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

MIT CSAIL

SIC Saarland Informatics Campus

BOSTON COLLEGE

The Historic Foundation of Iris

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)

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

Running Example: Impredicative Invariants

Actually …

later modality masks

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

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

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

Example: A Typical Iris Proof

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

Example: A Typical Iris Proof

no more later

$$\dfrac{\dfrac{\vdots}{\vdash \{(\exists n:\mathbb{N}.\, \ell \mapsto n)\}\, !\ell\, \{v.\, v \in \mathbb{N} * \triangleright(\exists n:\mathbb{N}.\, \ell \mapsto n)\}}}{\dfrac{\vdash \{\triangleright(\exists n:\mathbb{N}.\, \ell \mapsto n)\}\, !\ell\, \{v.\, v \in \mathbb{N} * \triangleright(\exists n:\mathbb{N}.\, \ell \mapsto n)\}}{\boxed{\exists n:\mathbb{N}.\, \ell \mapsto n} \vdash \{\mathsf{True}\}\, !\ell\, \{v.\, v \in \mathbb{N}\}}}$$

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

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

- 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

$$\triangleright(P * Q) \vdash \triangleright P * \triangleright Q \qquad \triangleright(\exists x.\, P) \vdash \exists x.\, \triangleright P \qquad \ldots$$

- 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

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

Limitations of the Existing Options

Existing options apply to most invariants

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

Limitations of the Existing Options

Existing options apply to most invariants

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

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

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

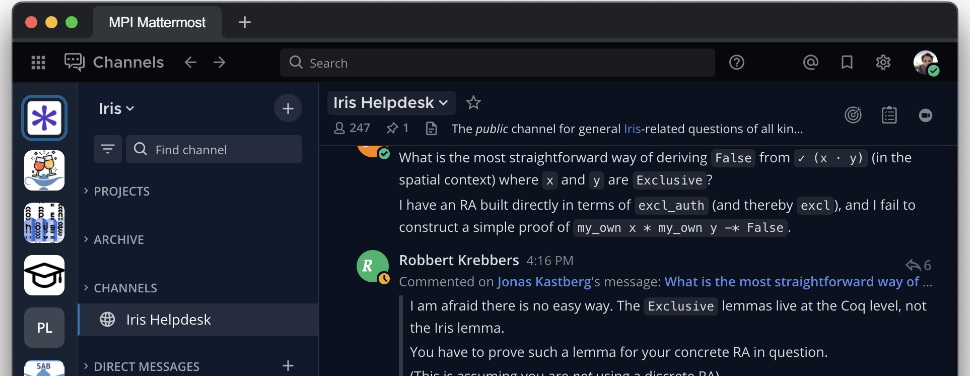
We are stuck ...

invariant guarded by a later

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

So what then?

> “Help …



So what then?

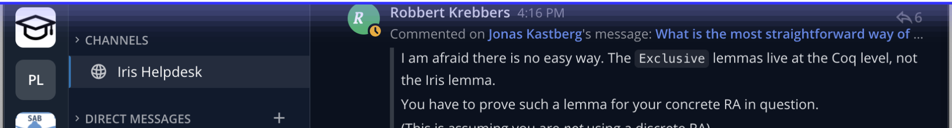
> "Help ...

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

- flattening your invariant hierarchy

⋮

or **considered giving up?**



Developing a Fourth Option

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

$$\frac{\{R\}\, e'\, \{v.\, Q\} \qquad e \rightarrow_{\mathsf{pure}} e'}{\{\triangleright R\}\, e\, \{v.\, Q\}}$$

becomes

$$\frac{\{R * \pounds\, 1\}\, e'\, \{v.\, Q\} \qquad e \rightarrow_{\mathsf{pure}} e'}{\{R\}\, e\, \{v.\, Q\}} \qquad \frac{\{R\}\, e\, \{v.\, Q\}}{\{\pounds\, 1 * \triangleright R\}\, e\, \{v.\, Q\}}$$

Novelty: Prepaid Reasoning

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

we obtain $\pounds\,1$

we spend $\pounds\,1$

Prepaid Reasoning in Action

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

Prepaid Reasoning in Action

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

Prepaid Reasoning in Action

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

Prepaid Reasoning in Action

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

Prepaid Reasoning in Action

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

Prepaid Reasoning in Action

we spend our credit

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

Prepaid Reasoning in Action

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

$$\{\triangleright \boxed{(\exists n : \mathbb{N}.\, \ell \mapsto n)} * £\,1\}\ !\ell\ \{v.\, v \in \mathbb{N} * \triangleright \boxed{(\exists n : \mathbb{N}.\, \ell \mapsto n)}\ \}$$

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

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

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

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

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

“ That cannot be sound, can it?

