A Forward Unprovability Calculus for Intuitionistic Propositional Logic

Camillo Fiorentini[1], Mauro Ferrari[2]

[1]DI, Univ. degli Studi di Milano, Milano, Italy

[2]DiSTA, Univ. degli Studi dell'Insubria, Varese, Italy

TABLEAUX 2017

Brasilia, September 27th, 2017

The Inverse Method

- The *inverse method*, introduced in the 1960s by Maslov, is a saturation based theorem proving technique closely related to (hyper)resolution
- It relies on a *forward* proof-search strategy and can be applied to cut-free calculi enjoying the subformula property.
- Some references:

  - S. Ju. Maslov. An invertible sequential version of the constructive predicate calculus. Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), 1967.

  - A. Degtyarev and A. Voronkov. *The inverse method*. Handbook of Automated Reasoning, 2001.

The Iron Curtain of Automated Reasoning

A large part of the work on automated reasoning done in the Soviet Union in the sixties and seventies was based on the inverse method proposed by Sergey Maslov in 1964.

The role of the inverse method in the Soviet work on proof procedures for predicate logic can be compared to the role of resolution method in theorem proving projects in the West.

For a number of reasons, this work has not been duly appreciated outside a small circle of Maslov's associates.

V. Lifschitz. *What is the inverse method?*. JAR, 1989

The Universal Recipe of Inverse Method

A. Degtyarev and A. Voronkov. *The inverse method*.
Handbook of Automated Reasoning, 2001.

- Goal

  Prove a formula G *(goal formula)*.

- Calculus

  Design a specialized calculus $\mathbf{C}_G$ satisfying the *Finite Rule Property* :

  - √ $\mathbf{C}_G$ has a finite number of axioms (= rules with no premises)
  - √ Given a finite number of sequents, there is only a finite number of rules of $\mathbf{C}_G$ applicable to them.

- Forward proof-search

  Forward apply the rules of $\mathbf{C}_G$ starting from axioms until possible (saturation process).

The Universal Recipe of Inverse Method

A naive proof-search strategy for $\mathbf{C}_G$ can be implemented as follows.

We keep a *database* DB of proved sequents.

- Start

  Add to DB all the axioms of $\mathbf{C}_G$.

- Main Loop

  If DB contains sequents $\sigma_1, \ldots, \sigma_n$ and

  $$\frac{\sigma_1 \quad \cdots \quad \sigma_n}{\sigma}$$

  is (an instance of) a rule of $\mathbf{C}_G$, then add σ to DB.

- Stop

  The goal is proved or no new sequent can be added to DB.

By properties of $\mathbf{C}_G$, the procedure always terminates

Cooking it ...

- Classical and Intuitionistic Logic [Handbook AR, 2001]
- Logic of Bunched Implication [Donelly et al., LPAR 2004]
- Many-valued logics [Voronkov et al., MICAI 2013]
- A significant investigation about Intuitionistic Logic is presented in

  K. Chaudhuri and F. Pfenning. A focusing inverse method theorem prover for first-order linear logic. CADE 2005

  K. Chaudhuri, F. Pfenning, and G. Price. A logical characterization of forward and backward chaining in the inverse method. IJCAR 2006.

  Here focused calculi and polarization of formulas are exploited to reduce the search spaces in forward proof-search.

  These techniques are at the heart of the design of the prover Imogen

  S. McLaughlin and F. Pfenning. Imogen: Focusing the polarized inverse method for intuitionistic propositional logic. LPAR 2008.

Our contribution

In all the mentioned papers, the inverse method has been exploited to prove the *validity* of a goal formula in a specific logic.

Here we follow the dual approach:

- we design a forward calculus to derive the unprovability of a goal formula in Intuitionistic Propositional Logic (**IPL**)

This different perspectives requires a deep adjustment of the method itself.

