Formal Verification of Proof Search and Countermodel Construction for Intuitionistic Propositional Logic

Liisi Nõojärv
Supervisor Tarmo Uustalu

Tallinn University of Technology

Reliability

Soundness: only valid statements are provable

Completeness: we can prove everything that is valid

Proof done in Lean

Proof search

Proof in what system?

- Intuitionistic (statement is true, only if we have proof)
- Sequent calculus

$$\Gamma \vdash \Delta$$

- Gentzen LJ => G3ip/m-G3ip => IG

Proof search is performed root-up: from the goal sequent we move upward with applying inference rules backwards until axioms are reached.

What is needed

- **Termination** (nontrivial in intuitionistic systems)
- **Soundness**
- **Completeness**
  - Refutation calculus
  - **Counter-model** (witness of unprovability)

Algorithm returns EITHER proof(s) OR refutation(s)

$$\neg p = p \supset \bot$$

$$\dfrac{\dfrac{\dfrac{}{p \vdash \bot, p}\,\mathrm{Ax}}{\vdash p, \neg p}\,R\supset}{\vdash p \vee \neg p}\,R\vee$$

classical calculus (G3c)

$$\dfrac{\dfrac{p \vdash \bot}{\vdash p, \neg p}\,R\supset}{\vdash p \vee \neg p}\,R\vee$$

Multi-succedent calculus (m-G3ip)

Corsi and Tassi IG

IG is a multi-succedent intuitionistic system.

Metarules: how and when to apply implication rules.

Provides termination for proof search.

$$\frac{}{p, \Gamma \vdash p, \Delta}\ \mathrm{Id} \qquad \frac{}{\bot, \Gamma \vdash \Delta}\ L\bot$$

$$\frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}\ L\wedge \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ R\wedge$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}\ L\vee \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ R\vee$$

$$\frac{A \supset B, \Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{A \supset B, \Gamma \vdash \Delta}\ L\supset \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \supset B, \Delta}\ R\supset$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash A \supset B, \Delta}\ \textit{a fortiori}$$

Termination

$$\frac{}{p, \Gamma \vdash p, \Delta}\ \mathrm{Ax} \qquad \frac{}{\bot, \Gamma \vdash \Delta}\ \bot L$$

$$\frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}\ L\wedge \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ R\wedge$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}\ L\vee \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ R\vee$$

$$\frac{A \supset B, \Gamma \vdash A, \Delta \quad B, \Gamma \vdash \Delta}{A \supset B, \Gamma \vdash \Delta}\ L\supset \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \supset B, \Delta}\ R\supset$$

Endless proofsearch caused by copy

THE JOURNAL OF SYMBOLIC LOGIC
Volume 72, Number 4, Dec. 2007

INTUITIONISTIC LOGIC FREED OF ALL METARULES

GIOVANNA CORSI AND GABRIELE TASSI

Abstract. In this paper we present two calculi for intuitionistic logic. The first one, IG, is characterized by the fact that every proof-search terminates and termination is reached without jeopardizing the subformula property. As to the second one, SIC, proof-search terminates, the subformula property is preserved and moreover proof-search is performed without any recourse to metarules, in particular there is no need to back-track. As a consequence, proof-search in the calculus SIC is accomplished by a *single* tree as in classical logic.

§1. Introduction. Proof search in sequent calculi for intuitionistic logic is performed from root to leaves, by applying the rules of inference to the node that in that step of computation is a leaf. One always needs a metarule - a rule for applying rules - to choose the rule or the rules that can be applied to a leaf; this is usually a simple pattern-matching between the formula and the formula schema of the conclusion of the rule of inference, if this is presented in a schematic notation. If more than one rule can be applied at a given time, the final proof-tree should not depend on which rule is chosen. However, it is not always the case that a metarule is a simple pattern matching; there are computable metarules that are not expressible in a schematic notation: usually these rules are simply given in the natural language, as side conditions.

