Aesop: White-Box Best-First Proof Search for Lean

Jannis Limperg[1] Asta Halkjær From[2]

[1]Vrije Universiteit Amsterdam, jannis@limperg.de

[2]Technical University of Denmark, ahfrom@dtu.dk

TU Delft, 15 February 2023

White-Box and Black-Box Proof Search

Proof Search Without Metavariables

Proof Search With Metavariables

White-Box and Black-Box Proof Search

Proof Search Without Metavariables

Proof Search With Metavariables

Interactive Theorem Proving Is Great

- No functional bugs

Interactive Theorem Proving Is Great

- No functional bugs
- Small kernel, big trust

Interactive Theorem Proving Is Great

- No functional bugs
- Small kernel, big trust
- Can verify everything*

Interactive Theorem Proving Is Great

- No functional bugs
- Small kernel, big trust
- Can verify everything*
- No functional bugs!

Interactive Theorem Proving Is Annoying

- Have to actually understand the code I wrote yesterday.

Interactive Theorem Proving Is Annoying

- Have to actually understand the code I wrote yesterday.
- Have to prove lots of trivialities.

Interactive Theorem Proving Is Annoying

- Have to actually understand the code I wrote yesterday.
- Have to prove lots of trivialities.

$$a \in [b] \leftrightarrow a = b$$

Interactive Theorem Proving Is Annoying

- Have to actually understand the code I wrote yesterday.
- Have to prove lots of trivialities.

$$a \notin xs \to a \notin ys \to a \notin xs ++ ys$$

Interactive Theorem Proving Is Annoying

- Have to actually understand the code I wrote yesterday.
- Have to prove lots of trivialities.

$$\mathrm{map}\ f\ xs \subseteq \mathrm{map}\ f\ ys \leftrightarrow xs \subseteq ys \quad \text{if } f \text{ is injective}$$

How Do We Make It Less Annoying?

1. Convince lots of mathematicians that they should formalise boring stuff for the greater good.

How Do We Make It Less Annoying?

1. Convince lots of mathematicians that they should formalise boring stuff for the greater good.
2. Let the computer do the boring stuff.

White-Box and Black-Box Proof Search

Black-box
hammers
SMT solvers
ML-based provers
Coq `sauto`
Agsy

White-box
Coq `eauto`
Matita `auto`
Isabelle `auto`
Isabelle `auto2`
PVS `grind`
ACL2 waterfall
Aesop

White-Box and Black-Box Proof Search

Black-box	**White-box**
fully automatic	needs configuration
powerful	weak
the future	boring old tech

White-Box and Black-Box Proof Search

Black-box	**White-box**
fully automatic	needs configuration
powerful	weak
the future	boring old tech
complex	simple
unpredictable	predictable
opaque	transparent
fixed performance	customisable performance
proof export is hard	proof export is easy(ish)

