Automating your Iris proofs with Diaframe

Ike Mulder

Radboud University Nijmegen

Iris Workshop 2022

May 2, 2022

Scope

Automation for *fine-grained concurrency*

Scope

Automation for *fine-grained concurrency*:

- standard `WP` goals
- support for invariants $\boxed{P}^{\mathcal{N}}$
- support for ghost state $\boxed{a}^{\gamma}$

Scope

Automation that can be used *interactively*:

- no global backtracking
- extensible in language, ghost theory

Diaframe

- Plugin for Iris
- tactic based-automation: `iStepsS`

Example

```
Definition parallel_add: expr :=
  let: "r" := ref #0 in
  (FAA "r" #2) ||| (FAA "r" #2);;
  !"r".
```

Prove:

$$\{\mathsf{True}\}\ \texttt{parallel\_add}\ \{v, \ulcorner v = 4 \urcorner\}$$

Example

```
Definition parallel_add: expr :=
  let: "r" := ref #0 in
  (FAA "r" #2) ||| (FAA "r" #2);;
  !"r".
```

$\{\text{True}\}\ \texttt{parallel\_add}\ \{v, \ulcorner v = 4 \urcorner\}$ proof:

1. execute `ref`
2. allocate invariant
3. use specification of |||
4. verify left & right thread
5. verify load

Example

```
Definition parallel_add: expr :=
  let: "r" := ref #0 in
  (FAA "r" #2) ||| (FAA "r" #2);;
  !"r".
```

$\{\text{True}\}\ \texttt{parallel\_add}\ \{v, \ulcorner v = 4 \urcorner\}$ proof:

1. ~~execute ref~~ run automation
2. allocate invariant
3. use specification of |||
4. ~~verify left & right thread~~ run automation
5. ~~verify load~~ run automation

Example

```
Definition parallel_add: expr :=
  let: "r" := ref #0 in
  (FAA "r" #2) ||| (FAA "r" #2);;
  !"r".
```

$\{\mathrm{True}\}$ `parallel_add` $\{v, \ulcorner v = 4 \urcorner\}$ proof:

1. run automation
2. allocate invariant
3. use specification of |||
4. run automation
5. run automation

about ±75% shorter

Diaframe approach

$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$

`Qed.`

Diaframe approach

$$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\} \xrightarrow{\text{symbolic execution}} \texttt{Qed.}$$

Diaframe approach

$$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\} \xrightarrow{\cancel{\text{symbolic execution}}} \texttt{Qed.}$$

Diaframe approach

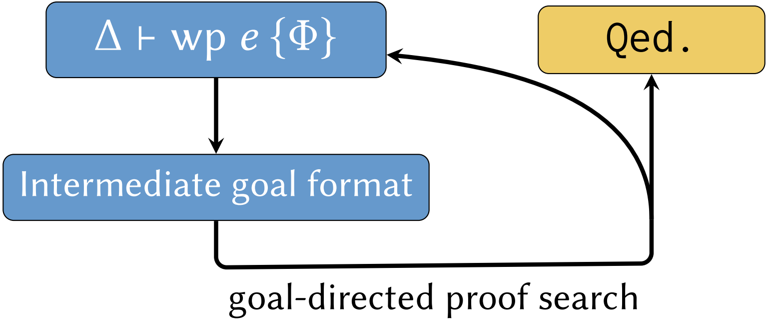
$$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$$

