful Reasoning for the Later Modality

Simon Spies, Lennard Gäher, Joseph Tassarotti, Ralf Jung,
Robbert Krebbers, Lars Birkedal, Derek Dreyer

Iris Workshop, May 2022
The Historic Foundation of Iris

Step-Indexed Logical Relations

Separation Logic
A Powerful Combination

Example: RustBelt

- step-indexing for recursive types
- separation logic for ownership types
Step-indexing enables recursive reasoning Löb induction, higher-order ghost state, …

but introduces irritating step-indexing artifacts. the later modality $P$
Running Example: Impredicative Invariants

**Opening Invariants** (from Iris 1.0)

\[
{P \ast R} e {Q \ast R} \quad e \text{ atomic}
\]

\[
\frac{}{R \vdash \{ P \} e \{ Q \}}
\]
Running Example: Impredicative Invariants

Actually ... later modality masks

\[
\{ P \triangleright R \} \ e \ \{ v. Q \triangleright R \}_{\mathcal{E}\setminus\mathcal{N}} \quad e \ \text{atomic} \quad \mathcal{N} \subseteq \mathcal{E}
\]

because invariants in Iris are step-indexed.
The later modality prevents inconsistent proofs, \( \triangleright R \) is sound, \( R \) not necessarily.

But in proofs we worry mostly about removing it. We want \( R \), not \( \triangleright R \).
Example: A Typical Iris Proof

\[ \exists n : \mathbb{N}. \ell \mapsto n \vdash \{ \text{True} \} !\ell \{ v. v \in \mathbb{N} \} \]
Example: A Typical Iris Proof

\[
\proves \left\{ \downarrow (\exists n : \mathbb{N}. \ell \mapsto n) \right\} !\ell \left\{ v. v \in \mathbb{N}^* \downarrow (\exists n : \mathbb{N}. \ell \mapsto n) \right\} \\
\exists n : \mathbb{N}. \ell \mapsto n \proves \left\{ \text{True} \right\} !\ell \left\{ v. v \in \mathbb{N} \right\}
\]
Example: A Typical Iris Proof

\[
\vdash \{ (\exists n : \mathbb{N}. \ell \mapsto n) \} !\ell \{ v. v \in \mathbb{N} \ast \triangleright (\exists n : \mathbb{N}. \ell \mapsto n) \}
\]

\[
\vdash \{ (\exists n : \mathbb{N}. \ell \mapsto n) \} !\ell \{ v. v \in \mathbb{N} \ast \triangleright (\exists n : \mathbb{N}. \ell \mapsto n) \}
\]

\[
\exists n : \mathbb{N}. \ell \mapsto n \vdash \{ \text{True} \} !\ell \{ v. v \in \mathbb{N} \}
\]
The Later Elimination Problem
We have \(\triangleright R\) in our context, but we need \(R\) to proceed.

Existing Options
- Timeless Propositions
- Commuting Rules
- Program Steps
We have to solve …

The Later Elimination Problem
We have \( \triangleright R \) in our context, but we need \( R \) to proceed.

Existing Options

- Timeless Propositions

\[
\begin{align*}
\{ P \star R \} & \quad e \quad \{ v. \ Q \} \quad \text{timeless}(R) \\
\Rightarrow \quad \{ P \triangleright R \} & \quad e \quad \{ v. \ Q \} \\
\text{timeless}(\ell \mapsto v)
\end{align*}
\]

- Commuting Rules

- Program Steps
We have to solve ...

The Later Elimination Problem
We have $\triangleright R$ in our context, but we need $R$ to proceed.

Existing Options

- Timeless Propositions
- Commuting Rules
  \[ \triangleright (P \ast Q) \vdash \triangleright P \ast \triangleright Q \]
  \[ \triangleright (\exists x. P) \vdash \exists x. \triangleright P \]
- Program Steps
We have to solve …

The Later Elimination Problem
We have $\triangleright R$ in our context, but we need $R$ to proceed.