White-Box and Black-Box Proof Search

Proof Search Without Metavariables

Proof Search With Metavariables

Basic Procedure

$$\vdash A \to C \to A \land (B \lor C)$$

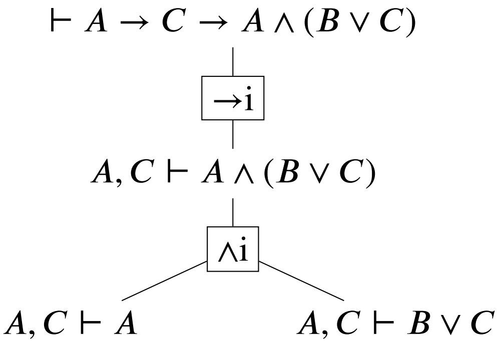
Basic Procedure

$$\vdash A \to C \to A \land (B \lor C)$$

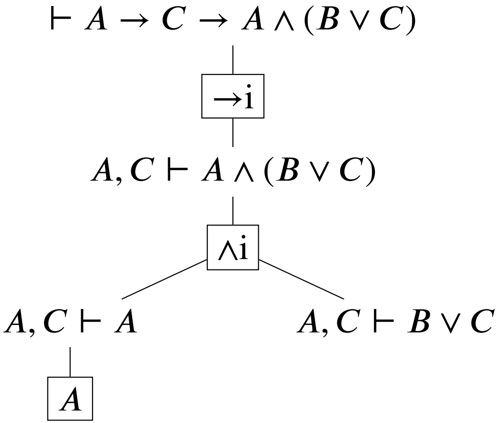
$\to$i

$$A, C \vdash A \land (B \lor C)$$

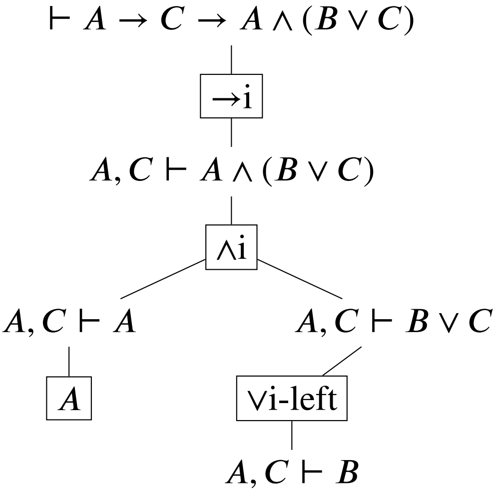
Basic Procedure



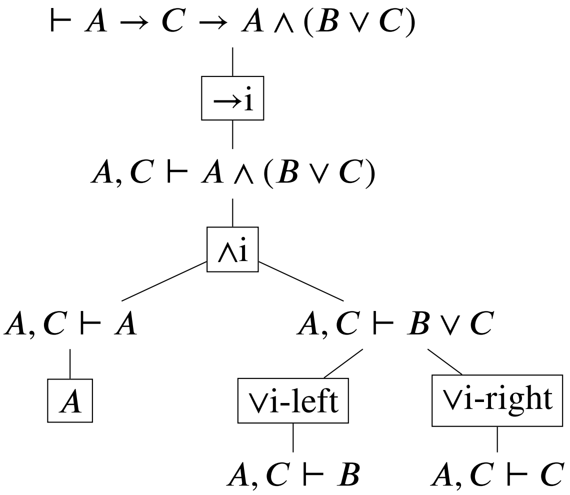
Basic Procedure



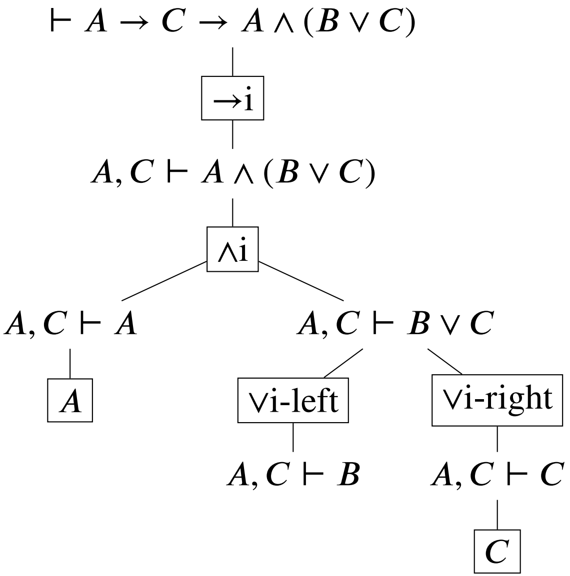
Basic Procedure



