Proof search and counter-model construction for bi-intuitionistic propositional logic

Luís Pinto[1]
Univ. Minho
Braga, Portugal

Theory Seminar at Inst. of Cybernetics
Tallinn, Estonia

9 April 2010

---

[1] Joint work with Tarmo Uustalu

Generalities on sequent calculus

- Formalism whose assertions are sequents $\Gamma \vdash \Delta$ (Γ, Δ "composed" of formulas $A, B, \ldots$).
- Typical interpretation of $\Gamma \vdash \Delta$: the formula $\bigwedge \Gamma \supset \bigvee \Delta$ is valid.
- Each connective has rules for introducing it at the right or at the left of $\vdash$, *e.g.* (in classical logic):

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

- Axioms and cut:

$$\frac{}{\Gamma, A \vdash A, \Delta}\ id \qquad \frac{\Gamma \vdash \Delta, A \quad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\ cut$$

- Structural rules:

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ \textit{weak-L} \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \textit{contract-L}$$

Generalities on sequent calculus (cont.)

- Derivation of a sequent $\Gamma \vdash \Delta$:
  - a tree of sequents whose root is $\Gamma \vdash \Delta$, built up using the available axioms and rules.
- Cut-elimination:
  - a sequent calculus has *the cut-elimination property* if any derivable sequent can be derived without using the cut-rule;
  - typical consequences: *subformula property*, *consistency*.
- Basis of a proof-search method:
  - decompose sequents successively (applying rules bottom-up), until all sequents become axioms or else some sequent cannot be further decomposed neither it is an axiom.
  - Usual problems: which rule to apply when there are alternatives; non-termination.

Bi-intuitionistic logic

- Extends intuitionistic logic with a connective "$-$" dual to implication, called subtraction (or co-implication, exclusion ...)
  - $A - B$ roughly means: A and not B
- Proposed by Cecilia Rauszer in the 70's:
  - semantics via Kripke structures and Heyting-Brouwer algebras;
  - formal systems *à la* Hilbert and sequent calculus.
- Recent interest for its proof theory motivated by *proof-search*, but also from the computational interpretations viewpoint (Curry-Howard).

Propositional bi-intuitionistic logic (**BiInt**)

- Formulas: $A, B := p \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \supset B \mid A - B$
- Two defined negations: $\neg A := A \supset \bot$ (strong negation)
  $\backsim A := \top - A$ (weak negation)
- Some properties:
  - conservatively extends propositional intuitionistic logic;
  - $A \wedge \backsim A$ is not contradictory (just as $A \vee \neg A$ is not intuitionistically válid), $A \vee \backsim A$ is valid (just as $A \wedge \neg A$ is intuitionistically contradictory).
  - strict implications:

$$\neg \backsim A \supset \backsim\backsim A \supset A \supset \neg\neg A \supset \backsim \neg A$$

Kripke sematics for **BiInt**

Def.: $K = (W, \leq, I)$ is a *Kripke structure* if:

- $(W, \leq)$ is a non-empty poset ($\leq$ called *accessibility relation*)
- I is monotone map associating a set of prop. vars. to each element (*world*) of W ($\forall w' \geq w, I(w) \subseteq I(w')$).

Def.: $\models_K$, the *validity* relation (between worlds and formulas) is s.t.:

- $w \models_K p$ iff $p \in I(w)$; $w \not\models_K \bot$; $w \models_K \top$;
- $w \models_K A \wedge B$ iff $w \models_K A$ and $w \models_K B$;
- $w \models_K A \vee B$ iff $w \models_K A$ or $w \models_K B$;
- $w \models_K A \supset B$ iff for all $w' \geq w$, $w' \models_K A$ implies $w' \models_K B$;
- $w \models_K A - B$ iff there exists $w' \leq w$ s.t. $w' \models_K A$ and $w' \not\models_K B$.

Def.: A formula A is *Kripke valid* if $w \models_K A$ for all K, w.

