Proof Automation for Disjunctions and Logical Atomicity in Iris

Ike Mulder

Radboud University Nijmegen

Iris Workshop 2023

May 22, 2023

Diaframe, last year

Automation for *fine-grained concurrency*:

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

Diaframe, updates

1. Extensible for other goals

   i.e., logical atomicity, contextual refinement
2. Better support for disjunctions
3. Available on opam: `coq-diaframe`

Diaframe, updates

1. Extensible for other goals

   i.e., logical atomicity, contextual refinement
2. **Better support for disjunctions**
3. Available on opam: `coq-diaframe`

Disjunctions in Iris verifications

After opening invariant $\boxed{I}$ and symbolic execution:

$$\Delta \vdash \Rrightarrow I * \mathrm{wp}\ e\ \{\Phi\}$$

Disjunctions in Iris verifications

After opening invariant $\boxed{I_1 \vee I_2}$ and symbolic execution:

$$\Delta \vdash \Rrightarrow (I_1 \vee I_2) * \mathrm{wp}\ e\ \{\Phi\}$$

Disjunction example

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 13 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15$$

Overview

1. *Backtracking is unwanted*
2. Case distinctions make disjunctions harder
3. Idea: find connections from hypothesis to goal

   application to our example
4. Limitations

Backtracking proof search on disjunctions

As done by `auto`, old Diaframe, Caper:

$$\dfrac{\dfrac{\dfrac{\text{solved or unsolved}}{\vdots}}{\Delta \vdash P}}{\Delta \vdash P \lor Q}\ \textsc{try-left}$$

Backtracking proof search on disjunctions

As done by `auto`, old Diaframe, Caper:

$$\dfrac{\dfrac{\dfrac{\text{solved or unsolved}}{\vdots}}{\Delta \vdash P}}{\Delta \vdash P \lor Q}\ \textsc{try-left}$$

if unsolved: go back and try right

Disjunction example, try left

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 13 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\dfrac{\dfrac{\vdash \ulcorner m = 10 \urcorner}{\ell \mapsto m \vdash \ell \mapsto 10}\ \textsc{diaframe-hint}}{\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15}\ \textsc{try-left}$$

Disjunction example, try left

What if automation cannot prove

$$7 \leq m \leq 13 \longrightarrow m \equiv 0 \pmod 5 \longrightarrow m = 10?$$

Disjunction example, try left

What if automation cannot prove

$$7 \leq m \leq 13 \to m \equiv 0 \pmod 5 \to m = 10?$$

… since `lia` requires a special incantation for mod?

Disjunction example, try right

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 13 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\dfrac{\dfrac{\vdash \ulcorner m = 10 \urcorner \quad \text{✗ proof fails}}{\ell \mapsto m \vdash \ell \mapsto 10}\ \textsc{diaframe-hint}}{\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15}\ \textsc{try-left}$$

Disjunction example, try right

$$\forall m : \mathbb{Z}.\ \ 7 \le m \le 13 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\dfrac{\ell \mapsto m \vdash \ell \mapsto 15 \quad \text{✗}}{\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15}\ \textsc{try-right}$$

Disjunction example, try right

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 13 \ \longrightarrow\ \ m \equiv 0 \pmod 5 \longrightarrow$$

$$\dfrac{\ell \mapsto m \vdash \ell \mapsto 15 \quad ✗}{\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15}\ \textsc{try-right}$$

… goal is left unsolved

If backtracking proof search fails..

1. Reason of failure often unclear
2. No canonical remaining goal for user

Bad for interactive proofs

Overview

1. Backtracking is unwanted
2. *Case distinctions make disjunctions harder*
3. Idea: find connections from hypothesis to goal

   application to our example
4. Limitations

Disjunction example: it gets worse

$$\forall m : \mathbb{Z}.\ \ 7 \le m \le 18 \ \rightarrow\ m \equiv 0 \pmod{5} \rightarrow$$

$$\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15$$

Disjunction example: it gets worse

$$\forall m : \mathbb{Z}.\;\; 7 \le m \le 18 \;\to\; m \equiv 0 \pmod 5 \to$$

$$\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15$$

Backtracking directly is hopeless!

