

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



MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS



AARHUS
UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Radboud Universiteit



SIC Saarland Informatics
Campus



BOSTON
COLLEGE

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: A Double Edged Sword

Step-indexing enables recursive reasoning

Löb induction, higher-order ghost state, ...

but introduces irritating step-indexing artifacts.

the later modality $\triangleright P$

Running Example: Impredicative Invariants

Opening Invariants (from Iris 1.0)

$$\frac{\{P * R\} e \{Q * R\} \quad e \text{ atomic}}{\boxed{R} \vdash \{P\} e \{Q\}}$$

Running Example: Impredicative Invariants

Actually ...

later modality

masks

$$\frac{\{P * \triangleleft R\} e \{v. Q * \triangleright R\}_{\mathcal{E} \setminus \mathcal{N}} \quad e \text{ atomic} \quad \mathcal{N} \subseteq \mathcal{E}}{\boxed{R}^{\mathcal{N}} \vdash \{P\} e \{v. Q\}_{\mathcal{E}}}$$

because invariants in Iris **are step-indexed**.

The Akward Role of the Later Modality

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

$$\boxed{\exists n : \mathbb{N}. \ell \mapsto n} \vdash \{\mathbf{True}\} !\ell \{v. v \in \mathbb{N}\}$$

Example: A Typical Iris Proof

$$\frac{\vdash \{\triangleright(\exists n : \mathbb{N}. \ell \mapsto n)\} !\ell \{v. v \in \mathbb{N} * \triangleright(\exists n : \mathbb{N}. \ell \mapsto n)\}}{\boxed{\exists n : \mathbb{N}. \ell \mapsto n} \vdash \{\mathbf{True}\} !\ell \{v. v \in \mathbb{N}\}}$$

Example: A Typical Iris Proof

no more later

$$\frac{\vdash \{(\exists n : \mathbb{N}. \ell \mapsto n)\} !\ell \{v. v \in \mathbb{N} * \triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\} \\ \vdash \{\triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\} !\ell \{v. v \in \mathbb{N} * \triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\}}{\boxed{\exists n : \mathbb{N}. \ell \mapsto n} \vdash \{\mathbf{True}\} !\ell \{v. v \in \mathbb{N}\}}$$

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

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

$$\frac{\{P * R\} e \{v. Q\} \quad \text{timeless}(R)}{\{P * \triangleright R\} e \{v. Q\}} \quad \text{timeless}(\ell \mapsto v)$$

- 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

$$\triangleright(P * Q) \vdash \triangleright P * \triangleright Q \quad \triangleright(\exists x. P) \vdash \exists x. \triangleright P \quad \dots$$

- 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

$$\frac{\{R\} e' \{v. Q\} \quad e \rightarrow_{\text{pure}} e'}{\{\triangleright R\} e \{v. Q\}} \dots$$

Limitations of the Existing Options

Existing options apply to most invariants

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

Limitations of the Existing Options

Existing options apply to most invariants

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

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

$$R = \boxed{\exists n : \mathbb{N}. \ell \mapsto n} \quad \text{where} \quad \boxed{\exists n : \mathbb{N}. \ell \mapsto n} \text{ not timeless}$$

We are stuck ...

invariant guarded by a later

$$\vdash \{\triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\} !\ell \{v. v \in \mathbb{N} * \triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\}$$

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



So what then?

“ Help ...

The screenshot shows the MPI Mattermost application interface. The title bar says "MPI Mattermost". The left sidebar has icons for Iris, Projects, Archive, Channels, PL, and SAB. The "Iris Helpdesk" channel is selected and highlighted in blue. The main pane shows a message from Jonas Kastberg asking about deriving `False` from `x * y`. Robbert Krebbers commented that it's not straightforward because Exclusive lemmas live at the Coq level, not the Iris lemma. The bottom of the screenshot includes a footer with the text "(This is assuming you are not using a discrete RA)".