Heyting-Brouwer semantics for **BiInt**

Def.: $H = (X, \wedge, \vee, \supset, -, \bot, \top)$ is a *Heyting-Brouwer algebra* if:

- $(X, \wedge, \vee)$ is a lattice with smallest elem. $\bot$ and largest elem. $\top$;
- $\supset$ and $-$ are binary operations on X (*relative pseudo-complement* and *pseudo-difference* resp.) s.t.:
  - $a \supset b$ is the largest $x \in X$ s.t. $a \wedge x \leq b$.
  - $b - a$ is the smallest $x \in X$ s.t. $a \vee x \geq b$.

Def.: Let $H = (X, \wedge, \vee, \supset, -, \bot, \top)$ be an Heyting-Brouwer algebra.

- v map from prop. var. to X is *H-valuation*, when: $v(\bot) = \bot$, $v(\top) = \top$ and $v(A \Box B) = v(A) \Box v(B)$, for all $\Box \in \{\wedge, \vee, \supset, -\}$.

Def.: A formula A is *Heyting-Brouwer valid* if $v(A) =_H \top$ for all H,v.

Sequent calculus for **BiInt**

- *Sequents*: pairs $\Gamma \vdash \Delta$ of multisets of formulas
  (in Rauszer: Γ and Δ cannot simultaneously have more than one formula)
- Rules:

axioms and cuts:

$$\frac{}{\Gamma, A \vdash A, \Delta}\ id \qquad\qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\ cut$$

logical rules:

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

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot L \qquad\qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \bot, \Delta}\ \bot R$$

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

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

Sequent calculus for **BiInt** (cont.)

Logical rules for $\supset$ and $-$:

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

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

Thm. (Soundness and Completeness): $\vdash A$ is derivable iff A is Kripke valid (iff A is Heyting-Brouwer valid).

Impossibility of cut-elimination

- Without the cut rule we cannot derive $p \vdash q, r \supset ((p - q) \wedge r)$:

$$\dfrac{\overset{?}{p, r \vdash (p - q) \wedge r}}{p \vdash q, r \supset ((p - q) \wedge r)}\ \supset R$$

(the premiss is already invalid).

- With the cut rule:

$$\dfrac{\dfrac{\dfrac{}{p \vdash q, p, \ldots}\ id \qquad \dfrac{}{p, q \vdash q, p - q, \ldots}\ id}{p \vdash q, \boxed{p - q}, \ldots}\ -R \qquad \dfrac{\dfrac{\dfrac{}{p, p - q, r \vdash p - q}\ id \qquad \dfrac{}{p, p - q, r \vdash r}\ id}{p, p - q, r \vdash (p - q) \wedge r}\ \wedge R}{p, \boxed{p - q} \vdash q, r \supset ((p - q) \wedge r)}\ \supset R}{p \vdash q, r \supset ((p - q) \wedge r)}\ cut$$

$\mathbf{L}$: a labelled sequent calculus

- Inspired in a method of Sara Negri to devise cut-free labelled sequent calculi for modal logics.
- *Labels*: $x, y, z, \ldots$ (see as: worlds of Kripke structures).
- *Labelled formulas*: pairs $x : A$ (see as: A valid in x).
- *Sequents*: triples $\Gamma \vdash_G \Delta$, where
  - Γ, Δ finite multisets of labelled formulas;
  - G (a graph) finite binary relation on labels (see as: accessibility relation).