CONTRACTION-FREE SEQUENT CALCULI FOR INTUITIONISTIC LOGIC

ROY DYCKHOFF

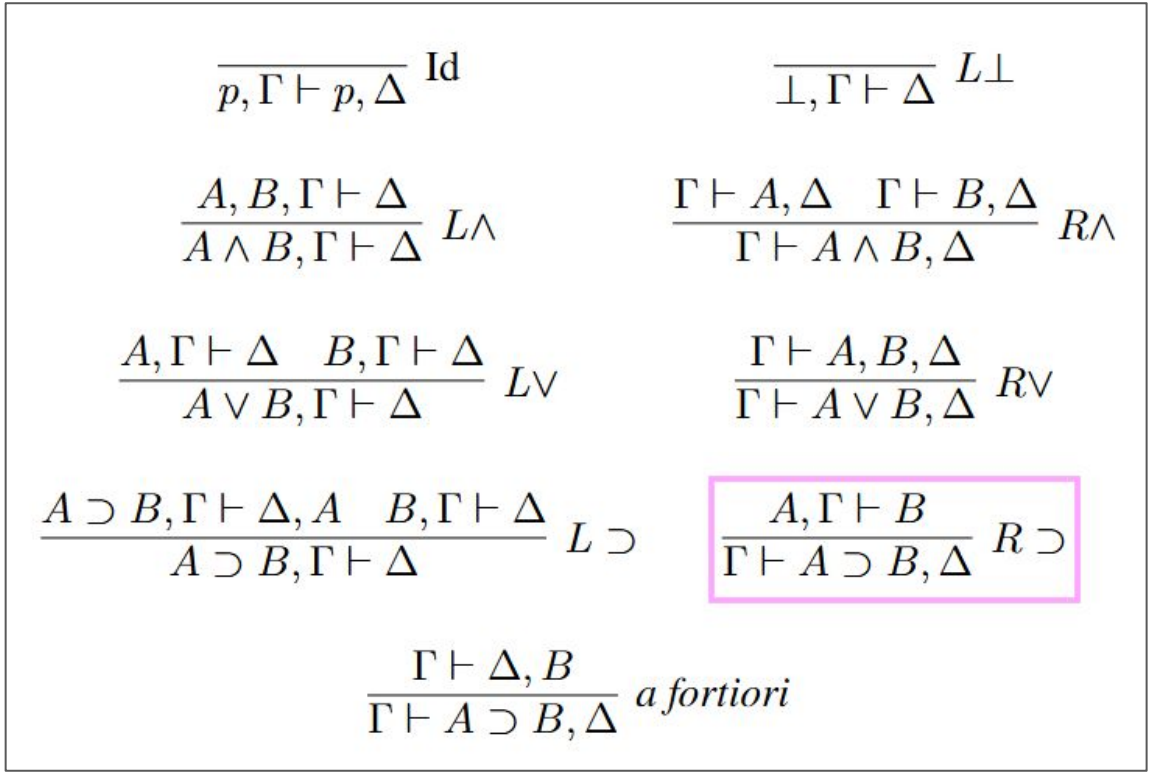
§0. Prologue. Gentzen's sequent calculus LJ, and its variants such as G3 [21], are (as is well known) convenient as a basis for automating proof search for IPC (intuitionistic propositional calculus). But a problem arises: that of detecting loops, arising from the use (in reverse) of the rule $\supset \Rightarrow$ for implication introduction on the left. We describe below an equivalent calculus, yet another variant on these systems, where the problem no longer arises: this gives a simple but effective decision procedure for IPC.

The underlying method can be traced back forty years to Vorob′ev [33], [34]. It has been rediscovered recently by several authors (the present author in August 1990, Hudelmaier [18], [19], Paulson [27], and Lincoln et al. [23]). Since the main idea is not plainly apparent in Vorob′ev's work, and there are mathematical applications [28], it is desirable to have a simple proof. We present such a proof, exploiting the Dershowtiz-Manna theorem [4] on multiset orderings.

