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 $P^N$
- support for ghost state $a^γ$
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 $I$ and symbolic execution:

$$\Delta \vdash I \Rightarrow I \ast \text{wp } e \{ \Phi \}$$
Disjunctions in Iris verifications

After opening invariant $l_1 \lor l_2$ and symbolic execution:

$$\Delta \vdash \iff (l_1 \lor l_2) \ast \wp e \{\Phi\}$$
Disjunction example

\[ \forall m \in \mathbb{Z}. \ 7 \leq m \leq 13 \rightarrow m \equiv 0 \pmod{5} \rightarrow \\
\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \]
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:

\[
\begin{array}{c}
\text{solved or unsolved} \\
\hline
\vdots \\
\hline
\Delta \vdash P \\
\hline
\Delta \vdash P \lor Q \quad \text{TRY-LEFT}
\end{array}
\]
Backtracking proof search on disjunctions

As done by auto, old Diaframe, Caper:

\[
\begin{align*}
\text{solved or unsolved} \\
\vdots \\
\vdots \\
\Delta \vdash P \\
\Delta \vdash P \lor Q
\end{align*}
\]

if unsolved: go back and try right
Disjunction example, try left

\[
\forall m : \mathbb{Z}. \ 7 \leq m \leq 13 \implies m \equiv 0 \pmod{5} \implies \\
\begin{array}{c}
\vdash \neg m = 10 \\
\ell \leftrightarrow m \vdash \ell \leftrightarrow 10 \\
\ell \leftrightarrow m \vdash \ell \leftrightarrow 10 \lor \ell \leftrightarrow 15
\end{array}
\]
Disjunction example, try left

What if automation cannot prove

$$7 \leq m \leq 13 \rightarrow m \equiv 0 \pmod{5} \rightarrow m = 10?$$
Disjunction example, try left

What if automation cannot prove

\[ 7 \leq m \leq 13 \rightarrow m \equiv 0 \pmod{5} \rightarrow m = 10? \]

... since lia requires a special incantation for mod?
Disjunction example, try right

\[ \forall m : \mathbb{Z}. \ 7 \leq m \leq 13 \rightarrow m \equiv 0 \ (\text{mod} \ 5) \rightarrow \]

\[ \not\vdash \neg m = 10 \quad \times \quad \text{proof fails} \]

[1] DIAFRAME-HINT

\[ \ell \leftrightarrow m \vdash \ell \leftrightarrow 10 \]

[2] TRY-LEFT

\[ \ell \leftrightarrow m \vdash \ell \leftrightarrow 10 \lor \ell \leftrightarrow 15 \]
Disjunction example, try right

\( \forall m : \mathbb{Z}. \ 7 \leq m \leq 13 \to m \equiv 0 \pmod{5} \to \)

\[
\ell \mapsto m \vdash \ell \mapsto 15 \quad \text{X}
\]

\[
\ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \quad \text{TRY-RIGHT}
\]
Disjunction example, try right

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

\[ \ell \leadsto m \vdash \ell \leadsto 15 \xmark \]

\[ \ell \leadsto m \vdash \ell \leadsto 10 \lor \ell \leadsto 15 \ 	ext{TRY-RIGHT} \]

... 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

\[ \forall m : \mathbb{Z}. \ 7 \leq m \leq 18 \rightarrow m \equiv 0 \ (\text{mod} \ 5) \rightarrow \]
\[ \ell \dashv m \vdash \ell \dashv 10 \lor \ell \dashv 15 \]
Disjunction example: it gets worse

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

\[ \ell \mapsto m \uplus \ell \mapsto 10 \lor \ell \mapsto 15 \]

Backtracking directly is hopeless!

Case distinction \( m = 10 \lor m \neq 10 \) is not very obvious
Disjunctions in classical logic

\[
\Delta, \neg Q \vdash P
\]

\[
\Delta \vdash P \lor Q \quad \lor\text{-INTRO-L}
\]
Disjunctions in classical logic

$\Delta, \neg Q \vdash P$

$\Delta \vdash P \lor Q$ \hspace{1cm} $\Delta \vdash P \lor Q$

$\vdash \text{-INTRO-L}$ \hspace{1cm} $\neg\text{-ELIM}$

$\Delta, \neg Q \vdash P$
Disjunctions in classical logic

\[
\Delta, \neg Q \vdash P \\
\hline
\Delta \vdash P \lor Q
\]
\[\lor\text{-INTRO-L}\]

\[
\Delta \vdash P \lor Q \\
\hline
\Delta, \neg Q \vdash P
\]
\[\neg\text{-ELIM}\]

\[\lor\text{-INTRO-L} \text{ and commutes with proof rules! } i.e., \text{ with:}\]

\[
\Delta, P \vdash R \\
\hline
\Delta, Q \vdash R \\
\hline
\Delta, P \lor Q \vdash R
\]
\[\lor\text{-ELIM}\]
Disjunctions in classical logic

\[
P, \neg Q \vdash P \quad P \vdash Q \lor P
\]

\[
P, \neg P \vdash Q \quad Q, \neg P \vdash Q
\]

\[
P \lor Q, \neg P \vdash Q
\]

\[
P \lor Q \vdash Q \lor P
\]
...but Iris is inherently non-classical

Separation logics are incompatible with LEM if:

1. affine; or
2. step-indexed

⇒ 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*:

\[ A \rightarrow (B \lor C), A \vdash C \lor B \]

from hypothesis to goal
Disjunction example, revisited

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

\[ \ell \mapsto m \upharpoonright \ell \mapsto 10 \lor \ell \mapsto 15 \]
Disjunction example, revisited