Iris Helpdesk

247 1 The public channel for general Iris-related questions of all kin...

What is the most straightforward way of deriving `False` from `x * y` (in the spatial context) where `x` and `y` are `Exclusive`?
I have an RA built directly in terms of `excl_auth` (and thereby `excl`), and I fail to construct a simple proof of `my_own x * my_own y -* False`.

Robbert Krebbers 4:16 PM

Commented on Jonas Kastberg's message: What is the most straightforward way of ...
I am afraid there is no easy way. The `Exclusive` lemmas live at the Coq level, not the Iris lemma.
You have to prove such a lemma for your concrete RA in question.

(This is assuming you are not using a discrete RA)

So what then?

“ Help ...

Have you tried these **non-local refactorings** of your proof

- flattening your invariant hierarchy

:

or **considered giving up?**



> CHANNELS



Iris Helpdesk



> DIRECT MESSAGES



Robbert Krebbers 4:16 PM

Commented on Jonas Kastberg's message: What is the most straightforward way of ...

I am afraid there is no easy way. The Exclusive lemmas live at the Coq level, not the Iris lemma.

You have to prove such a lemma for your concrete RA in question.

(This is assuming you are not using a discrete RA)

↳ 6

Developing a Fourth Option

Step-Indexed
Logical
Re



Separation
Logic

How about using this pillar to
develop another option?

Our Contribution: Later Credits

Later credits turn

the right to eliminate a later into an

transform $\triangleright R$ into R

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

$$\frac{\{R\} e' \{v. Q\} \quad e \rightarrow_{\text{pure}} e'}{\{\triangleright R\} e \{v. Q\}}$$

becomes

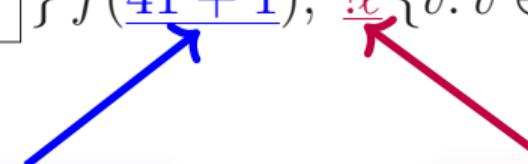
$$\frac{\{R * \mathcal{L} 1\} e' \{v. Q\} \quad e \rightarrow_{\text{pure}} e'}{\{R\} e \{v. Q\}} \qquad \frac{\{R\} e \{v. Q\}}{\{\mathcal{L} 1 * \triangleright R\} e \{v. Q\}}$$

Novelty: Prepaid Reasoning

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

we obtain £1

we spend £1



Prepaid Reasoning in Action

$$\{\boxed{\exists n : \mathbb{N}. \ell \mapsto n}\} f(\textcolor{blue}{41 + 1}); !\ell \{v. v \in \mathbb{N}\}$$

Prepaid Reasoning in Action

$$\frac{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} * \textcolor{blue}{\ell 1} \} f(42); !\ell \{v. v \in \mathbb{N}\}}{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} \} f(41 + 1); !\ell \{v. v \in \mathbb{N}\}}$$

Prepaid Reasoning in Action

$$\frac{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} * \mathcal{E} 1 \} f(42); !\ell \{v. v \in \mathbb{N}\}}{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} \} f(41 + 1); !\ell \{v. v \in \mathbb{N}\}}$$

Prepaid Reasoning in Action

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

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

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

Prepaid Reasoning in Action

$$\frac{\{ \triangleright [(\exists n : \mathbb{N}. \ell \mapsto n)] * \mathcal{E} 1 \} !\ell \{ v. v \in \mathbb{N} * \triangleright [(\exists n : \mathbb{N}. \ell \mapsto n)] \}}{\frac{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] * \mathcal{E} 1 \} !\ell \{ v. v \in \mathbb{N} \}}{\frac{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] * \mathcal{E} 1 \} f(42); !\ell \{ v. v \in \mathbb{N} \}}{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] \} f(41 + 1); !\ell \{ v. v \in \mathbb{N} \}}}}$$

