Intuitionistic propositional logic and proof search: What you could consider knowing

Tarmo Uustalu
Institute of Cybernetics

Theory Days at Põlva, 25–27 Jan. 2008

Proof search for intuitionistic propositional logic

- In functional programming, we infer types for terms. What about inferring terms for types?
  Then we don't have to program?
- Via Curry-Howard, simply-typed lambda calculus is the same as intuitionistic propositional logic (IPL):
  types = formulae, lambda-terms = proofs.
- So this amounts to proof search.
- Tough: While proof search for CPL is NP-complete, this proof search for IPL is PSPACE-complete.

Natural deduction system for IPL

$$\frac{C \in \Gamma}{\Gamma \vdash_{e} C}\ \text{hyp} \qquad \frac{C\ \text{atom} \quad \Gamma \vdash_{e} C}{\Gamma \vdash_{i} C}\ \text{mid}$$

$$\frac{}{\Gamma \vdash_{i} \top}\ \wedge\top$$

$$\frac{\Gamma \vdash_{e} A \wedge B}{\Gamma \vdash_{e} A}\ \wedge\mathcal{E}_0 \qquad \frac{\Gamma \vdash_{i} A_0 \quad \Gamma \vdash_{i} A_1}{\Gamma \vdash_{i} A_0 \wedge A_1}\ \wedge\mathcal{I}$$

$$\frac{\Gamma \vdash_{e} A_0 \wedge A_1}{\Gamma \vdash_{e} A_1}\ \wedge\mathcal{E}_1$$

$$\frac{\Gamma \vdash_{e} A \supset B \quad \Gamma \vdash_{i} A}{\Gamma \vdash_{e} B}\ \supset\mathcal{E} \qquad \frac{\Gamma, A \vdash_{i} B}{\Gamma \vdash_{i} A \supset B}\ \supset\mathcal{I}$$

- Proofs respecting the e/i annotations – β-normal proofs proofs respecting the atomic midformula condition – η-long-normal proofs

. . . with lambda terms

$$\frac{z : C \in \Gamma}{\Gamma \vdash_{\mathsf{e}} z : C}\ \text{hyp} \qquad \frac{C\ \text{atom} \quad \Gamma \vdash_{\mathsf{e}} t : C}{\Gamma \vdash_{\mathsf{i}} t : C}\ \text{mid}$$

$$\frac{}{\Gamma \vdash_{\mathsf{i}} () : \top}\ \wedge\top$$

$$\frac{\Gamma \vdash_{\mathsf{e}} t : A_0 \wedge A_{:}1}{\Gamma \vdash_{\mathsf{e}} \pi_0\, t : A_0}\ \wedge\mathcal{E}_0 \qquad \frac{\Gamma \vdash_{\mathsf{i}} t_0 : A_0 \quad \Gamma \vdash_{\mathsf{i}} t_1 : A_1}{\Gamma \vdash_{\mathsf{i}} (t_0, t_1) : A_0 \wedge A_1}\ \wedge\mathcal{I}$$

$$\frac{\Gamma \vdash_{\mathsf{e}} t : A_0 \wedge A_1}{\Gamma \vdash_{\mathsf{e}} \pi_1\, t : A_1}\ \wedge\mathcal{E}_1$$

$$\frac{\Gamma \vdash_{\mathsf{e}} t : A \supset B \quad \Gamma \vdash_{\mathsf{i}} u : A}{\Gamma \vdash_{\mathsf{e}} t\, u : B}\ \supset\mathcal{E} \qquad \frac{\Gamma, x : A \vdash_{\mathsf{i}} t : B}{\Gamma \vdash_{\mathsf{i}} \lambda x\, t : A \supset B}\ \supset\mathcal{I}$$