$$\downarrow$$

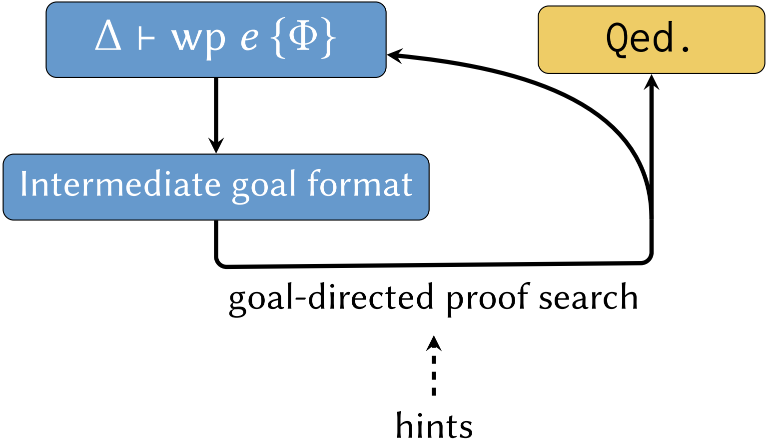
Intermediate goal format

`Qed.`

Diaframe approach



Diaframe approach

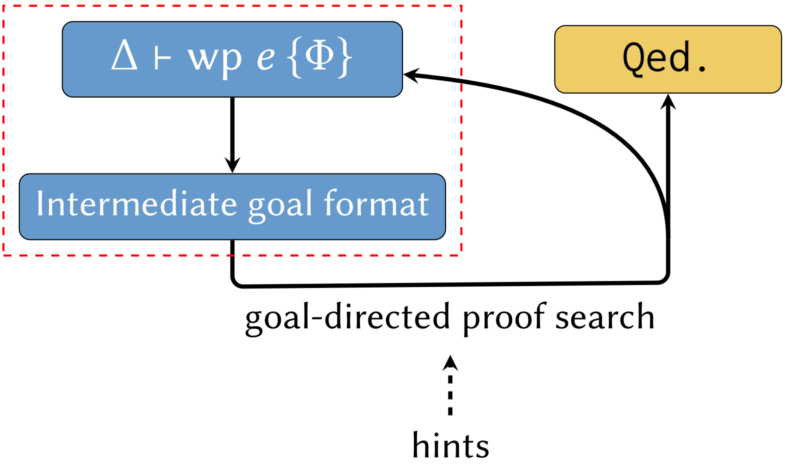


Diaframe: results

Verified 24 examples from the literature

Comparable proof burden to automated tools, but *foundational*

Caper, Voila, Starling


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
Intermediate goal format
goal-directed proof search
hints

Goal format

$$\ell \mapsto v \vdash \mathrm{wp}\ !\ell\ \{\Phi\} \qquad \texttt{wp\_load}\ ✔$$

$$\boxed{\exists v.\, \ell \mapsto v}^{\mathcal{N}} \vdash \mathrm{wp}\ !\ell\ \{\Phi\} \qquad \texttt{wp\_load}\ ?$$

Goal format

$$\ell \mapsto v \vdash \text{wp } !\ell \; \{\Phi\}$$

`wp_load` ✔

$$\boxed{\exists v.\, \ell \mapsto v}^{\mathcal{N}} \vdash \text{wp } !\ell \; \{\Phi\}$$

`wp_load` ✗

hard to determine directly what invariant to open

Goal format

$$\frac{\Delta \vdash {}^{\top}\!\!\Rrightarrow^{?} \exists u.\, \ell \mapsto u * (\ell \mapsto u \mathrel{-\!\!*} {}^{?}\!\!\Rrightarrow^{\top} \Phi\, u)}{\Delta \vdash \mathrm{wp}\ !\ell\ \{\Phi\}}$$

Goal format

can still open invariants

$$\frac{\Delta \vdash {}^{\top}\!\!\Rrightarrow^{?}\, \exists u.\, \ell \mapsto u * (\ell \mapsto u \mathrel{-\!\!*} {}^{?}\!\!\Rrightarrow^{\top} \Phi\, u)}{\Delta \vdash \mathrm{wp}\; !\ell\; \{\Phi\}}$$

Goal format

for when witness is inside invariant

$$\frac{\Delta \vdash {}^{\top}{\Rrightarrow}^{?}\, \exists u.\, \ell \mapsto u * (\ell \mapsto u \mathrel{-\!\!*} {}^{?}{\Rrightarrow}^{\top}\, \Phi\, u)}{\Delta \vdash \mathrm{wp}\ !\ell\ \{\Phi\}}$$

Goal format

find hypothesis that can make progress

$$\Delta, \boxed{\ell \mapsto v} \vdash {}^{\top}\!\!\models\!\!\!\Rrightarrow^{?} \exists u.\ \boxed{\ell \mapsto u} * G$$