Prepaid Reasoning in Action

we spend our credit

$$\frac{\frac{\frac{\{ \triangleright [(\exists n : \mathbb{N}. \ell \mapsto n)] * \cancel{\ell} 1\} !\ell \{v. v \in \mathbb{N} * \triangleright [(\exists n : \mathbb{N}. \ell \mapsto n)]\}}}{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] * \cancel{\ell} 1\} !\ell \{v. v \in \mathbb{N}\}}}{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] * \cancel{\ell} 1\} f(42); !\ell \{v. v \in \mathbb{N}\}}}{\{ [(\exists n : \mathbb{N}. \ell \mapsto n)] \} f(41 + 1); !\ell \{v. v \in \mathbb{N}\}}$$

Prepaid Reasoning in Action

$$\frac{\frac{\frac{\{ \boxed{(\exists n : \mathbb{N}. \ell \mapsto n)} \} !\ell \{v. v \in \mathbb{N} * \triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\}}{\{\triangleright (\exists n : \mathbb{N}. \ell \mapsto n) * \mathcal{E} 1\} !\ell \{v. v \in \mathbb{N} * \triangleright (\exists n : \mathbb{N}. \ell \mapsto n)\}}$$
$$\frac{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} * \mathcal{E} 1\} !\ell \{v. v \in \mathbb{N}\}}{\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} * \mathcal{E} 1\} f(42); !\ell \{v. v \in \mathbb{N}\}}$$
$$\{ \boxed{\exists n : \mathbb{N}. \ell \mapsto n} \} f(41 + 1); !\ell \{v. v \in \mathbb{N}\}$$

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?

no later

$$\frac{\{P * \downarrow R\} e \{v. Q * R\} \quad e \text{ atomic}}{\boxed{R} \vdash \{P\} e \{v. Q\}}$$



“ That cannot be sound, can it?

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * \mathcal{L} 1}$$

such that we get **direct access** to R .

$$\frac{\begin{array}{c} \{R * P\} e \{v. Q * R * \mathcal{L} 1\} \\ \hline \boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\} \end{array}}{e \text{ atomic}}$$


Later Credits in Invariants

Idea: We **prepay** the later elimination

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

generated by the
next step

such that we get **direct access** to R .

$$\frac{\overbrace{\{R * P\} e \{v. Q * R * \mathcal{L}1\}}^{\text{e atomic}}}{[R]_{\text{pre}} \vdash \{P\} e \{v. Q\}}$$

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * \mathcal{L}1}$$

such that we get **direct access** to R .

$$\frac{\frac{\frac{\frac{\frac{\{R * P\} e \{v. Q * R * \mathcal{L}1\}}}{\{\mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}}}{\{\triangleright \mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}}}{\{P * \triangleright(R * \mathcal{L}1)\} e \{v. Q * \triangleright(R * \mathcal{L}1)\}}}{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}}$$

spend credit
timelessness of $\mathcal{L}n$
later shuffling
open invariant

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * \mathcal{L}1}$$

such that we get **direct access** to R .

$$\frac{\frac{\frac{\frac{\{R * P\} e \{v. Q * R * \mathcal{L}1\}}}{\{\mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}} \text{spend credit}}{\{\triangleright \mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}} \text{timelessness of } \mathcal{L}n}{\{P * \triangleright(R * \mathcal{L}1)\} e \{v. Q * \triangleright(R * \mathcal{L}1)\}} \text{later shuffling}}{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}} \text{open invariant}$$

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * \mathcal{L}1}$$

such that we get **direct access** to R .

$$\frac{\frac{\frac{\frac{\frac{\{R * P\} e \{v. Q * R * \mathcal{L}1\}}}{\{\mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}} \text{spend credit}}}{\{\triangleright \mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}} \text{timelessness of } \mathcal{L}n}}{\{\triangleright(R * \mathcal{L}1)\} e \{v. Q * \triangleright(R * \mathcal{L}1)\}} \text{later shuffling}} \text{open invariant}$$
$$\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}$$