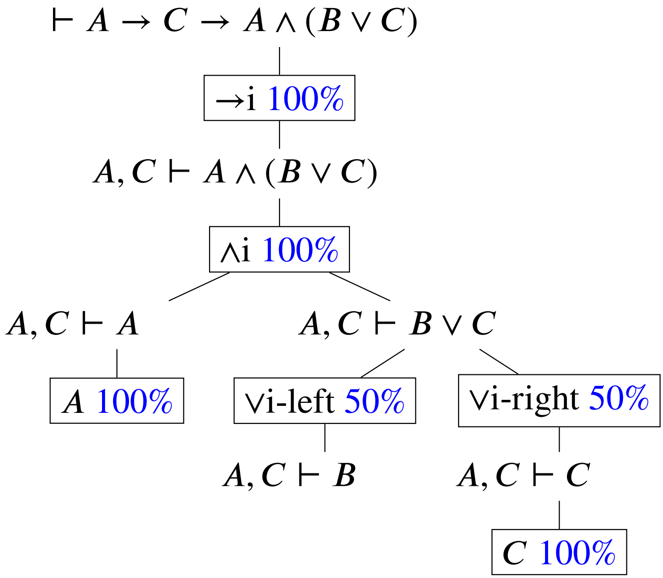
Basic Procedure



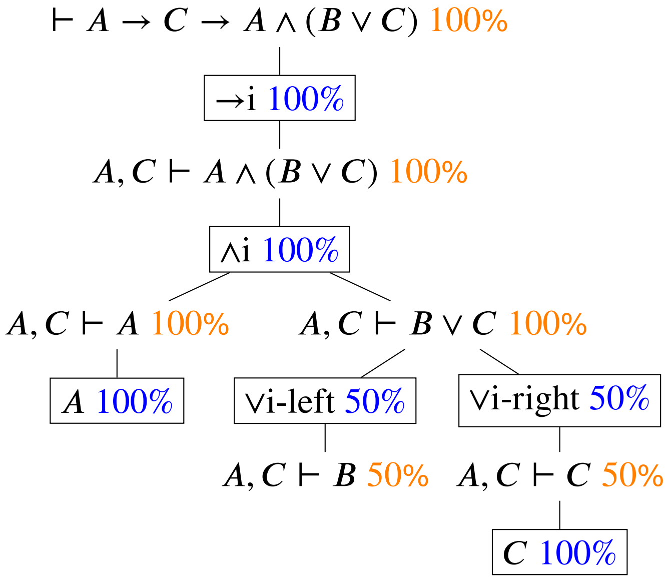
Basic Procedure



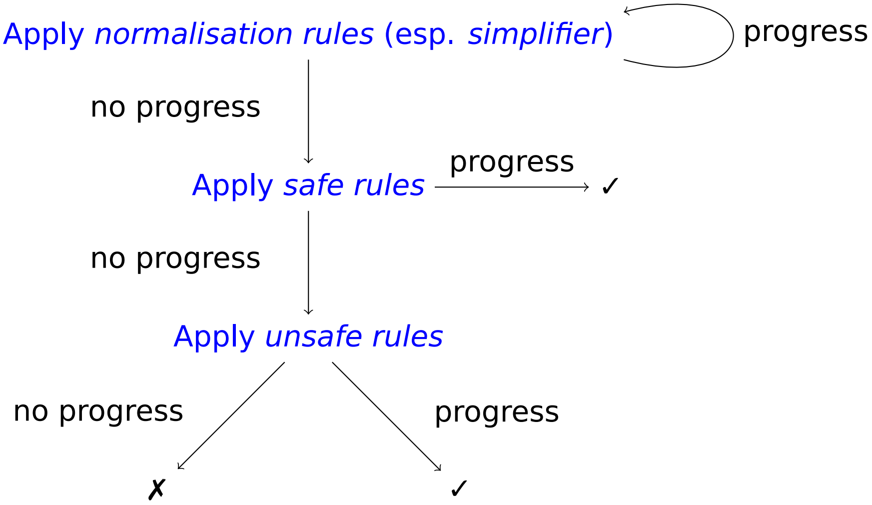
Best-First Search



Best-First Search

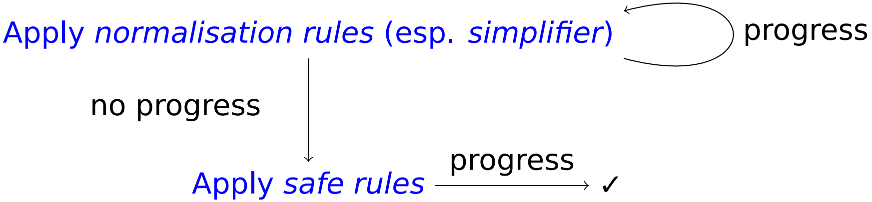


Extensions of the Basic Procedure

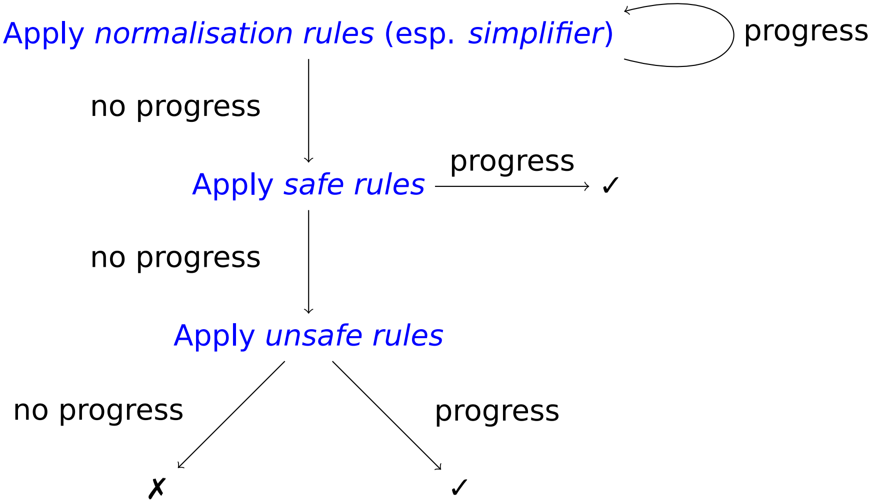


Apply *normalisation rules* (esp. *simplifier*) ↺ progress

$$\frac{\Gamma,\ A,\ B \vdash T}{\Gamma,\ A \wedge B \vdash T}\ \wedge\text{e}$$



$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \land B}\ \land\mathrm{i}$$