Goal format

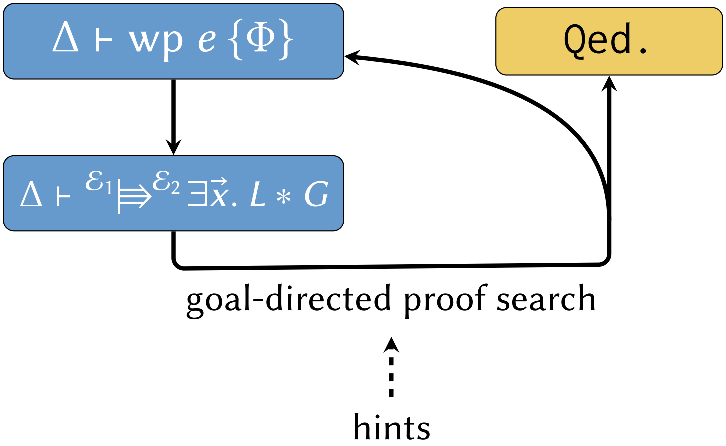
find hypothesis that can make progress

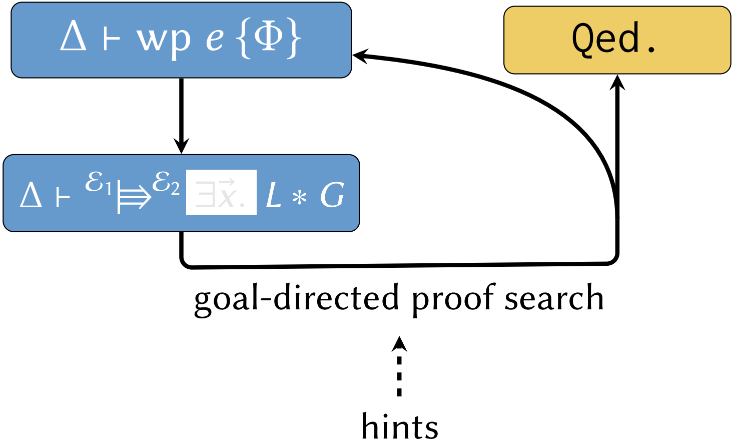
$$\Delta, \boxed{\exists v.\ \ell \mapsto v}^{\mathcal{N}} \vdash {}^{\top}{\models\!\!\!\Rrightarrow}^{?} \exists u.\ \ell \mapsto u * G$$

Goal format

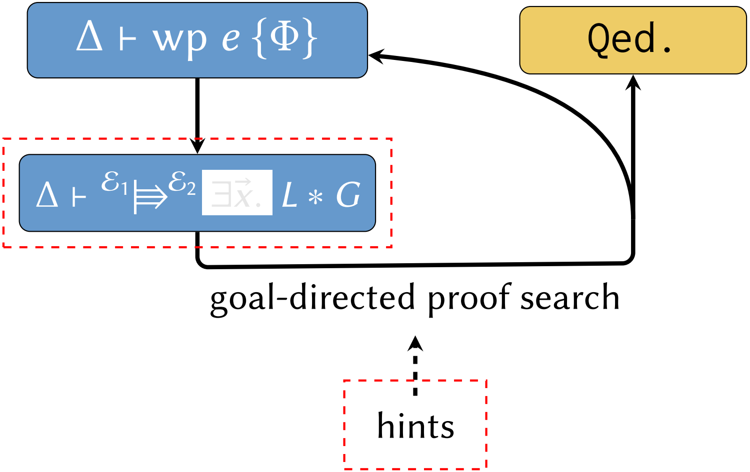
find hypothesis that can make progress

$$\Delta, \boxed{\exists v.\ \ell \mapsto v * B}^{\mathcal{N}} \vdash {}^{\top}\!\Rrightarrow^{?} \exists u.\ \ell \mapsto u * G$$


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
$\Delta \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
Qed.
goal-directed proof search
hints



$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2}\ \exists \vec{x}.\ L * G$
goal-directed proof search
hints


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
hints

Hints

definition?

how to detect?

$$\frac{H \text{ can make progress on } A \qquad ??}{\Delta, H \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} A * G}$$