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * \mathcal{L}1}$$

such that we get **direct access** to R .

$$\frac{\frac{\frac{\frac{\frac{\{R * P\} e \{v. Q * R * \mathcal{L}1\}}}{\{\mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}}}{\{\triangleright \mathcal{L}1 * \triangleright(R * P)\} e \{v. Q * R * \mathcal{L}1\}}}{\{P * \triangleright(R * \mathcal{L}1)\} e \{v. Q * \triangleright(R * \mathcal{L}1)\}}}{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}}$$

spend credit
timelessness of $\mathcal{L}n$
later shuffling
open invariant

Prepaid Invariants

In fact, we obtain no later

$$\frac{\{P * \overleftarrow{R}\} e \{v. Q * R\} \quad e \text{ atomic}}{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}}$$

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:

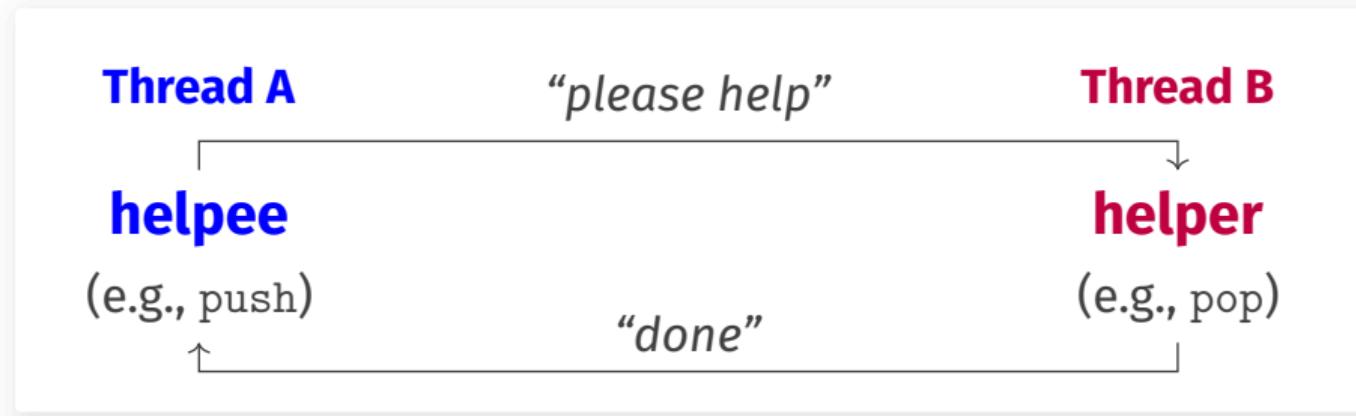
relaxed to “logically atomic” instructions

$$\frac{\{P * R\} e \{v. Q * R\}}{\boxed{R} \vdash \{P\} e \{v. Q\}}$$

e  **atomic**

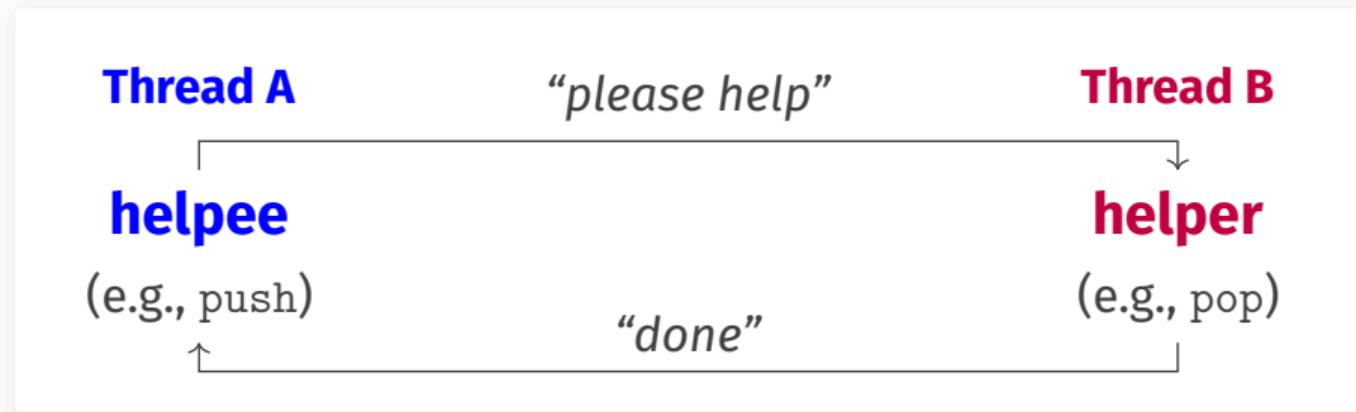
The later troubles ...