Proof of S

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{}{\ldots \vdash_{e} p \wedge q \supset r}\;\text{hyp}
          \qquad
          \dfrac{
            \dfrac{\dfrac{}{\ldots \vdash_{e} p}\;\text{hyp}}{\ldots \vdash_{i} p}\;\text{mid}
            \qquad
            \dfrac{
              \dfrac{
                \dfrac{}{\ldots \vdash_{e} p \supset q}\;\text{hyp}
                \qquad
                \dfrac{\dfrac{}{\ldots \vdash_{e} p}\;\text{hyp}}{\ldots \vdash_{i} p}\;\text{mid}
              }{\ldots \vdash_{e} q}\;\supset\mathcal{E}
            }{\ldots \vdash_{i} q}\;\text{mid}
          }{\ldots \vdash_{i} p \wedge q}\;\wedge\mathcal{I}
        }{\ldots \vdash_{e} r}\;\supset\mathcal{E}
      }{p \wedge q \supset r, p \supset q, p \vdash_{i} r}\;\text{mid}
    }{p \wedge q \supset r, p \supset q \vdash_{i} p \supset r}\;\supset\mathcal{I}
  }{p \wedge q \supset r \vdash_{i} (p \supset q) \supset (p \supset r)}\;\supset\mathcal{I}
}{\vdash_{i} (p \wedge q \supset r) \supset ((p \supset q) \supset (p \supset r))}\;\supset\mathcal{I}
$$

Multiple proofs of N

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p}\;\text{hyp}}{p \supset p, p \vdash_{\mathsf{i}} p}\;\text{mid}}{p \supset p \vdash_{\mathsf{i}} p \supset p}\;\supset\mathcal{I}}{\vdash_{\mathsf{i}} (p \supset p) \supset (p \supset p)}\;\supset\mathcal{I}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p \supset p}\;\text{hyp} \qquad \dfrac{\dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p}\;\text{hyp}}{p \supset p, p \vdash_{\mathsf{i}} p}\;\text{mid}}{p \supset p, p \vdash_{\mathsf{e}} p}\;\supset\mathcal{E}}{p \supset p, p \vdash_{\mathsf{i}} p}\;\text{mid}}{p \supset p \vdash_{\mathsf{i}} p \supset p}\;\supset\mathcal{I}}{\vdash_{\mathsf{i}} (p \supset p) \supset (p \supset p)}\;\supset\mathcal{I}$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p \supset p}\,\text{hyp}
      \qquad
      \dfrac{
        \dfrac{
          \dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p \supset p}\,\text{hyp}
          \qquad
          \dfrac{
            \dfrac{}{p \supset p, p \vdash_{\mathsf{e}} p}\,\text{hyp}
          }{p \supset p, p \vdash_{\mathsf{i}} p}\,\text{mid}
        }{p \supset p, p \vdash_{\mathsf{e}} p}\,\supset\mathcal{E}
      }{p \supset p, p \vdash_{\mathsf{i}} p}\,\text{mid}
    }{
      \dfrac{p \supset p, p \vdash_{\mathsf{e}} p}{p \supset p, p \vdash_{\mathsf{i}} p}\,\text{mid}
    }\,\supset\mathcal{E}
  }{p \supset p \vdash_{\mathsf{i}} p \supset p}\,\supset\mathcal{I}
}{\vdash_{\mathsf{i}} (p \supset p) \supset (p \supset p)}\,\supset\mathcal{I}
$$

Sequent calculus

$$\frac{C \text{ atom} \quad C \in \Gamma}{\Gamma \vdash C}\ \text{init} \qquad \frac{\Gamma \vdash C \quad \Gamma, C \vdash A}{\Gamma \vdash A}\ \text{cut}$$

$$\frac{\Gamma \vdash C}{\Gamma, \top \vdash C}\ \top\mathcal{L} \qquad \frac{}{\Gamma \vdash \top}\ \top\mathcal{R}$$

$$\frac{\Gamma, A_0, A_1 \vdash C}{\Gamma, A_0 \wedge A_1 \vdash C}\ \wedge\mathcal{L} \qquad \frac{\Gamma \vdash A_0 \quad \Gamma \vdash A_1}{\Gamma \vdash A_0 \wedge A_1}\ \wedge\mathcal{R}$$

$$\frac{\Gamma, \underline{A \supset B} \vdash A, \not{C} \quad \Gamma, B \vdash C}{\Gamma, A \supset B \vdash C}\ \supset\mathcal{L} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ \supset\mathcal{R}$$

- Note the choice of A in favor of C and the contraction (duplication) of $A \supset B$ in the $\supset L$ rule.
- Proofs without cut – β-normal proofs,
  proofs respecting the atomic initformula condition –
  η-long-normal proofs