Hints

A can make progress on A

$(B \mathrel{-\!\!*} A)$ can make progress on A

$\boxed{A * B}^{\mathcal{N}}$ can make progress on $\triangleright A$

$\boxed{\bullet a}^{\gamma}$ can make progress on $\boxed{\bullet a'}^{\gamma}$

Hints

$$
\begin{aligned}
A &\vdash A \\
(B \mathrel{-\!\!*} A) * B &\vdash A \\
\boxed{A * B}^{\mathcal{N}} &\vdash {}^{\top}{\mid\!\Rrightarrow}^{\top\setminus\mathcal{N}} \triangleright A * (\triangleright B * \ldots) \\
\boxed{\bullet a}^{\gamma} * \boxed{\circ b}^{\gamma} &\vdash \mid\!\dot{\Rrightarrow} \boxed{\bullet a'}^{\gamma} * \boxed{\circ b'}^{\gamma}
\end{aligned}
$$

Hints

H can make progress on A if

$$H * L \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} A * U$$

for some **sidecondition** L
residue U

Hints

H can make progress on A if

$$H * [L] \Vdash \left[{}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2}\right] A * [U] :=$$

$$H * L \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} A * U$$

for some **sidecondition** L

residue U

Hints

$$\frac{H * [L] \Vdash \left[{}^{\mathcal{E}_3}{\Rrightarrow}^{\mathcal{E}_2}\right] A * [U]}{\Delta, H \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} A * G}$$

Hints

$$\frac{H * [L] \Vdash \left[{}^{\mathcal{E}_3}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2}\right] A * [U] \qquad \Delta \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_3} L * (U \mathrel{-\!\!*} G)}{\Delta, H \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2} A * G}$$

Hints

$$\frac{H * [L] \Vdash \left[{}^{\mathcal{E}_3}{\Rrightarrow}^{\mathcal{E}_2}\right] A * [U] \qquad \Delta \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_3} L * (U \mathrel{-\!\!*} G)}{\Delta, H \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} A * G}$$

No backtracking: once a hint is found, we stick with it!

Hints

how to detect?

$$\frac{H * [L] \Vdash \left[{}^{\mathcal{E}_3}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2}\right] A * [U] \qquad \Delta \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_3} L * (U \mathrel{-\!\!*} G)}{\Delta, H \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2} A * G}$$

Hints

$H * [L] \Vdash \left[{}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2}\right] A * [U]$ is a typeclass

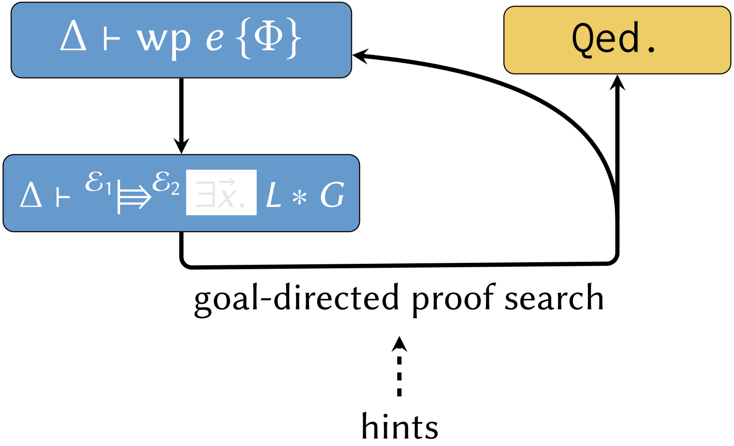
- Diaframe base hints
- Language-specific hints
- Libraries with ghost-theory hints

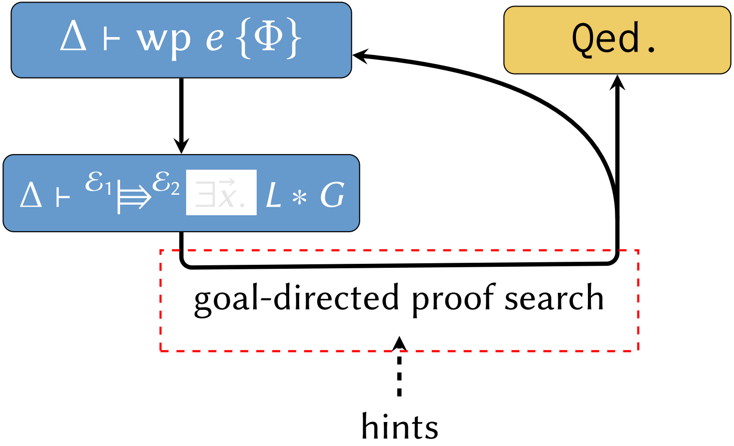
Hints

$H * [L] \Vdash \left[{}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2}\right] A * [U]$ is a typeclass