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\mathsf{pre}} \triangleq \boxed{R * £\,1}$$

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

$$\frac{\{R * P\}\; e\; \{v.\, Q * R * £\,1\} \qquad e \text{ atomic}}{\boxed{R}_{\mathsf{pre}} \vdash \{P\}\; e\; \{v.\, Q\}}$$

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * £\,1}$$

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

generated by the next step

$$\frac{\{R * P\}\, e\, \{v.\, Q * R * £\,1\} \qquad e \text{ atomic}}{\boxed{R}_{\text{pre}} \vdash \{P\}\, e\, \{v.\, Q\}}$$

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\mathsf{pre}} \triangleq \boxed{R * £\,1}$$

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

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

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * £\,1}$$

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

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

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}_{\text{pre}} \triangleq \boxed{R * £\,1}$$

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

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

Later Credits in Invariants

Idea: We **prepay** the later elimination

$$\boxed{R}^{\text{pre}} \triangleq \boxed{R * \pounds 1}$$

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

$$\cfrac{\cfrac{\cfrac{\cfrac{\{R * P\}\, e\, \{v.\, Q * R * \pounds 1\}}{\{\pounds 1 * \triangleright(R * P)\}\, e\, \{v.\, Q * R * \pounds 1\}}\ \text{spend credit}}{\{\triangleright \pounds 1 * \triangleright(R * P)\}\, e\, \{v.\, Q * R * \pounds 1\}}\ \text{timelessness of } \pounds n}{\{P * \triangleright(R * \pounds 1)\}\, e\, \{v.\, Q * \triangleright(R * \pounds 1)\}}\ \text{later shuffling}}{\boxed{R}^{\text{pre}} \vdash \{P\}\, e\, \{v.\, Q\}}\ \text{open invariant}$$

Prepaid Invariants

In fact, we obtain

no later

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

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 ...

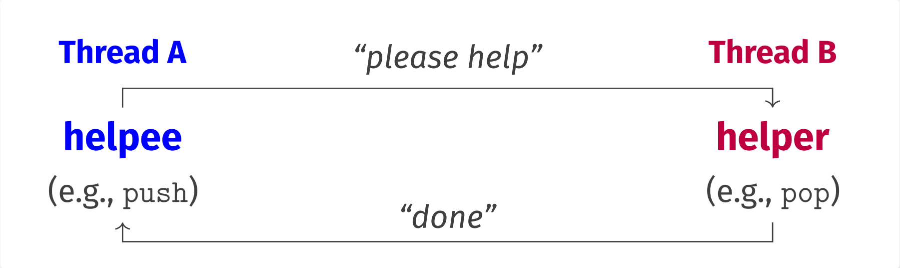
... in a nutshell:

relaxed to "logically atomic" instructions

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

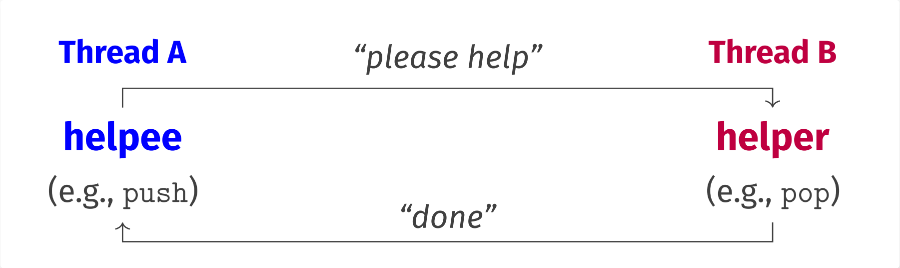
The later troubles …

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



The later troubles …

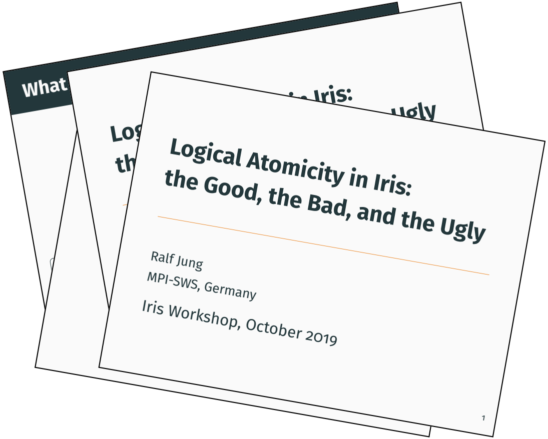
… arise for **data structures with helping.**



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

How does it work?