$\boxed{\text{Rules of } \mathbf{L}}$

pre-order rules:

$$\frac{\Gamma \vdash_{G \cup \{(x,x)\}} \Delta}{\Gamma \vdash_G \Delta}\ \mathit{refl} \qquad \frac{xGy \quad yGz \quad \Gamma \vdash_{G \cup \{(x,z)\}} \Delta}{\Gamma \vdash_G \Delta}\ \mathit{trans}$$

axiom:

$$\frac{}{\Gamma, x : A \vdash_G x : A, \Delta}\ \mathit{id}$$

monotonicity rules:

$$\frac{xGy \quad \Gamma, x : A, y : A \vdash_G \Delta}{\Gamma, x : A \vdash_G \Delta}\ \mathit{monL} \qquad \frac{yGx \quad \Gamma \vdash_G y : A, x : A, \Delta}{\Gamma \vdash_G x : A, \Delta}\ \mathit{monR}$$

Logical rules of **L** for $\supset$ and $-$

$$\frac{\Gamma \vdash_G y : B, \Delta \quad \Gamma, y : A \vdash_G \Delta}{\Gamma, x : B \supset A \vdash_G \Delta} \supset L \qquad xGy$$

$$\frac{\Gamma, y : B \vdash_{G \cup \{(x,y)\}} y : A, \Delta}{\Gamma \vdash_G x : B \supset A, \Delta} \supset R \qquad y \notin G, \Gamma, \Delta$$

$$\frac{\Gamma, y : A \vdash_{G \cup \{(y,x)\}} y : B, \Delta}{\Gamma, x : A - B \vdash_G \Delta} -L \qquad y \notin G, \Gamma, \Delta$$

$$\frac{\Gamma \vdash_G y : A, \Delta \quad \Gamma, y : B \vdash_G \Delta}{\Gamma \vdash_G x : A - B, \Delta} -R \qquad yGx$$

The counter-example to cut-elimination done in **L**

$$
\dfrac{
  \dfrac{
    \dfrac{}{x : p \vdash_{(x,y)} \boxed{x : p}}\ id
    \qquad
    \dfrac{}{\boxed{x : q} \vdash_{(x,y)} x : q}\ id
  }{
    x : p, y : r \vdash_{(x,y)} x : q, \boxed{y : p - q}
  }\ -R
  \qquad
  \dfrac{}{y : r \vdash_{(x,y)} y : r}\ id
}{
  \dfrac{x : p, y : r \vdash_{(x,y)} x : q, y : (p - q) \wedge r}{x : p \vdash_{\emptyset} x : q, x : r \supset ((p - q) \wedge r)}\ \supset R
}\ \wedge R
$$

Note the propagation of information from y to x at the $-R$ inference.

Soundness of **L**

Def.: A *counter-model* of $\Gamma \vdash_G \Delta$ is a pair (K, v), where $K = (W, \leq, I)$ is a Kripke structure and v a map from the set of labels to W, s.t.:

1. for all xGy, $v(x) \leq v(y)$;
2. for all $x : A \in \Gamma$, $v(x) \models A$;
3. for all $x : A \in \Delta$, $v(x) \not\models A$.

Def.: A sequent is *valid* if it has no counter-models.

Thm.: The sequents derivable in **L** are valid.

$\mathbf{L}^*$: an algorithmic variant of $\mathbf{L}$

- There are no explicit pre-order or monotonicity rules.
- Uses a *marking mechanism* to guarantee monotonicity and loop-detection.
- Sequents are triples $\Gamma \vdash_G \Delta$, but labelled formulas in Γ, Δ, can have additionally one of marks:

$$x : A^* \text{ or } x : A^\bullet.$$

Rules of $\mathbf{L}^*$

atomic rules:

$$\frac{\Gamma, x : p^\bullet, p^+, x : p^* \vdash_G \Delta}{\Gamma, x : p \vdash_G \Delta}\ \mathit{atomL} \qquad \frac{\Gamma \vdash_G x : p^\bullet, p^-, x : p^*, \Delta}{\Gamma \vdash_G x : p, \Delta}\ \mathit{atomR}$$

where $p^+ = \{y : p \mid xGy\}$ where $p^- = \{y : p \mid yGx\}$

axiom:

$$\overline{\Gamma, x : p^\bullet \vdash_G x : p^\bullet, \Delta}\ \mathit{id}$$

logical rules:

$$\frac{\Gamma \vdash_G \Delta}{\Gamma, x : \top \vdash_G \Delta}\ \top L \qquad \overline{\Gamma \vdash_G x : \top, \Delta}\ \top R$$

$$\overline{\Gamma, x : \bot \vdash_G \Delta}\ \bot L \qquad \frac{\Gamma \vdash_G \Delta}{\Gamma \vdash_G x : \bot, \Delta}\ \bot R$$

$$\frac{\Gamma, x : A, x : B \vdash_G \Delta}{\Gamma, x : A \wedge B \vdash_G \Delta}\ \wedge L \qquad \frac{\Gamma \vdash_G x : A, \Delta \quad \Gamma \vdash_G x : B, \Delta}{\Gamma \vdash_G x : A \wedge B, \Delta}\ \wedge R$$

$$\frac{\Gamma, x : A \vdash_G \Delta \quad \Gamma, x : B \vdash_G \Delta}{\Gamma, x : A \vee B \vdash_G \Delta}\ \vee L \qquad \frac{\Gamma \vdash_G x : A, x : B, \Delta}{\Gamma \vdash_G x : A \vee B, \Delta}\ \vee R$$

Rules of $\mathbf{L}^*$ for $\supset$ and $-$

$$\frac{\Gamma, (B \supset A)^+, x : (B \supset A)^* \vdash_G x : B, \Delta \quad \Gamma, x : A \vdash_G \Delta}{\Gamma, x : B \supset A \vdash_G \Delta} \supset L$$

$$(B \supset A)^+ = \{y : B \supset A \mid xGy\}$$

$$\frac{x : (B \supset A)^\bullet \notin \Delta \quad y \notin G, \Gamma, \Delta, \quad \Gamma, \Gamma^{y/x}, y : B \vdash_{G \cup \{(x,y)\}} y : A, x : (B \supset A)^\bullet, \Delta}{\Gamma \vdash_G x : B \supset A, \Delta} \supset R$$

$$\Gamma^{y/x} = \{y : C \mid x : C^* \in \Gamma\} \cup \{y : C^\bullet \mid x : C^\bullet \in \Gamma\} \cup \{y : (C - D)^\bullet \mid x : C - D \in \Gamma\}$$

$$\frac{x : (A - B)^\bullet \notin \Gamma \quad y \notin G, \Gamma, \Delta \quad \Gamma, x : (A - B)^\bullet, y : A \vdash_{G \cup \{(y,x)\}} y : B, \Delta^{y/x}, \Delta}{\Gamma, x : A - B \vdash_G \Delta} -L$$

$$\Delta^{y/x} = \{y : C \mid x : C^* \in \Delta\} \cup \{y : C^\bullet \mid x : C^\bullet \in \Delta\} \cup \{y : (D \supset C)^\bullet \mid x : D \supset C \in \Delta\}$$

$$\frac{\Gamma \vdash_G x : A, \Delta \quad \Gamma, x : B \vdash_G x : (A - B)^*, (A - B)^-, \Delta}{\Gamma \vdash_G x : A - B, \Delta} -R$$

$$(A - B)^- = \{y : A - B \mid yGx\}$$

Search procedure for $\mathbf{L}^*$

1. Given an $\mathbf{L}^*$-sequent, while possible, apply rules that do not create new labels (*saturation*).
2. For the top sequent of each of the resulting branches:
   - 2.1 check if it is an axiom and, if so, stop with *success* the branch;
   - 2.2 check for loops and proceed according to the respective *loop rule*;
   - 2.3 otherwise, apply $\supset R$ or $-L$ and restart at 1, or, if not possible, stop the whole search with *failure*.