Recursive rules for additional instances:

$$\frac{H * [L_2] \Vdash \left[{}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2}\right] A * [U]}{(L_1 \mathrel{-\!\!*} H) * [L_1 * L_2] \Vdash \left[{}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2}\right] A * [U]}$$


$\Delta \vdash \text{wp } e \ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\!\models\!\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
hints



$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
hints

Proof search

$$\frac{\forall \vec{x}.\ \{L\}\ e\ \{\Psi\} \qquad \text{atomic } e}{\begin{array}{c}\Delta \vdash {}^{\top}\!\Rrightarrow^{?}\, \exists \vec{x}.\ L * (\forall v.\ \Psi\ v \mathrel{-\!\!*} {}^{?}\!\Rrightarrow^{\top} \mathrm{wp}\ K[v]\ \{\Phi\}) \\ \hline \Delta \vdash \mathrm{wp}\ K[e]\ \{\Phi\}\end{array}}$$

combines WP-BIND, WP-ATOMIC and WP-WAND

Proof search

$$\boxed{{}^{\top}\!\Rrightarrow^{?}\exists\vec{x}.}\ L * (\boxed{\forall v.\, \Psi\ v \mathrel{-\!\!*}}\ {}^{?}\!\Rrightarrow^{\top} \mathrm{wp}\ K[v]\ \{\Phi\})$$

proceed like Lithium

postpone introduction when possible

Proof search

Like Lithium:

$$\frac{\forall x. \quad \Delta \vdash G}{\Delta \vdash \forall x.\, G} \qquad \frac{\Delta \vdash H_1 \mathrel{-\!\!*} (H_2 \mathrel{-\!\!*} G)}{\Delta \vdash (H_1 * H_2) \mathrel{-\!\!*} G}$$

$$\frac{\Delta \vdash \forall x.\, (H \mathrel{-\!\!*} G)}{\Delta \vdash (\exists x.\, H) \mathrel{-\!\!*} G} \qquad \frac{\Delta, H \vdash G}{\Delta \vdash H \mathrel{-\!\!*} G}$$

Proof search

$$L ::= \ulcorner \phi \urcorner \mid A \mid L * L$$

$$\frac{}{\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} L * G}$$

Proof search

$$L ::= \ulcorner \phi \urcorner \mid \colorbox{yellow}{A} \mid L * L$$

$$\frac{H * [L] \Vdash \left[{}^{\mathcal{E}_3}{\Rrightarrow}^{\mathcal{E}_2}\right] A * [U] \qquad \Delta \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_3} L * (U \mathrel{-\!\!*} G)}{\Delta, H \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} A * G}$$

Proof search

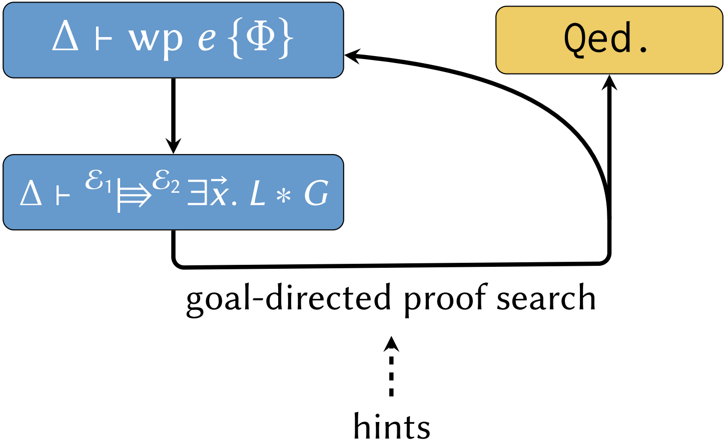
$$L ::= \ulcorner \phi \urcorner \mid A \mid \boxed{L * L}$$