Notation

- $\mathcal{V}$ is a set of propositional variables p, q, p_1, p_2, ...
- The language $\mathcal{L}$ based on $\mathcal{V}$ is the set of formulas A, B, ... such that:

$$\begin{array}{lll} A, B & ::= & \bot \mid p \mid A \wedge B \mid A \vee B \mid A \supset B \qquad p \in \mathcal{V} \\ \neg A & ::= & A \supset \bot \end{array}$$

- A Kripke model is a structure $\mathcal{K} = \langle P, \leq, \rho, V \rangle$, where:
  - $\langle P, \leq \rangle$ is a finite poset with minimum ρ (root)
  - $V : P \to 2^{\mathcal{V}}$ is a function such that $\alpha \leq \beta$ implies $V(\alpha) \subseteq V(\beta)$
  - $\Vdash \ \subseteq \ P \times \mathcal{L}$ is the forcing relation:
    - $\alpha \nVdash \bot$
    - $\alpha \Vdash p$ iff $p \in V(\alpha)$
    - $\alpha \Vdash A \wedge B$ iff $\alpha \Vdash A$ and $\alpha \Vdash B$
    - $\alpha \Vdash A \vee B$ iff $\alpha \Vdash A$ or $\alpha \Vdash B$
    - $\alpha \Vdash A \supset B$ iff, for every $\beta \in P$ s.t. $\alpha \leq \beta$, $\beta \nVdash A$ or $\beta \Vdash B$

- Sequents

$$\Gamma \Rightarrow A$$

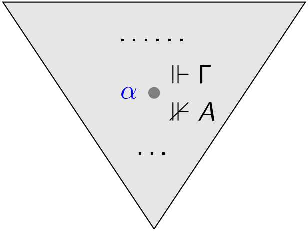
Formulas in $\Gamma \Rightarrow A$ are suitable subformulas of the goal formula G.

Understood meaning

A is not provable (in **IPL**) from the set of formulas Γ

Semantic viewpoint

In some world α of a Kripke model:



All the formulas in Γ are forced in α

A is not forced in α

Towards a Forward Unprovability Calculus for G

- Axioms

$$\Gamma^{\mathrm{At}} \Rightarrow F \qquad F\text{: a prop. variable or } \bot$$

Γ^{At} is a "maximal" subset of $\mathcal{V}$ such that $F \notin \Gamma^{\mathrm{At}}$.

Example

$$G \;=\; (\neg a \supset b \vee c) \;\supset\; (\neg a \supset b) \vee (\neg a \supset c)$$

$$\begin{array}{lc}
(\mathrm{Ax1}) & a, b \Rightarrow c \\
(\mathrm{Ax2}) & a, c \Rightarrow b \\
(\mathrm{Ax3}) & b, c \Rightarrow a \\
(\mathrm{Ax4}) & a, b, c \Rightarrow \bot
\end{array}$$

- In standard forward calculi for **IPL** axioms have a simpler form:

$$p \vdash p \qquad p \in \mathcal{V}$$

With the above goal formula G:

$$a \vdash a \qquad b \vdash b \qquad c \vdash c$$

Towards a Forward Unprovability Calculus for G

- Rules must preserve *unprovability* (in **IPL**)

  Examples of sound rules:

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \wedge B}\, R\wedge$$

If A is not provable from Γ, then $A \wedge B$ is not provable from Γ

$$\frac{A, \Gamma \Rightarrow C}{A \vee B, \Gamma \Rightarrow C}\, L\vee$$

If C is not provable from $\{A\} \cup \Gamma$, then C is not provable from $\{A \vee B\} \cup \Gamma$ (Inversion Principle for left $\vee$)

Towards a Forward Unprovability Calculus for G

Tricky task

How to cope with rules having more than one premise?

- Standard forward calculi

  Since rules have to preserve provability, left formulas must be gathered.

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma \cup \Delta \vdash A \wedge B}\ R\wedge$$

If A is provable from Γ and
B is provable from Δ, then
$A \wedge B$ is provable from $\Gamma \cup \Delta$

- Unprovability forward calculus

  Since rules have to preserve unprovability, left formulas must be intersected.

  Apparently, the rule $R\vee$ should be:

$$\frac{\Gamma \Rightarrow A \qquad \Delta \Rightarrow B}{\Gamma \cap \Delta \Rightarrow A \vee B}\ R\vee$$

If A is not provable from Γ and
B is not provable from Δ, then
$A \vee B$ is not provable from $\Gamma \cap \Delta$

Towards a Forward Unprovability Calculus for G

The alleged rule for right or is unsound!

Trivial counterexample

$$\dfrac{\overbrace{p \vee q}^{\Gamma} \Rightarrow p \qquad \overbrace{p \vee q}^{\Delta} \Rightarrow q}{\underbrace{p \vee q}_{\Gamma \cap \Delta} \Rightarrow p \vee q}\; R\vee$$

- Premises
  p is not provable from $p \vee q$
  q is not provable from $p \vee q$
- Conclusion
  $p \vee q$ is provable from $p \vee q$

Thus, the rule does not preserve unprovability.