$\boxed{\text{Loop-detection}}$

At a top sequent resulting from saturation of the premiss of $\supset R$:

$$\dfrac{y \notin G \quad \begin{array}{c} \Gamma \vdash_{G \cup \{(x,y)\}} \Delta \\ \vdots \\ \Gamma_0, \Gamma_0^{y/x}, y : A \vdash_{G \cup \{(x,y)\}} y : B, x : (A \supset B)^{\bullet}, \Delta_0 \end{array}}{\Gamma_0 \vdash_G x : A \supset B, \Delta_0} \supset R$$

check if the loop rule *loopUp* applies:

$$\dfrac{y \notin G \quad \Gamma \setminus y \vdash_G \Delta[x/y]}{\Gamma \vdash_{G \cup \{(x,y)\}} \Delta} \; \mathit{loopUp}, \qquad \mathit{if}: \; \begin{array}{l} \Gamma[y] \subseteq \Gamma[x] \cup \Gamma^{\bullet}[x], \\ \Gamma^{*}[y] \subseteq \Gamma^{*}[x], \end{array}$$

$$\mathit{with}: \;\; \Gamma[y] = \{A | y : A \in \Gamma\}, \Gamma^{*}[y] = \{A | y : A^{*} \in \Gamma\}, \mathit{etc}.$$

Soundness of the search procedure

- The procedure builds partial derivations in $\mathbf{L}^*$ augmented of the loop rules.

Prop.: If the search procedure, applied to an $\mathbf{L}$-sequent, stops with success in all branches, the sequent is derivable in $\mathbf{L}$.

Termination of the search procedure

Thm.: The procedure applied to $\mathbf{L}^*$-sequents whose graph is acyclic terminates.

Proof ideas:

- An infinite branch corresponds to infinitely many uses of $\supset R / - L$.
- It is impossible to have an infinite branch corresponding to an infinite ascending chain:

$$\begin{tikzcd} & & x_2 \arrow[ur, dotted, no head] & \\ & x_1 \arrow[ur] & & \\ x_0 \arrow[ur] & & & \end{tikzcd}$$

- It is impossible to have an infinite branch corresponding to an infinite zigzag, as *e.g.*:

$$\begin{tikzcd} & x_1 \arrow[dr] & & & & x_5 \arrow[dr, dotted, no head] & \\ x_0 \arrow[ur] & & x_2 \arrow[dr] & & x_4 \arrow[ur] & & \\ & & & x_3 \arrow[ur] & & & \end{tikzcd}$$

Counter-model construction and completeness

Thm. Let $\mathcal{B}$ be a failed branch of a proof attempt, let $\Gamma \vdash_G \Delta$ be the top sequent of $\mathcal{B}$ and let

1. $K = (W, \leq, I)$, with W the set of labels in the sequent, $\leq = G^*$ and $I(x) = \{p \mid x : p^\bullet \in \Gamma\}$ (which is a Kripke structure);
2. v=identity on labels.

Then, (K, v) is a counter-model of $\mathcal{B}$'s end sequent.

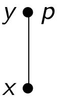
Corol.: Let $\Gamma \vdash_G \Delta$ be an **L**-sequent whose graph is acyclic. The following are equivalent:

i) $\Gamma \vdash_G \Delta$ is valid;

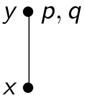
ii) the search procedure applied to $\Gamma \vdash_G \Delta$ terminates with success;

iii) $\Gamma \vdash_G \Delta$ is derivable in **L**.

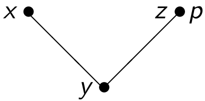
Some counter-models



$$\neg(p \wedge \backsim p)$$
$$\backsim p \supset \neg p$$
$$p \supset \backsim\backsim p$$



$$(p \wedge \backsim q) \supset (p - q)$$



$$\backsim\neg p \supset \neg\neg p$$

Related and future work

Related work:

Goré, Postniece e Tiu proposed also decision procedures for **BiInt**, based on extended sequent calculi (combination of derivations and refutations; nested sequents; display calculi).

Future work:

- Map **L**-derivations into label-free sequent calculus (and check for completeness of analytic cuts).
- *Contraction-free* sequent calculus for **BiInt** (avoiding loop-detection).