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



The later troubles ...

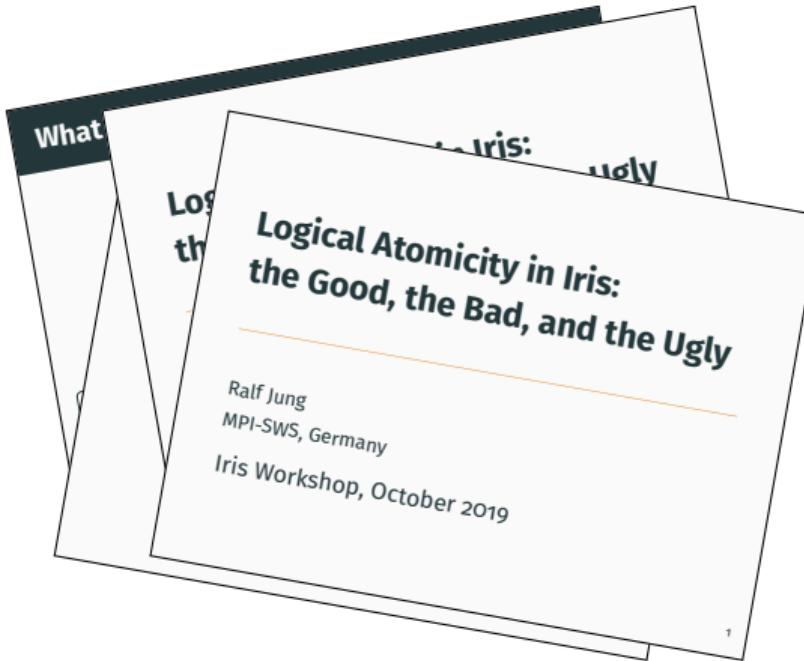
... arise for **data structures with helping**.



Complication. The interaction physically happens through memory, and logically happens **through invariants**.

How does it work?

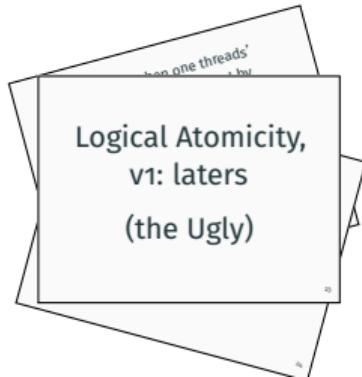
Ask Ralf!



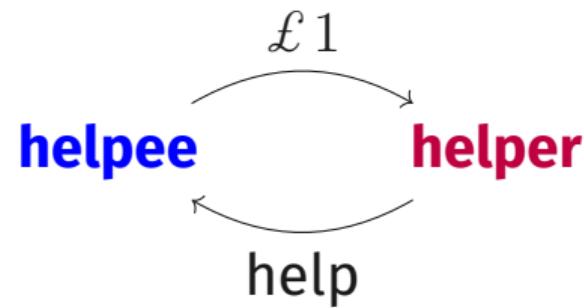
The Main Takeaway

Later credits remove the **ugly parts of** logical atomicity.
laterable

without later credits



with later credits



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 $\mathcal{L} n$

$$\mathcal{L}(n+m) \dashv\vdash \mathcal{L}n * \mathcal{L}m \quad \text{timeless}(\mathcal{L}n)$$