. . . with lambda terms

$$\frac{C \text{ atom} \quad z : C \in \Gamma}{\Gamma \vdash z : C}\ \text{init} \qquad \frac{\Gamma \vdash t : C \quad \Gamma, z : C \vdash u : A}{\Gamma \vdash u[t/z] : A}\ \text{cut}$$

$$\frac{\Gamma \vdash t : C}{\Gamma, x : \top \vdash t : C}\ \top\mathcal{L} \qquad \frac{}{\Gamma \vdash () : \top}\ \top\mathcal{R}$$

$$\frac{\Gamma, y_0 : A_0, y_1 : A_1 \vdash t : C}{\Gamma, x : A_0 \wedge A_1 \vdash t[\pi_0\, x/y_0][\pi_1\, x/y_1] : C}\ \wedge\mathcal{L} \qquad \frac{\Gamma \vdash t_0 : A_0 \quad \Gamma \vdash t_1 : A_1}{\Gamma \vdash (t_0, t_1) : A_0 \wedge A_1}\ \wedge\mathcal{R}$$

$$\frac{\Gamma, x : A \supset B \vdash t : A \quad \Gamma, y : B \vdash u : C}{\Gamma, x : A \supset B \vdash u[x\, t/y] : C}\ \supset\mathcal{L} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x\, t : A \supset B}\ \supset\mathcal{R}$$

Proof of S

$$
\dfrac{\dfrac{}{p \land q \supset r, p \supset q, p \vdash p}\;\text{init} \qquad \dfrac{}{p \land q \supset r, p \vdash q}\;\text{init}}{p \land q \supset r, p \supset q, p \vdash q}\;\supset\mathcal{L}
$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p \land q \supset r, p \supset q, p \vdash p}\;\text{init} \qquad \begin{matrix} \vdots \\ p \land q \supset r, p \supset q, p \vdash q \end{matrix}}{p \land q \supset r, p \supset q, p \vdash p \land q}\;\land\mathcal{I} \qquad \dfrac{}{r, p \supset q, p \vdash r}\;\text{init}}{p \land q \supset r, p \supset q, p \vdash r}\;\supset\mathcal{L}}{p \land q \supset r, p \supset q \vdash p \supset r}\;\supset\mathcal{R}}{p \land q \supset r \vdash (p \supset q) \supset (p \supset r)}\;\supset\mathcal{R}}{\vdash (p \land q \supset r) \supset ((p \supset q) \supset (p \supset r))}\;\supset\mathcal{R}
$$

How to search for a proof?

- Choice between
  - natural deduction vs sequent calculus
  - backward (root-first) search vs forward (leaves-first) search
- The two directions don't mean the same thing for natural deduction and sequent calculus:
  - forward with $\mathcal{E}$ rules $=$ backward with $\mathcal{L}$ rules.
- Good idea to search for normal proofs (every provable formula has a normal proof).
- Good idea to realize that for normal proofs we have a (polarized) subformula property.
- Today:
  - backward search in sequent calculus (well-known)
  - forward search in natural deduction (little-known)

Backward search in sequent calculus

- Rules except $\supset \mathcal{L}$ permutable, so any order of applying them is give the same.
- Backtracking necessary because of the choice in $\supset \mathcal{L}$.
- Good idea to minimize its effect by postponing applications of this rule.
- In addition, because of the contraction in $\supset \mathcal{L}$, proof search may loop.
- Solutions:
    - loop-detection
    - switching to a contraction-free sequent calculus
- Loop-detection: If $\Gamma' \subseteq \Gamma$, then proof of $\Gamma' \to C$ not attempted in a proof attempt of $\Gamma \to C$.

Necessity of backtracking

$$
\dfrac{\begin{matrix}\text{unprovable} \\ r \supset s, p \supset q, p \vdash r, \not{q}\end{matrix} \qquad \begin{matrix}\vdots \\ s, p \supset q, p \vdash q\end{matrix}}{r \supset s, p \supset q, p \vdash q} \supset \mathcal{L}
$$

$$
\dfrac{\dfrac{}{r \supset s, p \supset q, p \vdash p}\,\text{init} \qquad \dfrac{}{q, r \supset s, p \vdash q}\,\text{init}}{r \supset s, p \supset q, p \vdash q} \supset \mathcal{L}
$$