Existing Options
- Timeless Propositions
- Commuting Rules
- Program Steps

\[
\begin{align*}
\{R\} e' \{v. \, Q\} & \quad e \rightarrow_{\text{pure}} e' \\
\{\triangleright R\} e \{v. \, Q\} & \quad \cdots
\end{align*}
\]
Limitations of the Existing Options

*Existing options apply* to most invariants

\[
R = \exists n : \mathbb{N}. \ell \mapsto n \quad \text{where} \quad \exists n : \mathbb{N}. \ell \mapsto n \quad \text{timeless}
\]
Limitations of the Existing Options

Existing options apply to most invariants

$$R = \exists n : \mathbb{N}. \ell \mapsto n$$ where $$\exists n : \mathbb{N}. \ell \mapsto n$$ timeless

But they are no silver bullet. They do not apply to

$$R = \exists n : \mathbb{N}. \ell \mapsto n$$ where $$\exists n : \mathbb{N}. \ell \mapsto n$$ not timeless
We are stuck ...

$$\vdash \{ \triangleright (\exists n : N. \ell \leftrightarrow n) \} !\ell \{ v. v \in N \ast \triangleright (\exists n : N. \ell \leftrightarrow n) \}$$

$$\exists n : N. \ell \leftrightarrow n \vdash \{ \text{True} \} !\ell \{ v. v \in N \}$$

invariant guarded by a later
So what then?

“Help …”
So what then?

“Help …

Have you tried these non-local refactorings of your proof

- flattening your invariant hierarchy

or considered giving up?
Developing a Fourth Option

How about using this pillar to develop another option?
Later credits turn the right to eliminate a later transform $R$ into $R$ into an ownable resource, which is subject to a later credit £1, traditional separation logic reasoning, passing around, framing, sharing via invariants.
Later Credits in a Nutshell

\[
\begin{align*}
\{ R \} e' \{ v. Q \} & \quad e \rightarrow_{\text{pure}} e' \\
\{ R \} e \{ v. Q \} & \\
\{ \triangleright R \} e \{ v. Q \}
\end{align*}
\]

becomes

\[
\begin{align*}
\{ R \ast \mathcal{L} 1 \} e' \{ v. Q \} & \quad e \rightarrow_{\text{pure}} e' \\
\{ R \} e \{ v. Q \} & \\
\{ \mathcal{L} 1 \ast \triangleright R \} e \{ v. Q \}
\end{align*}
\]
Novelty: Prepaid Reasoning

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \} f(41 + 1); !\ell \{ v. v \in \mathbb{N} \} \]

we obtain £1

we spend £1
Prepaid Reasoning in Action

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \} \ f(41 + 1); !\ell \ \{v. \ v \in \mathbb{N}\} \]
Prepaid Reasoning in Action

\[
\{ \exists n : \mathbb{N} . \ell \mapsto n \} * \mathcal{L} 1 \} \quad f(42); !\ell \{v. v \in \mathbb{N}\}
\]

\[
\{ \exists n : \mathbb{N} . \ell \mapsto n \} \quad f(41 + 1); !\ell \{v. v \in \mathbb{N}\}
\]
Prepaid Reasoning in Action

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \} \ast \mathcal{L} 1 \, f(42); \! \ell \{v. \, v \in \mathbb{N}\} \]

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \} \, f(41 + 1); \! \ell \{v. \, v \in \mathbb{N}\} \]
Prepaid Reasoning in Action

{∃n : ℕ. ℓ ↦→ n} * L 1 \{v. v ∈ ℕ\}

{∃n : ℕ. ℓ ↦→ n} f(42); !l \{v. v ∈ ℕ\}

{∃n : ℕ. ℓ ↦→ n} f(41 + 1); !l \{v. v ∈ ℕ\}
Prepaid Reasoning in Action

\[ \{ (\exists n : \mathbb{N}. \ell \mapsto n) \* \ell 1 \} !\ell \{ v. v \in \mathbb{N} \* \ell (\exists n : \mathbb{N}. \ell \mapsto n) \} \]

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \* \ell 1 \} !\ell \{ v. v \in \mathbb{N} \} \]