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

\[ \ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \]

Diaframe thinks: HINT: \[ \ell \mapsto m \ast \neg m = 10 \vdash \ell \mapsto 10 \]
Disjunction example, revisited

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

\[ \vdash \left( m = 10 \right) \lor \left( \ell \mapsto m \ \ast \ell \mapsto 15 \right) \]

\[ \ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \]

Diaframe thinks: \( HINT: \ \ell \mapsto m \ \ast \left( \lceil m = 10 \rceil \vdash \ell \mapsto 10 \right) \)

21
Disjunction example, revisited

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

\[\top \quad \neg m = 10 \wedge (\ell \mapsto m \ast \ell \mapsto 15)\]

\[\ell \mapsto m \quad \vdash \ell \mapsto 10 \lor \ell \mapsto 15\]

Diaframe thinks: \(HINT: \ell \mapsto m \ast \neg m = 10 \vdash \ell \mapsto 10\)
Disjunction example, revisited

\[ \forall m : \mathbb{Z}. \ 7 \leq m \leq 18 \rightarrow m \equiv 0 \ (\text{mod} \ 5) \rightarrow \]

\[ \vdash \begin{cases} m = 10 \downarrow \vee (\ell \mapsto m \ast \ell \mapsto 15) \\
\ell \mapsto m \vdash \ell \mapsto 10 \ \vee \ \ell \mapsto 15 \end{cases} \]
Disjunction example, revisited

\[ \forall m : \mathbb{Z}. \ 7 \leq m \leq 18 \implies m \equiv 0 \ (\text{mod } 5) \]

\[ \vdash \neg m = 10 \lor (\ell \mapsto m \lor \ell \mapsto 15) \]

\[ \ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \]

Diaframe thinks: **HINT:** \[ \vdash \neg m = 10 \lor \neg m \neq 10 \]
Disjunction example, revisited

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

\[ \vdash \left[ m \neq 10 \right] \ast \ell \mapsto m \ast \ell \mapsto 15 \]

\[ \vdash \left[ m = 10 \right] \lor \left( \ell \mapsto m \ast \ell \mapsto 15 \right) \]

\[ \ell \mapsto m \vdash \ell \mapsto 10 \lor \ell \mapsto 15 \]

Diaframe thinks: HINT: \( \vdash \left[ m = 10 \right] \lor \left[ m \neq 10 \right] \)
Disjunction example, revisited

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

\[ \vdash \neg m \neq 10 \uparrow \star \ell \leftrightarrow m \star \ell \mapsto 15 \]

\[ \vdash \neg m = 10 \uparrow \vee (\ell \leftrightarrow m \star \ell \mapsto 15) \]

\[ \ell \leftrightarrow m \vdash \ell \leftrightarrow 10 \vee \ell \leftrightarrow 15 \]
Disjunction example, revisited

If lia was not improved, remaining goal is:

\[ \forall m : \mathbb{Z}. \quad 7 \leq m \leq 18 \implies m \equiv 0 \pmod{5} \implies m \neq 10 \implies m = 15 \]
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

\[ \ell \mapsto 15 \vdash (P \not\rightarrow \ell \mapsto 10) \lor \ell \mapsto 15 \]

\[ \times \]
Limitations

Will commit to wands in disjunctions
\[ \ell \mapsto 15 \vdash (P \not\implies \ell \mapsto 10) \lor \ell \mapsto 15 \]

May still commit too early
\[ \ell \mapsto 15 \vdash (\exists m. \ell \mapsto m \cdot \neg m = 10) \lor \ell \mapsto 15 \]
Limitations

Will commit to wands in disjunctions
\[ \ell \mapsto 15 \vdash (P \rightarrow \ell \mapsto 10) \lor \ell \mapsto 15 \]

May still commit too early
\[ \ell \mapsto 15 \vdash (\exists m. \ell \mapsto m \land \neg m = 10^{-1}) \lor \ell \mapsto 15 \]

Order of disjuncts matters
\[ \ell \mapsto 15 \vdash \ell \mapsto 15 \lor (\exists m. \ell \mapsto m \land \neg m = 10^{-1}) \]
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

\[ H, [L] \models A \ast [U] \Downarrow [D] \quad := \quad H \ast L \vdash (A \ast U) \lor D \]
Hint application, simple

$$H, [L] 
\not\models A \ast [U]||[D]$$

$$\Delta \vdash \left( \begin{align*}
U \ast G_1 \\
L \ast \land \\
D \ast ((A \ast G_1) \lor G_2)
\end{align*} \right) \lor (H \ast G_2)$$

$$\Delta, H \vdash (A \ast G_1) \lor G_2$$
$$H, [\vec{y}; L] \models [\mathcal{E}_3 \models \mathcal{E}_2] \vec{x}; A * [U], [D] :=$$

$$\forall \vec{y}. \quad H * L \vdash \mathcal{E}_3 \models \mathcal{E}_2 (\exists \vec{x}. A * U) \lor D$$
Hint application, ‘full’

\[ H, [\vec{y}; L] \models [\mathcal{E}_3 \Rightarrow \mathcal{E}_2] \vec{x}; A \ast [U], [D] \]

\[ \Delta \vdash \mathcal{E}_1 \Rightarrow \mathcal{E}_3 \left( \forall \vec{x}. U \ast G_1 \land \exists \vec{y}. L \ast \land D \ast ((\exists \vec{x}. A \ast G_1) \lor G_2) \right) \lor (H \ast G_2) \]

\[ \Delta, H \vdash \mathcal{E}_1 \Rightarrow \mathcal{E}_2 (\exists \vec{x}. A \ast G_1) \lor G_2 \]