The problem of looping

$$\dfrac{\overset{\text{loop}}{p \supset p \vdash p} \qquad \dfrac{}{p \vdash p}\,\text{init}}{p \supset p \vdash p}\,\supset\mathcal{L}$$

Contraction-free sequent calculus (Vorobev)

(also Hudelmaier, Dyckhoff)
Replace rule

$$\frac{\Gamma, A \supset B \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \supset B \vdash C} \supset \mathcal{L}$$

with rules

$$\frac{A \text{ atom} \quad A \in \Gamma \quad \Gamma, B \vdash C}{\Gamma, A \supset B \vdash C} \supset \mathcal{L}_{\text{atom}}$$

$$\frac{\Gamma, B \vdash C}{\Gamma, \top \supset B \vdash C} \supset \mathcal{L}_{\top}$$

$$\frac{\Gamma, D_0 \supset (D_1 \supset B) \vdash C}{\Gamma, D_0 \wedge D_1 \supset B \vdash C} \supset \mathcal{L}_{\wedge}$$

$$\frac{\Gamma, E \supset B, D \vdash E \quad \Gamma, B \vdash C}{\Gamma, (D \supset E) \supset B \vdash C} \supset \mathcal{L}_{\supset}$$

- This does not find all proofs, only some proof of every provable formula.

...with lambda terms

Replace rule

$$\frac{\Gamma, x : A \supset B \vdash t : A \quad \Gamma, y : B \vdash u : C}{\Gamma, x : A \supset B \vdash u[x\,t/y] : C} \supset \mathcal{L}$$

with rules

$$\frac{A \text{ atom} \quad z : A \in \Gamma \quad \Gamma, y : B \vdash u : C}{\Gamma, x : A \supset B \vdash u[x\,z/y] : C} \supset \mathcal{L}_{\text{atom}}$$

$$\frac{\Gamma, y : B \vdash u : C}{\Gamma, x : \top \supset B \vdash u[y\,()/x] : C} \supset \mathcal{L}_{\top}$$

$$\frac{\Gamma, y : D_0 \supset (D_1 \supset B) \vdash u : C}{\Gamma, x : D_0 \wedge D_1 \supset B \vdash u[\lambda z\, y(\pi_0 z)\,(\pi_1 z)/x] : C} \supset \mathcal{L}_{\wedge}$$

$$\frac{\Gamma, x' : E \supset B, z : D \vdash s : E \quad \Gamma, y : B \vdash u : C}{\Gamma, x : (D \supset E) \supset B \vdash u[x\,(\lambda z\, s[\lambda w\, x(\lambda\_\, w)]/x'])/y] : C} \supset \mathcal{L}_{\supset}$$

Djinn

- A lambda-term synthesizer by Lennart Augustsson based on backward search in contraction-free sequent calculus.

Forward search in natural deduction

(Known as inverse method, Mints-style resolution, Stålmarck's method)

- With forward search, where should one start, if any sequent $\Gamma \vdash C$ with $C \in \Gamma$ qualifies as an axiom to start with?
- Idea: take the polarized subformula property of ND seriously.
- For any goal formula G, organize search in a ND calculus *specialized* for *this* formula.
- Notation:
  - egoals(G) – negative subformulas of G (e-goals)
  - igoals(G) – positive subformulas of G (i-goals)
  - hyps(G) – antecedents of positive subimplications of G (hypotheses)
    (these are a subset of the negative subformulas)

Goal-specialized natural deduction system

$$\frac{\Gamma \subseteq \mathrm{hyps}(G) \quad C \in \Gamma}{\Gamma \vdash_{\mathrm{e}} C}\ \mathrm{hyp} \qquad \frac{C \text{ atom} \quad C \in \mathrm{igoals}(G) \quad \Gamma \vdash_{\mathrm{e}} C}{\Gamma \vdash_{\mathrm{i}} C}\ \mathrm{mid}$$

$$\frac{\top \in \mathrm{igoals}(G)}{\Gamma \vdash_{\mathrm{i}} \top}\ \top\mathcal{I}$$

$$\frac{\Gamma \vdash_{\mathrm{e}} A \wedge B}{\Gamma \vdash_{\mathrm{e}} A}\ \wedge\mathcal{E}_0 \qquad \frac{\Gamma \vdash_{\mathrm{e}} A_0 \wedge A_1}{\Gamma \vdash_{\mathrm{e}} A_1}\ \wedge\mathcal{E}_1$$