The problem is that intersection is too big, we need more clever strategy to join sequents.

This leads to the Forward Refutation calculus **FRJ**(G).

The calculus $\mathbf{FRJ}(G)$

We introduce the standard classification of left/right (alias T/F, negative/positive) subformulas of the goal formula G.

$\mathrm{SL}(G)$ (left subf.) and $\mathrm{SR}(G)$ (right subf.) are the smallest subsets of subformulas of G such that:

- The goal formula is right ($G \in \mathrm{SR}(G)$)
- $\wedge$ and $\vee$ keep the sign

$\mathrm{SL}(G)$	$\mathrm{SL}(G)$
$A \wedge B$	$A,\ B$
$A \vee B$	$A,\ B$

$\mathrm{SR}(G)$	$\mathrm{SR}(G)$
$A \wedge B$	$A,\ B$
$A \vee B$	$A,\ B$

- $\supset$ preserves the consequent and swaps the antecedent

$\mathrm{SL}(G)$	$\mathrm{SL}(G)$	$\mathrm{SR}(G)$
$A \supset B$	B	A

$\mathrm{SR}(G)$	$\mathrm{SR}(G)$	$\mathrm{SL}(G)$
$A \supset B$	B	A

The calculus $\mathbf{FRJ}(G)$

$$\mathcal{L}^{\mathcal{V},\supset} \quad ::= \quad \underset{\text{prop. vars.}}{\mathcal{V}} \quad \underset{+}{\cup} \quad \underset{\supset\text{-formulas}}{\{\, A \supset B \mid A \supset B \in \mathcal{L} \,\}}$$

We use two kinds of sequents:

- Regular sequents

$$\Gamma \Rightarrow C$$

$$\Gamma \subseteq \mathrm{SL}(G) \cap \mathcal{L}^{\mathcal{V},\supset} \qquad C \in \mathrm{SR}(G)$$

* Formulas in Γ are left subformulas of G and C is a right subformula of G
* Formulas in Γ are propositional variables or implications

The calculus **FRJ**(G)

$$\mathcal{L}^{\mathcal{V},\supset} \ ::= \ \mathcal{V} \cup \{ \, A \supset B \mid A \supset B \in \mathcal{L} \, \}$$

- Irregular sequents

$$\Sigma \, ; \, \Theta \to C$$

$$\Sigma \cup \Theta \ \subseteq \ \mathrm{SL}(G) \cap \mathcal{L}^{\mathcal{V},\supset} \qquad C \in \mathrm{SR}(G)$$

  - ∗ Left formulas are partitioned into the sets Σ and Θ
  - ∗ Left formulas are left subformulas of G and C is a right subformula of G
  - ∗ Formulas in the left are propositional variables or implications

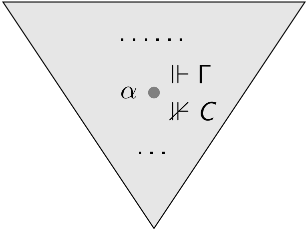
Irregular sequents are needed to properly formalize multi-premises rules:

> *the Σ-sets of the premises (the stable parts) must be preserved in the conclusion, whereas formulas in Θ might be lost.*

FRJ(G) satisfies the following soundness property:

- Regular sequents

  If $\Gamma \Rightarrow C$ is provable in **FRJ**(G), then there exists a world α of a model such that $\alpha \Vdash \Gamma$ and $\alpha \nVdash C$.



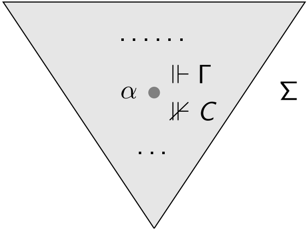
Accordingly, C is not provable from Γ in **IPL**.

The calculus $\mathbf{FRJ}(G)$

For irregular sequents, the property is a bit more intricate:

- Irregular sequents

  If $\sigma = \Sigma\,;\,\Theta \to C$ is provable in $\mathbf{FRJ}(G)$ and
  σ can be used to prove a regular sequent in $\mathbf{FRJ}(G)$, then
  there exist a world α of a model $\mathcal{K}$ and a set Γ such that
  $\Sigma \subseteq \Gamma \subseteq \Sigma \cup \Theta$ and $\alpha \Vdash \Gamma$ and $\alpha \nVdash C$.



$$\Sigma \subseteq \Gamma \subseteq \Sigma \cup \Theta$$

Thus, C is not provable from Γ in **IPL**.