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \* \ell 1 \} f(42); !\ell \{ v. v \in \mathbb{N} \} \]

\[ \{ \exists n : \mathbb{N}. \ell \mapsto n \} f(41 + 1); !\ell \{ v. v \in \mathbb{N} \} \]
Prepaid Reasoning in Action

we spend our credit

\[
\{ \vdash (\exists n : \mathbb{N}. \ell \mapsto n) \ast \mathcal{L} 1 \} \ \mathcal{L} \ \{ v. v \in \mathbb{N} \ast \vdash (\exists n : \mathbb{N}. \ell \mapsto n) \}
\]

\[
\{ \exists n : \mathbb{N}. \ell \mapsto n \ast \mathcal{L} 1 \} \ \mathcal{L} \ \{ v. v \in \mathbb{N} \}
\]

\[
\{ \exists n : \mathbb{N}. \ell \mapsto n \ast \mathcal{L} 1 \} \ f(42); \ \mathcal{L} \ \{ v. v \in \mathbb{N} \}
\]

\[
\{ \exists n : \mathbb{N}. \ell \mapsto n \} \ f(41 + 1); \ \mathcal{L} \ \{ v. v \in \mathbb{N} \}
\]
Prepaid Reasoning in Action

\[
\begin{align*}
\forall \ell \{ v.v \in \mathbb{N} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \} !\ell \{ v.v \in \mathbb{N} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \} \\
\forall \ell \{ v.v \in \mathbb{N} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \\
\forall \ell \{ v.v \in \mathbb{N} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \} \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \Rightarrow (\exists n : \mathbb{N}. \ell \mapsto n) \\
\end{align*}
\]
Application: Prepaid Invariants
sharing later credits via invariants

Application: Logical Atomicity
cleaning up existing proofs

Theory and Soundness
the intuition on a napkin
Application: Prepaid Invariants
sharing later credits via invariants

Application: Logical Atomicity
cleaning up existing proofs

Theory and Soundness
the intuition on a napkin
Do we really need a later?

That cannot be sound, can it?
Later Credits in Invariants

**Idea:** We **prepay** the later elimination

\[
R_{\text{pre}} \triangleq R * \mathcal{L} 1
\]

such that we get **direct access** to \( R \).

\[
\{ R * P \} e \{ v. \ Q * R * \mathcal{L} 1 \} e \text{ atomic}
\]

\[
R_{\text{pre}} \vdash \{ P \} e \{ v. \ Q \}
\]
Idea: We prepay the later elimination

$$R_{\text{pre}} \triangleq R \ast \mathcal{L} 1$$

such that we get direct access to $R$.

$$\{R \ast P\} e \{v. Q \ast R \ast \mathcal{L} 1\} \quad e \quad \text{atomic}$$

$$R_{\text{pre}} \vdash \{P\} e \{v. Q\}$$

generated by the next step
Later Credits in Invariants

**Idea:** We **prepay** the later elimination

\[ R \text{\_pre } \triangleq R \ast \mathcal{L} 1 \]

such that we get **direct access** to \( R \).

\[
\begin{align*}
\{R \ast P\} e \{v. \ Q \ast R \ast \mathcal{L} 1\} \\
\{\mathcal{L} 1 \ast \triangleright (R \ast P)\} e \{v. \ Q \ast R \ast \mathcal{L} 1\} \\
\triangleright \mathcal{L} 1 \ast \triangleright (R \ast P)\} e \{v. \ Q \ast R \ast \mathcal{L} 1\} \\
\{P \ast \triangleright (R \ast \mathcal{L} 1)\} e \{v. \ Q \ast \triangleright (R \ast \mathcal{L} 1)\} \\
R \text{\_pre } \vdash \{ P \} e \{v. \ Q\}
\end{align*}
\]

spend credit  

timelessness of \( \mathcal{L} n \)  

later shuffling  

open invariant
Later Credits in Invariants

**Idea:** We **prepay** the later elimination

\[ R_{\text{pre}} \triangleq R \ast \ell 1 \]

such that we get **direct access** to \( R \).

\[
\begin{align*}
\{ R \ast P \} e & \{ v. Q \ast R \ast \ell 1 \} \\
\{ \ell 1 \ast \triangleright (R \ast P) \} e & \{ v. Q \ast R \ast \ell 1 \} \\
\triangleright \ell 1 \ast \triangleright (R \ast P) e & \{ v. Q \ast R \ast \ell 1 \} \\
\{ P \ast \triangleright (R \ast \ell 1) \} e & \{ v. Q \ast \triangleright (R \ast \ell 1) \} \\
R_{\text{pre}} \vdash & \{ P \} e \{ v. Q \}
\end{align*}
\]

spend credit

timelessness of \( \ell n \)
later shuffling
open invariant
Later Credits in Invariants