$$\frac{A_0 \wedge A_1 \in \mathrm{igoals}(G) \quad \Gamma \vdash_{\mathrm{i}} A_0 \quad \Gamma \vdash_{\mathrm{i}} A_1}{\Gamma \vdash_{\mathrm{i}} A_0 \wedge A_1}\ \wedge\mathcal{I}$$

$$\frac{\Gamma \vdash_{\mathrm{e}} A \supset B \quad \Gamma \vdash_{\mathrm{i}} A}{\Gamma \vdash_{\mathrm{e}} B}\ \supset\mathcal{E} \qquad \frac{A \supset B \in \mathrm{igoals}(G) \quad \Gamma, A \vdash_{\mathrm{i}} B}{\Gamma \vdash_{\mathrm{i}} A \supset B}\ \supset\mathcal{I}$$

- In this system, one can only prove sequents $\Gamma \vdash_{\mathrm{e}} C$ where $\Gamma \subseteq \mathrm{hyps}(G)$ and $C \in \mathrm{egoals}(G)$ and $\Gamma \vdash_{\mathrm{i}} C$ where $\Gamma \subseteq \mathrm{hyps}(G)$ and $C \in \mathrm{igoals}(G)$.

Specialized natural deduction system for S

- Main goal:
  $G = (p \wedge q \supset r) \supset ((p \supset q) \supset (p \supset r))$
- e- and i-goals:
  $\text{egoals}(G) = \{p \wedge q \supset r, p \supset q, p, q, r\}$
  $\text{igoals}(G) = \{p, q, r, p \wedge q, p \supset r, (p \supset q) \supset (p \supset r),$
  $(p \wedge q \supset r) \supset ((p \supset q) \supset (p \supset r))\}$
- Hypotheses:
  $\text{hyps}(G) = \{p \wedge q \supset r, p \supset q, p\}$
- Example rules:

$$\frac{\Gamma \subseteq \text{hyps}(G) \quad \Gamma \vdash_{\text{i}} p \quad \Gamma \vdash_{\text{i}} q}{\Gamma \vdash_{\text{i}} p \wedge q} \wedge\mathcal{I}$$

$$\frac{\Gamma \subseteq \text{hyps}(G) \quad \Gamma \vdash_{\text{e}} p \wedge q \supset r \quad \Gamma \vdash_{\text{i}} p \wedge q}{\Gamma \vdash_{\text{e}} r} \supset\mathcal{E}$$

Forward search in natural deduction, ctd

- Basic idea now:
  Generate in forward manner all provable sequents $\Gamma \vdash_{\mathsf{e}} C$, $\Gamma \vdash_{\mathsf{i}} C$. If $\vdash_{\mathsf{i}} G$ is generated, a proof has been found.
- More detailed:
  For any $\Gamma \subseteq \mathrm{hyps}(G)$ produce all of its e- and i-conclusions in a separate process.
  If an i-goal B is achieved in the process for Γ, A and $A \supset B \in \mathrm{igoals}(G)$, communicate this to the process for Γ.
- With proper organization, this takes time $O(N \cdot 2^M)$ where
  - $N =$ size of G (# of subformula occurrences)
  - $M = |\mathrm{hyps}(G)|$ (# of positive subimplications of G)
- Bounding the interdependence of hypotheses (which gives incompleteness), we get $O(N)$.
- Practically, it makes sense to increase the bound iteratively.

Forward search in natural deduction, ctd

- Technical details:
- Work with names of goals and rules.
- Arrange for these static datastructures (in each process):
  - an association to each goal the list of rules it is a premise for
  - an association to each rule the goal it concludes
- Control generation with these dynamic datastructures (in each process):
  - a queue of rules ready to fire,
  - an association to each goal if it has been derived
  - an association to each rule the list of its premise goals not yet derived
- Generation: Initialize the dynamic datastructures. While queue nonempty, dequeue a rule and fire, i.e., update the dynamic datastructures.

Stålmarck's method

- Proof search for classical propositional logic based on the same ideas.
- Basis: A natural deduction system with signed formulae and a dilemma rule to account for bivalence. Forward search in a goal-specialized version.