The calculus $\mathbf{FRJ}(G)$

G is *provable* in $\mathbf{FRJ}(G)$ iff there exists an $\mathbf{FRJ}(G)$-derivation $\mathcal{D}$ of a regular sequent σ having G in the right, namely:

$$\underbrace{\begin{array}{c}\mathcal{D}\\ \Gamma \Rightarrow G\end{array}}_{\sigma}$$

Theorem (Completeness of $\mathbf{FRJ}(G)$)

G is provable in $\mathbf{FRJ}(G)$ iff G is not valid in **IPL**

Note the use of *subsumption*, which is typical in forward reasoning.
Actually, $\mathcal{D}$ shows that the formula $(\wedge\Gamma) \supset G$ is not valid in **IPL**, that is:

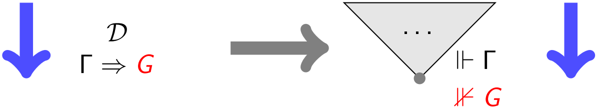
G is not provable in **IPL** *even if we assume* Γ.

This is a stronger statement than the plain unprovability of G.

From a derivation of G we can extract a countermodel for G, namely, a model where in some world G is not forced.

More precisely:

- If G is not provable in $\mathbf{FRJ}(G)$, there exists an $\mathbf{FRJ}(G)$-derivation $\mathcal{D}$ of $\Gamma \Rightarrow G$
- From $\mathcal{D}$ we can immediately extract a Kripke model such that, at its root, all the formulas in Γ are forced and G is not forced



We remark that both the derivation and the countermodel are built top-down (forward style):

- $\mathcal{D}$ is built top-down, starting from axioms.
- This corresponds to a top-down construction strategy of the countermodel for G starting from the top-worlds.

The calculus **FRJ**(G)

- Regular axioms

  Left: a maximal set of propositional variables

  Right: a propositional variable p or $\bot$

$$\frac{}{\overline{\Gamma}^{\mathrm{At}} \Rightarrow \bot}\ \mathrm{Ax}_{\Rightarrow} \qquad \frac{}{\overline{\Gamma}^{\mathrm{At}} \setminus \{p\} \Rightarrow p}\ \mathrm{Ax}_{\Rightarrow} \qquad \overline{\Gamma}^{\mathrm{At}} = \mathrm{SL}(G) \cap \mathcal{V}$$

- Irregular axioms

  Left: a maximal set of propositional variables and $\supset$-formulas; the Σ-zone is empty

  Right: a propositional variable p or $\bot$

$$\frac{}{\cdot\,;\,\overline{\Gamma} \rightarrow \bot}\ \mathrm{Ax}_{\rightarrow} \qquad \frac{}{\cdot\,;\,\overline{\Gamma} \setminus \{p\} \rightarrow p}\ \mathrm{Ax}_{\rightarrow} \qquad \overline{\Gamma} = \mathrm{SL}(G) \cap \mathcal{L}^{\mathcal{V},\supset}$$

The calculus $\mathbf{FRJ}(G)$

There are no left rules, but only rules to introduce the connectives $\wedge$, $\vee$, $\supset$ in the right and the rules $\bowtie^{\mathrm{At}}$ and $\bowtie^{\vee}$ to join sequents.

- Rules for $\wedge$

$$\frac{\Gamma \Rightarrow A_k}{\Gamma \Rightarrow A_1 \wedge A_2}\,\wedge \qquad\qquad \frac{\Sigma\,;\,\Theta \rightarrow A_k}{\Sigma\,;\,\Theta \rightarrow A_1 \wedge A_2}\,\wedge \quad k \in \{1,2\}$$

- Rules for $\supset$

  In standard refutation calculi, the rule for right implication has the form

$$\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \supset B}\,R\supset \quad A \in \Gamma$$

If B is not provable from Γ and $A \in \Gamma$, then $A \supset B$ is not provable from Γ

The antecedent A of the $\supset$-formula in the conclusion must be in the left.