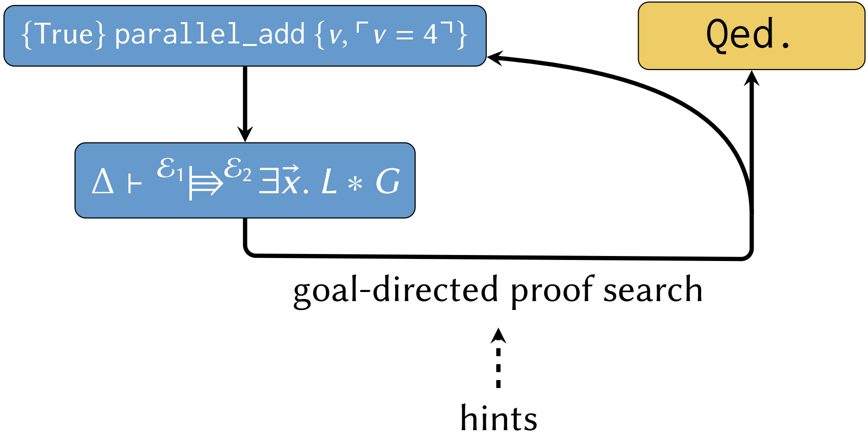
$$\frac{\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{?} L_1 * \left({}^{?}\!\!\Rrightarrow^{\mathcal{E}_2} L_2 * G\right)}{\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} (L_1 * L_2) * G}$$

Proof search

$$L ::= \boxed{\ulcorner \phi \urcorner} \mid A \mid L * L$$

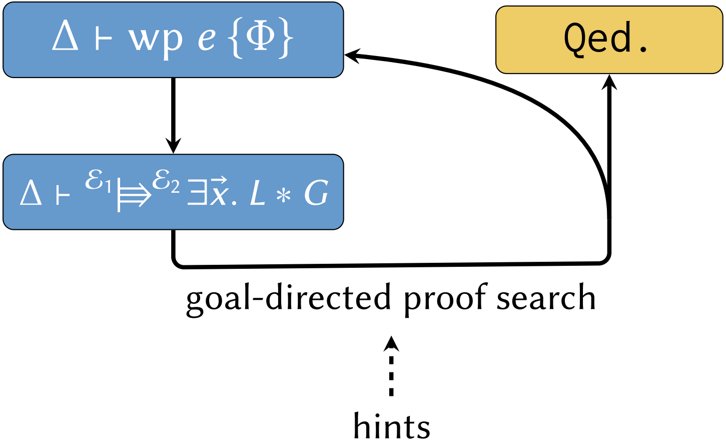
$$\frac{\phi \qquad \Delta \vdash G}{\Delta \vdash {}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}} \ulcorner \phi \urcorner * G}$$


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
hints



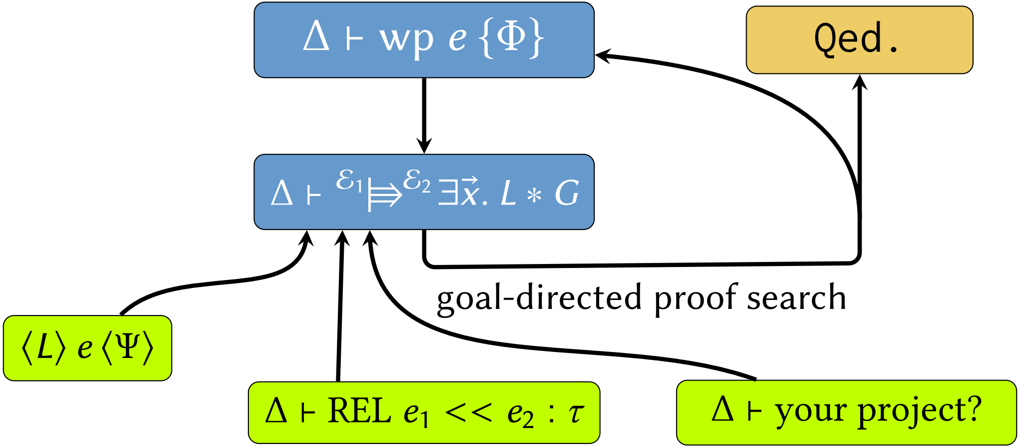

```
Definition parallel_add: expr :=
  let: "r" := ref #0 in
  (FAA "r" #2) ||| (FAA "r" #2);;
  !"r".
```