case distinction $m = 10 \lor m \neq 10$ is not very obvious

Disjunctions in classical logic

$$\frac{\Delta, \neg Q \vdash P}{\Delta \vdash P \vee Q} \ \vee\text{-INTRO-L}$$

Disjunctions in classical logic

$$\frac{\Delta, \neg Q \vdash P}{\Delta \vdash P \vee Q}\ \vee\text{-INTRO-L} \qquad \frac{\Delta \vdash P \vee Q}{\Delta, \neg Q \vdash P}\ \neg\text{-ELIM}$$

Disjunctions in classical logic

$$\frac{\Delta, \neg Q \vdash P}{\Delta \vdash P \lor Q}\ \lor\text{-INTRO-L} \qquad \frac{\Delta \vdash P \lor Q}{\Delta, \neg Q \vdash P}\ \neg\text{-ELIM}$$

$\lor$-INTRO-L and commutes with proof rules! *i.e.*, with:

$$\frac{\Delta, P \vdash R \qquad \Delta, Q \vdash R}{\Delta, P \lor Q \vdash R}\ \lor\text{-ELIM}$$

Disjunctions in classical logic

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P, \neg Q \vdash P}}{P \vdash Q \vee P}}{P, \neg P \vdash Q} \qquad \dfrac{}{Q, \neg P \vdash Q}}{P \vee Q, \neg P \vdash Q}}{P \vee Q \vdash Q \vee P}$$

…but Iris is inherently non-classical

Separation logics are incompatible with LEM if:

1. affine; or
2. step-indexed

$\Rightarrow$ we need to think of something else

Overview

1. Backtracking is unwanted
2. Case distinctions make disjunctions harder
3. *Idea: find connections from hypothesis to goal*
   application to our example
4. Limitations

Goal

Find a *deterministic* rule for disjunctions which *postpones the choice* of disjunct, until any required *case distinctions become apparent*

Inspiration: connection calculus

Connection calculus: complete proof search procedure for intuitionistic logic

Inspiration: connection calculus

Connection calculus: complete proof search procedure for intuitionistic logic

Relies on finding *connections*:

$$A \rightarrow (B \vee C), A \vdash C \vee B$$

from hypothesis to goal

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{}{\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15}$$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Diaframe thinks: *HINT:* $\ell \mapsto m * \ulcorner m = 10 \urcorner \vdash \ell \mapsto 10$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{\overline{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \twoheadrightarrow \ell \mapsto 15 \right)}}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Diaframe thinks: *HINT:* $\ell \mapsto m * \ulcorner m = 10 \urcorner \vdash \ell \mapsto 10$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\quad 7 \leq m \leq 18 \;\rightarrow\; m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \mathrel{-\!\!*} \ell \mapsto 15\right)}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Diaframe thinks: *HINT:* $\ell \mapsto m * \ulcorner m = 10 \urcorner \vdash \ell \mapsto 10$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \twoheadrightarrow* \ell \mapsto 15\right)}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow \ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\dfrac{\overline{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \ -\!\!* \ \ell \mapsto 15\right)}}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Diaframe thinks: *HINT:* $\vdash \ulcorner m = 10 \urcorner \vee \ulcorner m \neq 10 \urcorner$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \rightarrow\ \ m \equiv 0 \pmod 5 \rightarrow$$

$$\dfrac{\dfrac{\vdash \ulcorner m \neq 10 \urcorner \mathrel{-\!\!*} \ell \mapsto m \mathrel{-\!\!*} \ell \mapsto 15}{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \mathrel{-\!\!*} \ell \mapsto 15\right)}}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Diaframe thinks: *HINT:* $\vdash \ulcorner m = 10 \urcorner \vee \ulcorner m \neq 10 \urcorner$

Disjunction example, revisited

$$\forall m : \mathbb{Z}.\;\; 7 \le m \le 18 \;\rightarrow\; m \equiv 0 \pmod 5 \rightarrow$$

$$\frac{\dfrac{\vdash \ulcorner m \neq 10 \urcorner \twoheadrightarrow \ell \mapsto m \twoheadrightarrow \ell \mapsto 15}{\vdash \ulcorner m = 10 \urcorner \vee \left(\ell \mapsto m \twoheadrightarrow \ell \mapsto 15\right)}}{\ell \mapsto m \vdash \ell \mapsto 10 \vee \ell \mapsto 15}$$