Non-invertibility

Important to distinguish invertible and non-invertible rules for proof search

Invertibility: If a sequent is derivable in the conclusion of the inference rule, derivability in the premises follows.



Proof search algorithm

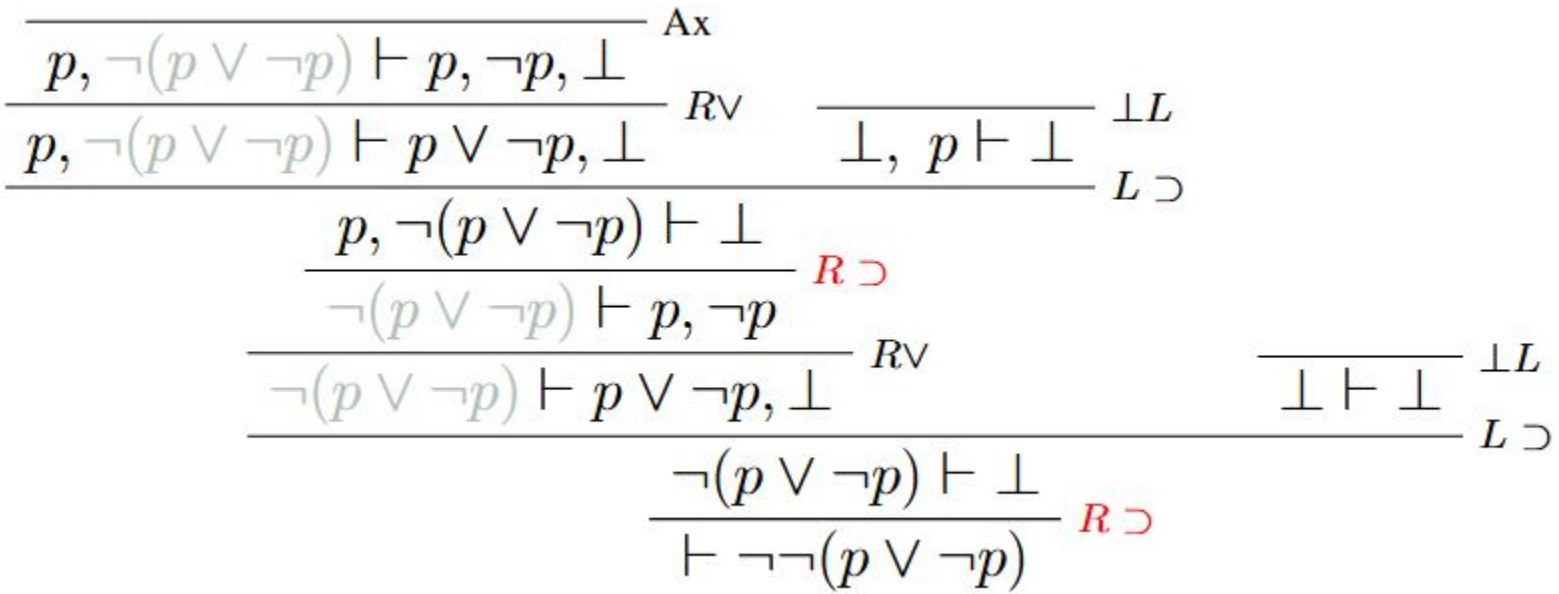
Algorithm works in two alternating phases:

1. First, all invertible rules are applied deterministically on the right and left side, until only atoms and (right)implications are left
2. Only then, apply non-invertible rule to all formulas at once

$$\frac{A_1, \Gamma \vdash B_1}{\Gamma \vdash A_1 \supset B_1}\, R\supset \quad \cdots \quad \frac{A_n, \Gamma \vdash B_n}{\Gamma \vdash A_n \supset B_n}\, R\supset$$

$$\Gamma \vdash A_1 \supset B_1, \ldots, A_n \supset B_n, \Delta$$

IG Proof


Ax
$p, \neg(p \vee \neg p) \vdash p, \neg p, \bot$
$R\vee$
$p, \neg(p \vee \neg p) \vdash p \vee \neg p, \bot$
$\bot L$
$\bot, p \vdash \bot$
$L\supset$
$p, \neg(p \vee \neg p) \vdash \bot$
$R\supset$
$\neg(p \vee \neg p) \vdash p, \neg p$
$R\vee$
$\neg(p \vee \neg p) \vdash p \vee \neg p, \bot$
$\bot L$
$\bot \vdash \bot$
$L\supset$
$\neg(p \vee \neg p) \vdash \bot$
$R\supset$
$\vdash \neg\neg(p \vee \neg p)$