Future work

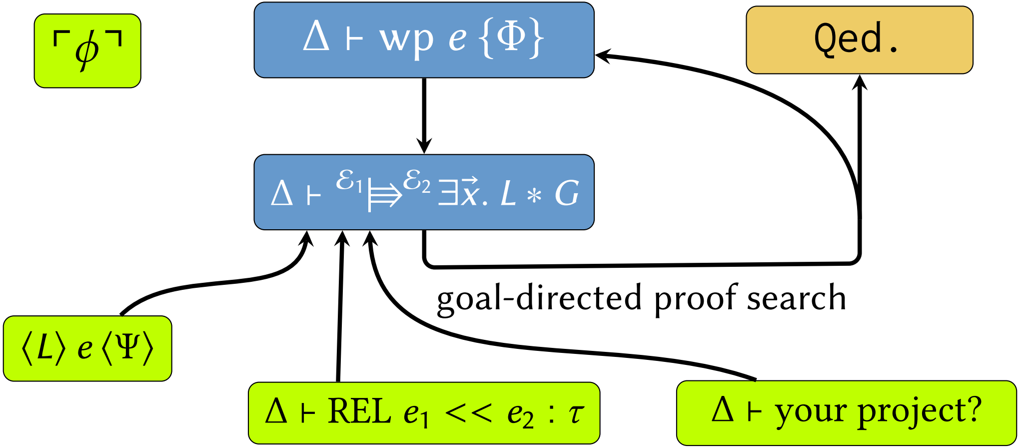


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2} \exists \vec{x}.\, L * G$
goal-directed proof search
hints

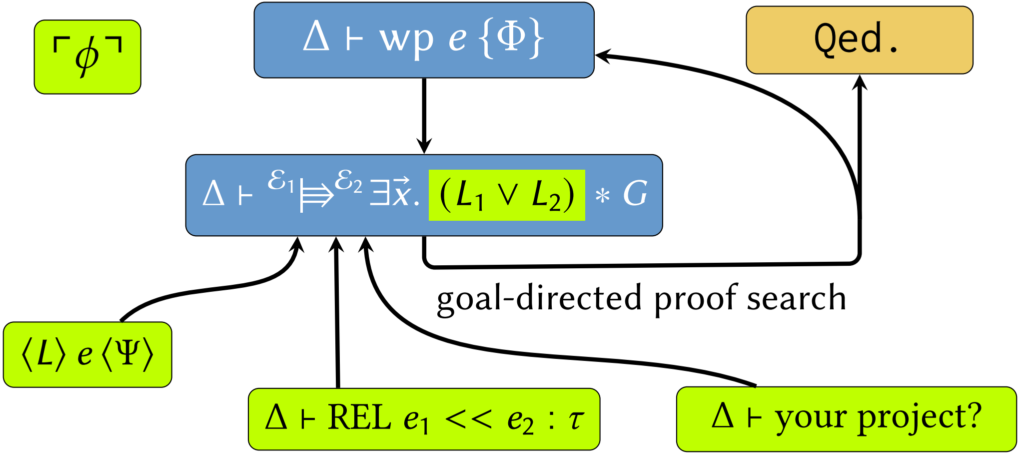
Future work


$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
$\langle L \rangle\ e\ \langle \Psi \rangle$
$\Delta \vdash \mathrm{REL}\ e_1 << e_2 : \tau$
$\Delta \vdash$ your project?