Ask Ralf!

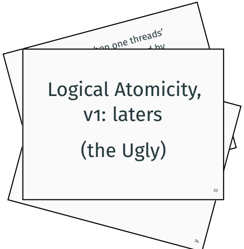


The Main Takeaway

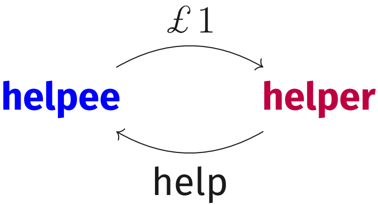
Later credits remove the **ugly parts of** logical atomicity.

`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 $\pounds\, n$

$$\pounds\,(n+m) \dashv\vdash \pounds\, n * \pounds\, m \qquad \text{timeless}(\pounds\, n)$$

an update $\Rrightarrow_{\mathsf{le}} P$

$$P \vdash \Rrightarrow_{\mathsf{le}} P \qquad \Rrightarrow_{\mathsf{le}} P * (P -\!\!* \Rrightarrow_{\mathsf{le}} Q) \vdash \Rrightarrow_{\mathsf{le}} Q \qquad \pounds\, 1 * \triangleright P \vdash \Rrightarrow_{\mathsf{le}} P$$

a monad

and Hoare rules

$$\frac{\{P\}\, e\, \{v.\, Q\}}{\{\Rrightarrow_{\mathsf{le}} P\}\, e\, \{v.\, Q\}} \qquad \frac{\{P * \pounds\, 1\}\, e'\, \{v.\, Q\} \qquad e \to_{\mathsf{pure}} e'}{\{P\}\, e\, \{v.\, Q\}}$$

Soundness

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

without credits $e_0 \xrightarrow{\triangleright\ \text{elim.}} e_1 \xrightarrow{\triangleright\ \text{elim.}} \cdots \xrightarrow{\triangleright\ \text{elim.}} e_n$

at most n later eliminations

with credits $e_0 \xrightarrow{\pounds\,1} e_1 \xrightarrow{\pounds\,1} \cdots \xrightarrow{\pounds\,1} e_n$

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 $\pounds 1$

traditional separation logic reasoning.

passing around, framing, sharing via invariants

Using Later Credits

Step 1. Replace $\Rrightarrow P$ with $\Rrightarrow_{\mathsf{le}} P$ 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.**

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

Later credits control **where laters are.**

$$£\,1 * \triangleright P \vdash \mathrel{\models\!\!\!\Rrightarrow}_{\mathsf{le}} P \qquad \text{and} \qquad \frac{\{R\}\; e\; \{v.\, Q\}}{\{£\,1 * \triangleright R\}\; e\; \{v.\, Q\}}$$

Later Credits + Time Receipts

We add time receipts $⧗ n$

$$\frac{\{P * £\,1 * ⧗ 1\}\; e_2\; \{v.\, Q\} \qquad e_1 \rightarrow_{\text{pure}} e_2}{\{P\}\; e_1\; \{v.\, Q\}} \qquad \frac{\{P\}\; e\; \{v.\, Q\} \qquad e \notin \textit{Val}}{\{P * ⧗ n\}\; e\; \{v.\, Q * £\,n * ⧗ n\}}$$

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

$$\frac{\boxed{R}_{\text{pre}} \vdash \{P\}\; e\; \{v.\, Q\}}{\{\triangleright R * £\,1 * ⧗ 1 * P\}\; e\; \{v.\, Q\}} \qquad \frac{\{P * R\}\; e\; \{v.\, Q * R\} \qquad e \text{ atomic}}{\boxed{R}_{\text{pre}} \vdash \{P\}\; e\; \{v.\, Q\}}$$

The Later Elimination Update

choose a path

add a later to your goal

$$|\!\!\Rrightarrow_{\mathsf{le}} P \triangleq \forall n.\ \pounds_\bullet n \mathrel{-\!\!*} |\!\!\Rrightarrow((\pounds_\bullet n * P) \vee (\exists m < n.\ \pounds_\bullet m * \triangleright |\!\!\Rrightarrow_{\mathsf{le}} P))$$

ghost state update

credit decrease

where $\pounds\, n \triangleq \boxed{\circ n}^{\gamma_{\mathsf{lc}}}$ and $\pounds_\bullet n \triangleq \boxed{\bullet n}^{\gamma_{\mathsf{lc}}}$ from *Auth*$(\mathbb{N}, +)$.