Termination

Termination is proven with an ordering consisting of:

- r = number of applications of the **R** $\supset$ rule along the branch,
- n = complexity of the formulas

$$(r, n) \prec (r', n') \quad \text{iff} \quad r > r' \vee (r = r' \wedge n < n').$$

r needs to be upper-bounded, for the order to be well-founded

Kripke semantics

- Multiple worlds represent gathered information
- Kripke model: **(W, ≥, (forced, rejected))**
- Truth monotonicity:
  - if w |= p, then ∀ w′ ≥ w, w′ |= p
  - if w ⊭ p, then ∀ w′ ≤ w, w’⊭ p
- Knowledge base can only grow, nothing can be forgotten

$$
\begin{array}{rcl}
w \models p & \text{iff} & p \in \text{forced} \\
w \not\models \bot & & \\
w \models A \wedge B & \text{iff} & w \models A \text{ and } w \models B \\
w \models A \vee B & \text{iff} & w \models A \text{ or } w \models B \\
w \models \neg A & \text{iff} & \forall\, w' \geq w,\ w' \not\models A \\
w \models A \supset B & \text{iff} & \forall\, w' \geq w,\ w' \not\models A \text{ or } w' \models B
\end{array}
$$

RIG (Refutation system for IG)

$$\frac{}{\Gamma, E \nvdash \Delta}\ \mathrm{Ax}^{\star}$$

$$\frac{A, B, \Gamma, E \nvdash \Delta}{A \wedge B, \Gamma, E \nvdash \Delta}\ L\wedge \qquad \frac{\Gamma, E \nvdash A, \Delta}{\Gamma, E \nvdash A \wedge B, \Delta}\ R_1\wedge \qquad \frac{\Gamma, E \nvdash B, \Delta}{\Gamma, E \nvdash A \wedge B, \Delta}\ R_2\wedge$$

$$\frac{A, \Gamma, E \nvdash \Delta}{A \vee B, \Gamma, E \nvdash \Delta}\ L_1\vee \qquad \frac{B, \Gamma, E \nvdash \Delta}{A \vee B, \Gamma, E \nvdash \Delta}\ L_2\vee \qquad \frac{\Gamma, E \nvdash A, B, \Delta}{\Gamma, E \nvdash A \vee B, \Delta}\ R\vee$$

$$\frac{\Gamma, A \supset B, E \nvdash A, \Delta}{A \supset B, \Gamma, E \nvdash \Delta}\ L_1\supset \qquad \frac{B, \Gamma, E \nvdash \Delta}{A \supset B, \Gamma, E \nvdash \Delta}\ L_2\supset \qquad \frac{\Gamma, E \nvdash B, \Delta}{\Gamma, E \nvdash A \supset B, \Delta}\ \textit{a fortiori}^{\diamond}$$

$$\frac{A_1, \Gamma, E \nvdash B_1, \Delta \quad \ldots \quad A_n, \Gamma, E \nvdash B_n, \Delta}{\Gamma, E \nvdash A_1 \supset B_1, \ldots, A_n \supset B_n, \Delta}\ R\supset^{\star}$$

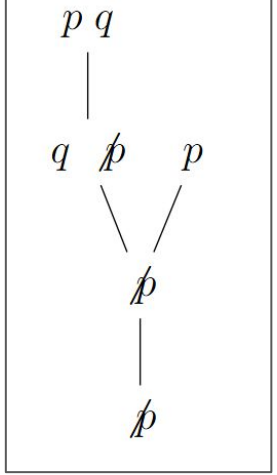
where
E contains blocked implications, $\boldsymbol{E}$ makes them usable again.
$\star$ Γ and Δ consist of atoms and are disjoint.
$\diamond$ $R\supset$ rule has already been applied to $A \supset B$.