But, due to the lack of left rules, using this rule alone the calculus would be incomplete.

$$\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \supset B}\ R\supset \qquad A \in \Gamma$$

With this rule alone we cannot prove the non-valid goal

$$G \;=\; (p_1 \wedge p_2) \supset q$$

Indeed, the antecedent $p_1 \wedge p_2$ cannot occur in the left of sequents.

We can only build derivations like these:

$$\dfrac{\dfrac{\overline{p_1, p_2 \Rightarrow q}\ \mathrm{Ax}_{\Rightarrow}}{p_1, p_2 \Rightarrow p_1 \supset q}\ R\supset}{p_1, p_2 \Rightarrow p_2 \supset (p_1 \supset q)}\ R\supset \qquad \dfrac{\dfrac{\overline{p_1, p_2 \Rightarrow q}\ \mathrm{Ax}_{\Rightarrow}}{p_1, p_2 \Rightarrow p_2 \supset q}\ R\supset}{p_1, p_2 \Rightarrow p_1 \supset (p_2 \supset q)}\ R\supset$$

To compensate for this, we have to relax the side condition.

The calculus $\mathbf{FRJ}(G)$

- Rule $\supset_\in$ (regular sequents)

$$\dfrac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \supset B}\ \supset_\in \qquad \cancel{A \in \Gamma} \quad A \in \mathcal{C}l(\Gamma)$$

$\mathcal{C}l(\Gamma)$ (the closure of Γ) is the smallest extension of Γ containing the formulas X of the kind:

$$X \ ::= \ C \mid X \wedge X \mid A \vee X \mid X \vee A \mid A \supset X \qquad C \in \Gamma,\ A \text{ any formula}$$

Now we can prove $G = (p_1 \wedge p_2) \supset q$ as follows:

$$\dfrac{\dfrac{}{p_1, p_2 \Rightarrow q}\ \mathrm{Ax}_\Rightarrow}{p_1, p_2 \Rightarrow p_1 \wedge p_2 \supset q}\ \supset_\in \qquad p_1 \wedge p_2 \in \mathcal{C}l(\{p_1, p_2\})$$

The calculus $\mathbf{FRJ}(G)$

- Rule $\supset_\in$ (irregular sequents)

  Similar idea, but this time we shift to the left of semicolon the set Λ needed to satisfy the side condition.

$$\frac{\Sigma\,;\,\Theta, \Lambda \to B}{\Sigma, \Lambda\,;\,\Theta \to A \supset B} \supset_\in \quad A \in \mathcal{C}l(\Sigma \cup \Lambda)$$

Note that $\supset_\in$ in general admits many applications to the same sequent since we can choose Λ in different ways.

To reduce the size of the DB of proved sequents, we can choose a *minimal* set Λ satisfying the side condition, namely:

$$\Lambda' \subsetneq \Lambda \quad \text{implies} \quad A \notin \mathcal{C}l(\,\Sigma \cup \Lambda'\,)$$

The calculus $\mathbf{FRJ}(G)$

- Rule $\supset_{\notin}$

  The premise is a regular sequent and the conclusion an irregular one.

$$\frac{\Gamma \Rightarrow B}{\cdot\,;\, \Theta \rightarrow A \supset B}\supset_{\notin} \qquad \begin{aligned} \overline{\Gamma} &= \mathrm{SL}(G) \cap \mathcal{L}^{\mathcal{V},\supset} \\ \Theta &\subseteq \mathcal{C}l(\Gamma) \cap \overline{\Gamma} \\ A &\in \mathcal{C}l(\Gamma) \setminus \mathcal{C}l(\Theta) \end{aligned}$$

  This is the only rule which, applied to a regular sequent, yields an irregular one.

To reduce the size of the DB of proved sequents, we can assume that Θ is a *maximal* set satisfying the side condition, namely:

$$\Theta \subsetneq \Theta' \subseteq \mathcal{C}l(\Gamma) \cap \overline{\Gamma} \quad \text{implies} \quad A \in \mathcal{C}l(\Theta')$$

The calculus **FRJ**(G)

- Rule $\vee$

  This rule has two irregular sequents σ_1 and σ_2 as premises and yields an irregular sequent σ introducing an $\vee$-formula in the right.