Apply *normalisation rules* (esp. *simplifier*)
progress
no progress
Apply *safe rules*
progress
✓
no progress
Apply *unsafe rules*
no progress
progress
✗
✓

White-Box and Black-Box Proof Search

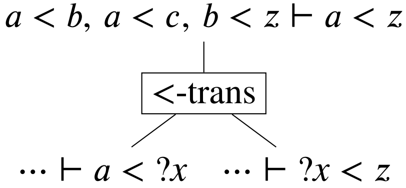
Proof Search Without Metavariables

Proof Search With Metavariables

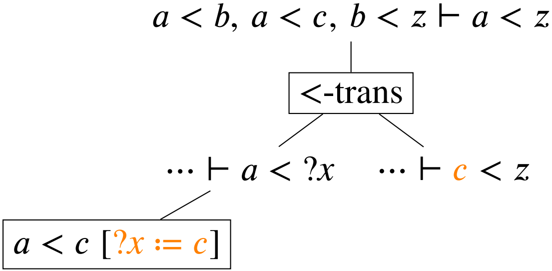
Proof Search With Metavariables

$$a < b,\ a < c,\ b < z \vdash a < z$$

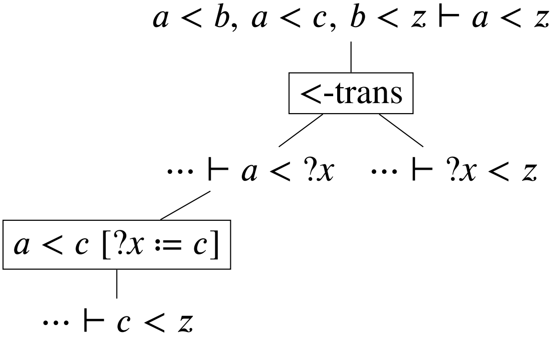
Proof Search With Metavariables



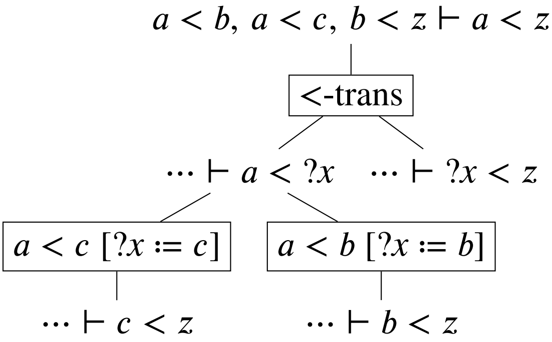
Proof Search With Metavariables



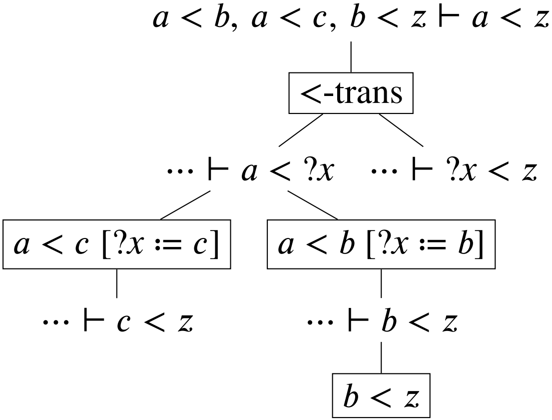
Proof Search With Metavariables



Proof Search With Metavariables



Proof Search With Metavariables



Also in the Paper

- Built-in rules
- Rule indexing
- UI for adding common sorts of rules
- Case studies
  - 173 basic lemmas about lists (Aesop + induction proves 94%)
  - Sequent calculus prover

Aesop: White-Box Best-First Proof Search for Lean

Jannis Limperg[1] Asta Halkjær From[2]

[1]Vrije Universiteit Amsterdam, jannis@limperg.de

[2]Technical University of Denmark, ahfrom@dtu.dk

TU Delft, 15 February 2023