Future work

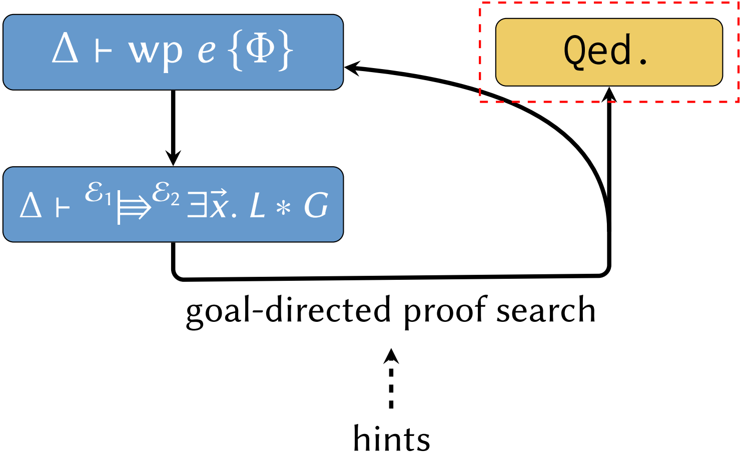

$\ulcorner \phi \urcorner$
$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
goal-directed proof search
$\langle L \rangle\ e\ \langle \Psi \rangle$
$\Delta \vdash \mathrm{REL}\ e_1 << e_2 : \tau$
$\Delta \vdash$ your project?

Future work



$\ulcorner \phi \urcorner$
$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
Qed.
$\Delta \vdash {}^{\mathcal{E}_1}\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ (L_1 \vee L_2) * G$
goal-directed proof search
$\langle L \rangle\ e\ \langle \Psi \rangle$
$\Delta \vdash \mathrm{REL}\ e_1 << e_2 : \tau$
$\Delta \vdash$ your project?

Questions?



$\Delta \vdash \mathrm{wp}\ e\ \{\Phi\}$
$\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\ L * G$
Qed.
goal-directed proof search
hints

Hint definition

$$
\begin{aligned}
H * [\vec{y}; L] \Vdash \left[{}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2}\right] \vec{x}; A * [U] := \\
\forall \vec{y}. \quad H * L \vdash {}^{\mathcal{E}_3}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}. A * U
\end{aligned}
$$

Proof search - detailed

$$L ::= \ulcorner \phi \urcorner \mid A \mid L * L \mid \exists z.\, L$$

$$\frac{}{\Delta \vdash {}^{\mathcal{E}_1}{\models\!\!\!\Rrightarrow}^{\mathcal{E}_2} \exists \vec{x}.\, L * G}$$

Proof search - detailed

$$L ::= \ulcorner \phi \urcorner \mid \colorbox{yellow}{A} \mid L * L \mid \exists z.\, L$$

$$\frac{H * [\vec{y}; L] \Vdash \left[{}^{\mathcal{E}_3}\!\Rrightarrow^{\mathcal{E}_2}\right] \; \vec{x}; A * [U] \qquad \Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_3} \exists \vec{y}.\, L * (\forall x.\, U \mathrel{-\!\!*} G)}{\Delta, H \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\, A * G}$$

Proof search - detailed

$$L ::= \ulcorner \phi \urcorner \mid A \mid \colorbox{yellow}{$L * L$} \mid \exists z.\, L$$

$$\frac{\vec{s} = \mathrm{FV}(L_1) \quad \vec{t} = \vec{x} \setminus \vec{s} \quad \Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{?} \exists \vec{s}.\, L_1 * \left({}^{?}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{t}.\, L_2 * G\right)}{\Delta \vdash {}^{\mathcal{E}_1}\!\!\Rrightarrow^{\mathcal{E}_2} \exists \vec{x}.\, (L_1 * L_2) * G}$$

Proof search - detailed

$$L ::= \ulcorner \phi \urcorner \mid A \mid L * L \mid \exists z.\, L$$

$$\frac{\phi[\vec{z}] \qquad \Delta \vdash G[\vec{x}/\vec{z}]}{\Delta \vdash {}^{\mathcal{E}}\!\!\Rrightarrow^{\mathcal{E}} \exists \vec{x}.\, \ulcorner \phi \urcorner * G}$$

Proof search - detailed

$$L ::= \ |A \mid L * L \mid \exists z.\ L$$

$$\frac{\Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} \exists(\vec{x}, t).\ L * G}{\Delta \vdash \exists \vec{x}.\ (\exists t.\ L) * G}$$