  Σ-sets are preserved, Θ-sets are intersected.

$$\frac{\sigma_1 \ = \ \Sigma_1 \,;\, \Theta_1 \rightarrow C_1 \qquad \sigma_2 \ = \ \Sigma_2 \,;\, \Theta_2 \rightarrow C_2}{\sigma \ = \ \Sigma_1, \Sigma_2 \,;\, \Theta_1 \cap \Theta_2 \rightarrow C_1 \vee C_2} \vee \qquad \begin{array}{l} \Sigma_1 \ \subseteq \ \Sigma_2 \cup \Theta_2 \\ \Sigma_2 \ \subseteq \ \Sigma_1 \cup \Theta_1 \end{array}$$

  Side conditions are needed to guarantee that:

$$\mathrm{Left}(\sigma) \ \subseteq \ \mathrm{Left}(\sigma_1) \cap \mathrm{Left}(\sigma_2)$$

  namely

$$\Sigma_1 \cup \Sigma_2 \cup (\Theta_1 \cap \Theta_2) \ \subseteq \ (\Sigma_1 \cup \Theta_1) \ \cap \ (\Sigma_2 \cup \Theta_2)$$

The calculus FRJ(G)

- Join rules

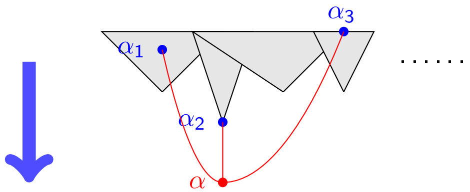
  Join rules are multi-premises rules which allow to introduce on the right an atomic formula (rule $\bowtie^{\mathrm{At}}$) or a disjunction (rule $\bowtie^{\vee}$).

  Premises of join rules are irregular sequents, the conclusion a regular sequent (only rules which perform such a transition).

  They have a similar structure and require some side conditions.

Join rules correspond to a step in *downward* countermodel construction:

⋆ we select $n \geq 1$ worlds $\alpha_1, \ldots, \alpha_n$ and we add a new world α having as immediate successors the chosen worlds.



α: new world having has immediate successors the chosen worlds α_1, α_2, α_3

- The Join rule $\bowtie^{\mathrm{At}}$

  It introduces a formula $F \in \mathcal{V} \cup \{\bot\}$ in the right.
  As in rule $\vee$, Σ-sets are gathered and Θ-sets intersected.

$$\sigma_j \;=\; \underbrace{\Sigma_j^{\mathrm{At}}, \Sigma_j^{\supset}}_{\Sigma_j} \,;\, \underbrace{\Theta_j^{\mathrm{At}}, \Theta_j^{\supset}}_{\Theta_j} \to A_j \qquad \text{where } \Sigma_j^{\mathrm{At}} \cup \Theta_j^{\mathrm{At}} \subseteq \mathcal{V} \text{ and } \Sigma_j^{\supset} \cup \Theta_j^{\supset} \subseteq \mathcal{L}^{\supset}$$

$$\frac{\sigma_1 \qquad \cdots \qquad \sigma_n}{\Sigma^{\mathrm{At}},\, \Theta^{\mathrm{At}} \setminus \{F\},\, \Sigma^{\supset},\, \Theta^{\supset} \Rightarrow F} \bowtie^{\mathrm{At}} \qquad \begin{array}{l} \Sigma_i \subseteq \Sigma_j \cup \Theta_j, \text{ for every } i \neq j \\ X \supset Y \in \Sigma^{\supset} \text{ implies } X \in \{A_1, \ldots, A_n\} \\ F \notin \Sigma^{\mathrm{At}} \end{array}$$

$$\begin{array}{lcl} \Sigma^{\mathrm{At}} & = & \bigcup_{1 \le j \le n} \Sigma_j^{\mathrm{At}} \\ \Theta^{\mathrm{At}} & = & \bigcap_{1 \le j \le n} \Theta_j^{\mathrm{At}} \\ \Sigma^{\supset} & = & \bigcup_{1 \le j \le n} \Sigma_j^{\supset} \\ \Theta^{\supset} & = & \{\, X \supset Y \;\in\; \bigcap_{1 \le j \le n} \Theta_j^{\supset} \mid X \in \{A_1, \ldots, A_n\} \,\} \end{array}$$

The calculus $\mathbf{FRJ}(G)$

- The Join rule $\bowtie^{\vee}$

  It introduces a formula $C_1 \vee C_2$ in the right.
  As in rule $\vee$, Σ-sets are gathered and Θ-sets intersected.