**Idea:** We *prepay* the later elimination

\[ R_{\text{pre}} \triangleq R \ast \mathcal{L} 1 \]

such that we get **direct access** to \( R \).

\[
\begin{align*}
\{ R \ast P \} & \models \{ v. Q \ast R \ast \mathcal{L} 1 \} \\
\{ \mathcal{L} 1 \ast \triangleright (R \ast P) \} & \models \{ v. Q \ast R \ast \mathcal{L} 1 \} \\
\triangleright \mathcal{L} 1 \ast \triangleright (R \ast P) & \models \{ v. Q \ast R \ast \mathcal{L} 1 \} \\
\{ P \ast \triangleright (R \ast \mathcal{L} 1) \} & \models \{ v. Q \ast \triangleright (R \ast \mathcal{L} 1) \} \\
\end{align*}
\]

spend credit

timelessness of \( \mathcal{L} n \)

later shuffling

open invariant

\[ R_{\text{pre}} \vdash \{ P \} \models \{ v. Q \} \]
Later Credits in Invariants

Idea: We **prepay** the later elimination

\[
R_{\text{pre}} \triangleq R \cdot \mathcal{L} 1
\]

such that we get **direct access** to \( R \).

\[
\begin{align*}
\{ R \cdot P \} & \ e \ \{ v \cdot Q \cdot R \cdot \mathcal{L} 1 \} \\
\{ \mathcal{L} 1 \cdot \triangleright (R \cdot P) \} & \ e \ \{ v \cdot Q \cdot R \cdot \mathcal{L} 1 \} \\
\triangleright \mathcal{L} 1 \cdot \triangleright (R \cdot P) & \ e \ \{ v \cdot Q \cdot R \cdot \mathcal{L} 1 \} \\
\{ P \cdot \triangleright (R \cdot \mathcal{L} 1) \} & \ e \ \{ v \cdot Q \cdot \triangleright (R \cdot \mathcal{L} 1) \} \\
R_{\text{pre}} & \vdash \{ P \} \ e \ \{ v \cdot Q \}
\end{align*}
\]

- spend credit
- timelessness of \( \mathcal{L} n \)
- later shuffling
- open invariant
In fact, we obtain no later

\[
\begin{align*}
\{ P \times R \} &\quad e \quad \{ v. Q \times R \} &\quad e \quad \text{atomic} \\
\hline
\end{align*}
\]

\[
\begin{array}{c}
\{ P \} &\quad e \quad \{ v. Q \} \\
\end{array}
\]

Disclaimer 1. To obtain this rule, we need to generate more than one credit per step. To do so, we modify Jourdan’s multiple-laters-per-step extension of Iris.

Disclaimer 2. The paradox is of course still true. Even with later credits, we cannot open invariants without a guarding later around updates.
Application: Prepaid Invariants
sharing later credits via invariants

Application: Logical Atomicity
cleaning up existing proofs

Theory and Soundness
the intuition on a napkin
Logical Atomicity …

… in a nutshell:

relaxed to “logically atomic” instructions

\[
\frac{\{P \times R\} e \{v. Q \times R\}}{\text{atomic}}
\]

\[
\{P\} e \{v. Q\}
\]
The later troubles …

… arise for **data structures with helping**.

![Diagram showing the interaction between Thread A and Thread B](null)

- **Thread A**
  - helpee (e.g., push)
  - "please help"

- **Thread B**
  - helper (e.g., pop)
  - "done"
The later troubles …

… arise for **data structures with helping.**

**Complication.** The interaction physically happens through memory, and logically happens **through invariants.**
How does it work?

Ask Ralf!

Logical Atomicity in Iris: the Good, the Bad, and the Ugly

Ralf Jung
MPI-SWS, Germany

Iris Workshop, October 2019
Later credits remove the **ugly parts of** logical atomicity.

Later credits make logical atomicity *laterable*, allowing for help to occur when one thread’s linearization point is executed by another thread.

Without later credits, $\downarrow$AU is useless!

With later credits, help is possible, as demonstrated by the helper (helper) helping the helpee: $\uparrow$AU $\cdot$ £1.