RIG captures the unprovability for IG, allowing to extract a counter-model from the "anti-proof"

$$\cfrac{\cfrac{\cfrac{\cfrac{}{p \nvdash}\ \mathrm{Ax}}{p \nvdash \bot}\ R\bot}{\nvdash p, \neg p}\ R\supset}{\nvdash p \vee \neg p}\ R\vee$$

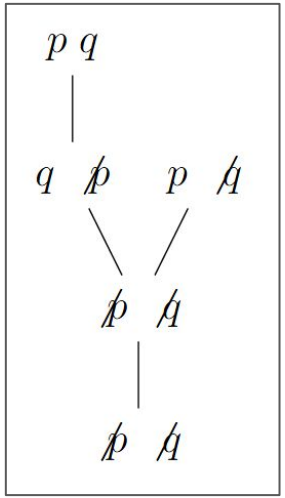
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p,q,(\neg p \supset \neg q)^* \nvdash}\,\text{AX}}{p,q,(\neg p \supset \neg q)^* \nvdash \bot,\bot}\,\bot R,\bot R}{q,p,(\neg p \supset \neg q)^* \nvdash p \supset \bot,\bot}\,AF\supset}{\neg p \supset \neg q, q, p \nvdash \bot}\,L_1\supset}{q,(\neg p \supset \neg q)^* \nvdash p,\neg p}\,R\supset}{\neg p \supset \neg q, q \nvdash p} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{p,(\neg p \supset \neg q)^* \nvdash}\,\text{AX}}{p,(\neg p \supset \neg q)^* \nvdash \bot,\bot}\,\bot R,\bot R}{p,(\neg p \supset \neg q)^* \nvdash p \supset \bot,\bot}\,AF\supset}{\neg p \supset \neg q, p \nvdash \bot}\,L_1\supset$$

$$\dfrac{\dfrac{(\neg p \supset \neg q)^* \nvdash q \supset p,\neg p}{\neg p \supset \neg q \nvdash q \supset p}\,L_1\supset}{\nvdash ((\neg p \supset \neg q) \supset (q \supset p))}\,R\supset$$



$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p,q,(\neg p \supset \neg q)^* \nvdash}\,\text{AX}}{p,q,(\neg p \supset \neg q)^* \nvdash \bot}\,\bot R,\bot R}{q,p,(\neg p \supset \neg q)^* \nvdash p \supset \bot,\bot}\,AF\supset}{\neg p \supset \neg q, q, p \nvdash \bot}\,L_1\supset}{q,(\neg p \supset \neg q)^* \nvdash p,\neg p}\,R\supset}{\neg p \supset \neg q, q \nvdash p} \qquad \dfrac{\dfrac{\dfrac{}{p,\neg q^* \nvdash q}\,\text{AX}}{p,\neg q^* \nvdash \bot,q}\,\bot R}{q \supset \bot, p \nvdash \bot}\,L_1\supset}{\neg p \supset \neg q, p \nvdash \bot}\,L_2\supset$$

$$\dfrac{\dfrac{(\neg p \supset \neg q)^* \nvdash q \supset p,\neg p}{\neg p \supset \neg q \nvdash q \supset p}\,L_1\supset}{\nvdash ((\neg p \supset \neg q) \supset (q \supset p))}\,R\supset$$



Soundness and Completeness

Output: proof OR refutation

✔ Soundness: if the algorithm returns a proof, the sequent is valid

✔ Completeness: if a refutation is found and the counter-model extracted, then the sequent is not true in the given model

Conclusion

- Formally verified
- terminating proof search algorithm with
  a. derivation and
  b. refutation construction
- for intuitionistic propositional logic
- in Lean proof assistant

Thank you!