$$\sigma_j \;=\; \underbrace{\Sigma_j^{\mathrm{At}}, \Sigma_j^{\supset}}_{\Sigma_j}\,;\,\underbrace{\Theta_j^{\mathrm{At}}, \Theta_j^{\supset}}_{\Theta_j} \to A_j \qquad \text{where } \Sigma_j^{\mathrm{At}} \cup \Theta_j^{\mathrm{At}} \subseteq \mathcal{V} \text{ and } \Sigma_j^{\supset} \cup \Theta_j^{\supset} \subseteq \mathcal{L}^{\supset}$$

$$\frac{\sigma_1 \qquad \cdots \qquad \sigma_n}{\Sigma^{\mathrm{At}},\, \Theta^{\mathrm{At}},\, \Sigma^{\supset},\, \Theta^{\supset} \Rightarrow C_1 \vee C_2}\,\bowtie^{\vee} \qquad \begin{array}{l} \Sigma_i \subseteq \Sigma_j \cup \Theta_j, \text{ for every } i \neq j \\ X \supset Y \in \Sigma^{\supset} \text{ implies } X \in \{A_1, \dots, A_n\} \\ \{C_1,\, C_2\} \;\subseteq\; \{A_1, \dots, A_n\} \end{array}$$

$$\begin{array}{lcl} \Sigma^{\mathrm{At}} & = & \bigcup_{1 \leq j \leq n} \; \Sigma_j^{\mathrm{At}} \\ \Theta^{\mathrm{At}} & = & \bigcap_{1 \leq j \leq n} \; \Theta_j^{\mathrm{At}} \\ \Sigma^{\supset} & = & \bigcup_{1 \leq j \leq n} \; \Sigma_j^{\supset} \\ \Theta^{\supset} & = & \{\; X \supset Y \;\in\; \bigcap_{1 \leq j \leq n} \; \Theta_j^{\supset} \mid X \in \{A_1, \dots, A_n\} \;\} \end{array}$$

The calculus $\mathbf{FRJ}(G)$

The calculus $\mathbf{FRJ}(G)$ is terminating.

Indeed, we can define a weight function wg on sequents such that for every rule

$$\frac{\sigma_1 \quad \cdots \quad \sigma_n}{\sigma}$$

it holds that

$$0 \leq \mathrm{wg}(\sigma) < \mathrm{wg}(\sigma_i) \qquad i = 1 \cdots n$$

By definition of wg the following properties easily follow.

- Let $\mathcal{D}$ be an $\mathbf{FRJ}(G)$-derivation and N the size of G ($=$ number of symbols occurring in G). Then:
  - (i) $\mathrm{height}(\mathcal{D}) \;=\; O(\,N^2\,)$
  - (ii) $\mathrm{height}(\,\mathrm{Model}(\mathcal{D})\,) \;\leq\; N$

Proof-search

The naive proof-search procedure is not efficient:

- To apply join rules, we have to consider every combination of $n \geq 1$ irregular sequents and check the side conditions on them
- Too many redundant sequents are generated

In forward calculi, redundancies are reduced by exploiting a *subsumption* relation between sequents:

⋆ If σ_1 and σ_2 are in $\mathtt{DB}$ and σ_1 subsumes σ_2, then σ_2 is redundant and can be thrown out.

Proof-search

In $\mathbf{FRJ}(G)$ we can introduce the following subsumption relation:

- $\Gamma, \Gamma' \Rightarrow C$ subsumes $\Gamma \Rightarrow C$

  same right formula, larger Γ*-set*

- $\Sigma\,;\,\Theta, \Theta' \rightarrow C$ subsumes $\Sigma\,;\,\Theta \rightarrow C$

  same Σ*-set and right formula, larger* Θ*-set*

In the Main Loop of proof-search, we perform the usual forward and backward subsumption tests.

Let σ be the new sequent obtained by applying a rule of the calculus:

- Forward subsumption

  If σ is subsumed by a sequent in `DB`, then σ is discarded, otherwise σ is added to `DB`

- Backward subsumption

  We delete from `DB` all the sequents σ' which are subsumed by σ and all the sequents which have been derived using σ'.

Countermodels

There is a close correspondence between an **FRJ**(G)-derivation $\mathcal{D}$ of G and the countermodel $\mathcal{K} = \langle P, \leq, \rho, V \rangle$ for G extracted from $\mathcal{D}$.