Logical Atomicity, v1: laterable (
(the Ugly)
Application: Prepaid Invariants
sharing later credits via invariants

Application: Logical Atomicity
cleaning up existing proofs

Theory and Soundness
the intuition on a napkin
The Later Credit Mechanism

A resource $£n$

$£(n + m) ⊢ £n * £m$  \hspace{1cm} \text{timeless}(£n)$

an update $\Rightarrow_{le} P$

$P \vdash \Rightarrow_{le} P$  \hspace{1cm} $\Rightarrow_{le} P * (P \rightarrow \Rightarrow_{le} Q) \vdash \Rightarrow_{le} Q$  \hspace{1cm} $£1 * \triangleright P \vdash \Rightarrow_{le} P$

a monad

and Hoare rules

\[
\frac{\{P\} e \{v. Q\}}{\{\Rightarrow_{le} P\} e \{v. Q\}} \hspace{1cm} \frac{\{P * £1\} e' \{v. Q\} \hspace{1cm} e \rightarrow_{\text{pure}} e'}{\{P\} e \{v. Q\}}
\]
Soundness

**Observation.** Adequacy in Iris is only concerned with the amortized number of later eliminations.

without credits

\[ e_0 \xrightarrow{\text{elim.}} e_1 \xrightarrow{\text{elim.}} \cdots \xrightarrow{\text{elim.}} e_n \]

at most \( n \) later eliminations

with credits

\[ e_0 \xrightarrow{\mathcal{L} 1} e_1 \xrightarrow{\mathcal{L} 1} \cdots \xrightarrow{\mathcal{L} 1} e_n \]
Later credits turn the right to eliminate a later transform $R\rightarrow R$ into an ownable resource, which is subject to a later credit £1 traditional separation logic reasoning. passing around, framing, sharing via invariants
Using Later Credits

**Step 1.** Replace $\implies P$ with $\implies_{le} P$ in your definitions.\(^1\)

**Step 2.** Profit

- ✔ in program verification proofs
- ✔ in logical relation constructions
- ✔ in ghost theories
- ✔ in logical atomicity proofs

\(^1\)Mostly backwards compatible. Missing interaction rules with plain propositions.
Later Credits vs. Time Receipts

**Time receipts** track the number of laters per step.

\[ e_0 \xrightarrow{\triangleright} e_1 \xrightarrow{\triangleright^2} \cdots \xrightarrow{\triangleright^n} e_n \]

**Later credits** control where laters are.

\[ \mathcal{L} 1 \triangleright P \vdash \Rightarrow_{le} P \quad \text{and} \quad \{ R \} e \{ v. Q \} \]

\[ \{ \mathcal{L} 1 \triangleright R \} e \{ v. Q \} \]
Later Credits + Time Receipts

We add time receipts $\nabla n$

\[
\begin{align*}
&P \ast L1 \ast \nabla 1 \rightarrow_{\text{pure}} e2 \{v. Q\} & e1 \rightarrow_{\text{pure}} e2 \\
&P \{v. Q\} \\
&\{P\} e1 \{v. Q\}
\end{align*}
\]

by integrating with **Jourdan’s multiple-laters-per-step extension**. The definition of prepaid invariants becomes $R_{\text{pre}} \triangleq R \ast L1 \ast \nabla 1$, satisfying

\[
\begin{align*}
&R_{\text{pre}} \vdash \{P\} e \{v. Q\} \\
&\{\triangleright R \ast L1 \ast \nabla 1 \ast P\} e \{v. Q\}
\end{align*}
\]

\[
\begin{align*}
&\{P \ast R\} e \{v. Q \ast R\} & e \text{ atomic} \\
&R_{\text{pre}} \vdash \{P\} e \{v. Q\}
\end{align*}
\]
The Later Elimination Update

\[ \models_{le} P \triangleq \forall n. \mathcal{L} \cdot n \rightarrow \models ((\mathcal{L} \cdot n \star P) \lor (\exists m < n. \mathcal{L} \cdot m \star \models_{le} P)) \]

where \( \mathcal{L} n \triangleq \mathcal{L} n^{\gamma_{lc}} \) and \( \mathcal{L} \cdot n \triangleq \mathcal{L} \cdot n^{\gamma_{lc}} \) from \( Auth(\mathbb{N}, +) \).

choose a path  
add a later to your goal

ghost state update  
credit decrease