an update $\Rightarrow_{\text{le}} P$

$$\frac{P \vdash \Rightarrow_{\text{le}} P \quad \Rightarrow_{\text{le}} P * (P \multimap \Rightarrow_{\text{le}} Q) \vdash \Rightarrow_{\text{le}} Q}{\text{a monad}}$$

and Hoare rules

$$\frac{\{P\} e \{v. Q\}}{\Rightarrow_{\text{le}} P \vdash e \{v. Q\}}$$

$$\frac{\{P * \mathcal{L} 1\} e' \{v. Q\} \quad e \rightarrow_{\text{pure}} e'}{\{P\} e \{v. Q\}}$$

Soundness

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

without credits

$$e_0 \xrightarrow{\triangleright \text{ elim.}} e_1 \xrightarrow{\triangleright \text{ elim.}} \dots \xrightarrow{\triangleright \text{ elim.}} e_n$$



at most n later eliminations

with credits

$$e_0 \xrightarrow{\ell 1} e_1 \xrightarrow{\ell 1} \dots \xrightarrow{\ell 1} e_n$$

Our Contribution: Later Credits

Later credits turn

the right to eliminate a later into an

transform $\triangleright R$ into R

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 $\Rightarrow P$ with $\Rightarrow_{\text{le}} P$ in your definitions.¹

Step 2. Profit

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

¹Mostly backwards compatible. Missing interaction rules with plain propositions.

Later Credits vs. Time Receipts

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

$$e_0 \xrightarrow{\triangleright} e_1 \xrightarrow{\triangleright^2} \dots \xrightarrow{\triangleright^n} e_n$$

Later credits control **where laters are**.

$$\mathcal{L} 1 * \triangleright P \vdash \Rightarrow_{\text{le}} P$$

and

$$\frac{\{R\} e \{v. Q\}}{\{\mathcal{L} 1 * \triangleright R\} e \{v. Q\}}$$

Later Credits + Time Receipts

We add time receipts Σn

$$\frac{\{P * \mathcal{L} 1 * \Sigma 1\} e_2 \{v. Q\} \quad e_1 \rightarrow_{\text{pure}} e_2}{\{P\} e_1 \{v. Q\}}$$

$$\frac{\{P\} e \{v. Q\} \quad e \notin \text{Val}}{\{P * \Sigma n\} e \{v. Q * \mathcal{L} n * \Sigma n\}}$$

by integrating with **Jourdan's multiple-laters-per-step extension**. The definition of prepaid invariants becomes $\boxed{R}_{\text{pre}} \triangleq R * \mathcal{L} 1 * \Sigma 1$, satisfying

$$\frac{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}}{\{\triangleright R * \mathcal{L} 1 * \Sigma 1 * P\} e \{v. Q\}}$$

$$\frac{\{P * R\} e \{v. Q * R\} \quad e \text{ atomic}}{\boxed{R}_{\text{pre}} \vdash \{P\} e \{v. Q\}}$$

The Later Elimination Update

$$\Rightarrow_{\text{le}} P \triangleq \forall n. \mathcal{L}_n * \Rightarrow ((\mathcal{L}_n * P) \vee (\exists m < n. \mathcal{L}_m * \triangleright \Rightarrow_{\text{le}} P))$$

choose a path
add a later to your goal

ghost state update
credit decrease

where $\mathcal{L} n \triangleq [\text{on}]^{\gamma_{\text{lc}}}$ and $\mathcal{L}_n \triangleq [\bullet n]^{\gamma_{\text{lc}}}$ from $\text{Auth}(\mathbb{N}, +)$.