Goal-Directed Proof Search

CIS700 — Fall 2024

Kris Micinski

Last time, saw G3ip, an intuitionistic sequent calculus.
Chapter 3 of the Negri and von Plato book presents a generalization to the classical sequent calculus, which adds multiple possible (disjunctive) outcomes on the right-hand side

Axiom $\dfrac{}{P, \Gamma \Rightarrow P}$

Logical rules:

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\!\to \frac{A \to B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \to B, \Gamma \Rightarrow C} \qquad R\!\to \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \to B}$$

This time, we will briefly talk about *goal-directed* proof search

Axiom $$\frac{}{P, \Gamma \Rightarrow P}$$

Logical rules:

$$L\wedge\ \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge\ \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot\ \frac{}{\bot\,, \Gamma \Rightarrow C}$$

$$L\vee\ \frac{A, \Gamma \Rightarrow C \qquad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1\ \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2\ \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\rightarrow\ \frac{A \rightarrow B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \rightarrow B, \Gamma \Rightarrow C} \qquad R\rightarrow\ \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

This time, we will briefly talk about *goal-directed* proof search

The idea in goal-directed proof search is to take a statement we want to prove and search backwards, exploring potential derivations to some depth

For example, if we take $\Rightarrow A \wedge A \to B \vee A$, we can see that only one rule possibly applies in G3ip; so we "apply" $R\to$ rule

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\to \frac{A \to B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \to B, \Gamma \Rightarrow C} \qquad R\to \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \to B}$$

Tactic-based theorem provers often present the **goal state** and a set of **assumptions** in context

Applications of rules (such as $R\rightarrow$) are done via tactics (e.g., in Coq, the "apply" tactic)

These tactics update the proof state: the environment (assumptions) and the current goal

Assumptions are…

$A \wedge A$

Goal is…

$B \vee A$

$$R\rightarrow \frac{A \wedge A \Rightarrow B \vee A}{\Rightarrow A \wedge A \rightarrow B \vee A}$$

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\rightarrow \frac{A \rightarrow B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \rightarrow B, \Gamma \Rightarrow C} \qquad R\rightarrow \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

Here we have two possible rules we could apply!

In a tactic-based prover, it's on **us** to choose the right one. Only applying $R\vee_2$ will lead us to the proof we want, otherwise we get an unprovable proof state
Note: we also could choose $L\vee$, we can do that now, or later—either way will lead us to a correct proof, and it's another option

$$R\rightarrow \frac{A \wedge A \Rightarrow B \vee A}{\Rightarrow A \wedge A \rightarrow B \vee A}$$

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\rightarrow \frac{A \rightarrow B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \rightarrow B, \Gamma \Rightarrow C} \qquad R\rightarrow \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

Assumptions are…

$A \wedge A$

Goal is…

B

STUCK

$$R\vee_1 \frac{A \wedge A \Rightarrow B}{A \wedge A \Rightarrow B \vee A}$$

$$R\rightarrow \frac{A \wedge A \Rightarrow B \vee A}{\Rightarrow A \wedge A \rightarrow B \vee A}$$

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\rightarrow \frac{A \rightarrow B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \rightarrow B, \Gamma \Rightarrow C} \qquad R\rightarrow \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

As the user, we may just give up on this proof and try it another way… By applying another tactic.

An automated search heuristic might employ backtracking to try another tactic

Assumptions are…

$A \wedge A$

Goal is…

B

Backtrack

$$R\to \dfrac{R\vee_2 \dfrac{A \wedge A \Rightarrow A}{A \wedge A \Rightarrow B \vee A}}{\Rightarrow A \wedge A \to B \vee A}$$

$$L\wedge \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\to \frac{A \to B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \to B, \Gamma \Rightarrow C} \qquad R\to \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \to B}$$

Only one rule applies this time (also applied before, we just didn't choose it yet): $L\wedge$, which solves the goal

Assumptions are…

$A \wedge A$

Goal is…

B

Axiom

$$
\begin{array}{ll}
L\wedge & \dfrac{A, A \Rightarrow A}{A \wedge A \Rightarrow A} \\
R\vee_2 & \dfrac{A \wedge A \Rightarrow A}{A \wedge A \Rightarrow B \vee A} \\
R\rightarrow & \dfrac{A \wedge A \Rightarrow B \vee A}{\Rightarrow A \wedge A \rightarrow B \vee A}
\end{array}
$$

$$L\wedge \; \frac{A, B, \Gamma \Rightarrow C}{A \wedge B, \Gamma \Rightarrow C} \qquad R\wedge \; \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B} \qquad L\bot \; \frac{}{\bot, \Gamma \Rightarrow C}$$

$$L\vee \; \frac{A, \Gamma \Rightarrow C \quad B, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C} \qquad R\vee_1 \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \qquad R\vee_2 \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$$

$$L\rightarrow \; \frac{A \rightarrow B, \Gamma \Rightarrow A \qquad B, \Gamma \Rightarrow C}{A \rightarrow B, \Gamma \Rightarrow C} \qquad R\rightarrow \; \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \rightarrow B}$$

In a **tactic-based** prover, users use commands to guide which tactics to apply—this enables grappling with the large potential number of options at any one point in the proof, and many provers also enable using a logic programming language (Coq/LTac, Lean4, …) to enable automating proof search

Apply $R\rightarrow$
Apply $R\vee_2$
Apply $L\wedge$
Axiom
QED

$$
\cfrac{\cfrac{\cfrac{\overset{\textit{Axiom}}{A, A \Rightarrow A}}{A \wedge A \Rightarrow A}\,L\wedge}{A \wedge A \Rightarrow B \vee A}\,R\vee_2}{\Rightarrow A \wedge A \rightarrow B \vee A}\,R\rightarrow
$$

For example, the left is what a pseudo-proof-script might look like for the proof tree on the right. The script is linear (no branches) because there are no subgoals in the proof.

As the user types a proof script, the goal and context is updated to guide the user in helping constructing a tactic. There are very powerful tactics like **lia** (handles ~all linear arithmetic goals), **ring** (solves problems related to ring theory), **auto** (tries everything in scope up to some bound).