Disjunction example, revisited

If `lia` was not improved, remaining goal is:

$$\forall m : \mathbb{Z}.\ \ 7 \leq m \leq 18 \ \longrightarrow\ \ m \equiv 0 \pmod 5 \longrightarrow$$
$$m \neq 10 \longrightarrow m = 15 \qquad ✔$$

Implementation challenges

How to define and detect a ‘connection’? Account for:

- modalities
- quantification

When to commit to a disjunct? as late as possible, but..

Overview

1. Backtracking is unwanted
2. Case distinctions make disjunctions harder
3. Idea: find connections from hypothesis to goal

   application to our example
4. *Limitations*

Limitations

Will commit to wands in disjunctions

$\ell \mapsto 15 \vdash (P \twoheadrightarrow \ell \mapsto 10) \vee \ell \mapsto 15$ ✗

Limitations

Will commit to wands in disjunctions

$\ell \mapsto 15 \vdash (P \mathrel{-\!\!*} \ell \mapsto 10) \lor \ell \mapsto 15$ ✗

May still commit too early

$\ell \mapsto 15 \vdash (\exists m.\, \ell \mapsto m * \ulcorner m = 10 \urcorner) \lor \ell \mapsto 15$ ✗

Limitations

Will commit to wands in disjunctions

$\ell \mapsto 15 \vdash (P \mathrel{-\!\!*} \ell \mapsto 10) \vee \ell \mapsto 15$ ✗

May still commit too early

$\ell \mapsto 15 \vdash (\exists m.\, \ell \mapsto m * \ulcorner m = 10 \urcorner) \vee \ell \mapsto 15$ ✗

Order of disjuncts matters

$\ell \mapsto 15 \vdash \ell \mapsto 15 \vee (\exists m.\, \ell \mapsto m * \ulcorner m = 10 \urcorner)$

Limitations

Will commit to wands in disjunctions

May still commit too early

Order of disjuncts matters

… Diaframe provides some tactics to help with this

Conclusion

Diaframe, proof automation library for Iris:

1. Extensible for other goals

   i.e., logical atomicity, contextual refinement

2. Better support for disjunctions

   by finding *connections* from hypothesis to goal

3. Available on opam: `coq-diaframe`

Questions?

Hint definition, simple

$$H, [L] \Vdash A * [U] \mid [D] \;:=\; H * L \vdash (A * U) \vee D$$

Hint application, simple

$$
\frac{H, [L] \Vdash A * [U] \| [D] \qquad \Delta \vdash \left(L * \begin{array}{c} U \mathrel{-\!\!*} G_1 \\ \land \\ D \mathrel{-\!\!*} ((A * G_1) \lor G_2) \end{array} \right) \lor (H \mathrel{-\!\!*} G_2)}{\Delta, H \vdash (A * G_1) \lor G_2}
$$

Hint definition, full

$$H, [\vec{y}; L] \Vdash \left[{}^{\mathcal{E}_3}{\Rrightarrow}^{\mathcal{E}_2}\right] \vec{x}; A * [U], [D] :=$$

$$\forall \vec{y}. \quad H * L \vdash {}^{\mathcal{E}_3}{\Rrightarrow}^{\mathcal{E}_2} (\exists \vec{x}. A * U) \lor D$$

Hint application, ‘full’

$$\dfrac{H, [\vec{y}; L] \Vdash \left[{}^{\mathcal{E}_3}\!\Rrightarrow^{\mathcal{E}_2}\right] \vec{x}; A * [U], [D] \qquad \Delta \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_3} \left(\exists \vec{y}.\, L * \begin{array}{c} \forall \vec{x}.\, U \mathrel{-\!\!*} G_1 \\ \wedge \\ D \mathrel{-\!\!*} ((\exists \vec{x}.\, A * G_1) \vee G_2) \end{array} \right) \vee (H \mathrel{-\!\!*} G_2)}{\Delta, H \vdash {}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} (\exists \vec{x}.\, A * G_1) \vee G_2}$$