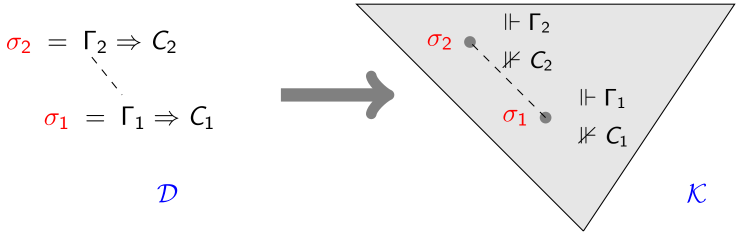
- Worlds

$$P \;=\; \{\; \sigma \in \mathcal{D} \mid \sigma \text{ is a reg. axiom or } \sigma \text{ is the conclusion of a Join rule } \}$$

- Ordering relation

  $\sigma_1 \leq \sigma_2$ in $\mathcal{K}$ iff σ_1 is below σ_2 in the derivation $\mathcal{D}$
- Valuation

$$V(\sigma) \;=\; \{\; p \in \mathcal{V} \mid\; p \text{ belongs to in the left of } \sigma \,\}$$



Countermodels

Our proof/countermodel-search procedure is dual to the standard bottom-up methods, which mimic the backward application of rules.

This different approach has a significant impact on the outcome:

- Backward procedures

  Countermodels are always trees, which might contain many redundancies (the same sequent might occur many times in the tree)

- Forward procedures

  Prone to re-use sequents as much as possible and to not generate redundant ones (the `DB` does not contain duplications)
  Thus the obtained countermodels are in general very concise.

We have implemented `frj`, a Java prototype of our proof-search procedure based on JTabWb (a Java framework for developing provers)

`http://github.com/ferram/jtabwb_provers/`

Example: Anti-Scott principle

$$G \;=\; (\,((\neg\neg p \supset p) \supset (\neg p \vee p)) \supset (\neg\neg p \vee \neg p)\,) \;\;\supset\;\; ((\neg\neg p \supset p) \vee \neg\neg p)$$

$$G \;=\; S \supset ((\neg\neg p \supset p) \vee \neg\neg p)$$

$$S \;=\; H \supset (\neg\neg p \vee \neg p) \qquad H \;=\; (\neg\neg p \supset p) \supset (\neg p \vee p)$$

The goal G is an instance of Anti-Scott principle (not valid in **IPL**).

To prove the goal, `frj` runs 10 iterations of the main loop.

Legenda

sub(n):	sequent subsumed by sequent n (backward subsumption)
(n):	sequent needed to prove the goal
(n):	sequent corresponding to a world of the countermodel

- Iteration 0 (axioms)

sub(15)	$\cancel{(0)}$	$\mathrm{Ax}_{\Rightarrow}$	$\cancel{p \Rightarrow \bot}$
sub(10)	$\cancel{(1)}$	$\mathrm{Ax}_{\Rightarrow}$	$\cancel{\cdot \Rightarrow p}$
	(2)	$\mathrm{Ax}_{\rightarrow}$	$\cdot\,;\ p, \neg p, \neg\neg p, \neg\neg p \supset p, S \rightarrow \bot$
	(3)	$\mathrm{Ax}_{\rightarrow}$	$\cdot\,;\ \neg p, \neg\neg p, \neg\neg p \supset p, S \rightarrow p$

Example: Anti-Scott principle

- Iteration 1

$sub(19)$	$\cancel{(4)}$	$\supset_{\in}$ (0)	$\cancel{p \Rightarrow \neg p}$
$sub(20)$	$\cancel{(5)}$	$\supset_{\notin}$ (0)	$\cancel{\cdot\,;\ \neg\neg p \supset p \to \neg p}$
	(6)	$\supset_{\in}$ (2)	$p\,;\ \neg p, \neg\neg p, \neg\neg p \supset p, S \to \neg p$
	(7)	$\supset_{\in}$ (2)	$\neg p\,;\ p, \neg\neg p, \neg\neg p \supset p, S \to \neg\neg p$
	(8)	$\supset_{\in}$ (3)	$\neg\neg p\,;\ \neg p, \neg\neg p \supset p, S \to \neg\neg p \supset p$
$sub(17)$	$\cancel{(9)}$	$\bowtie^{\mathrm{At}}$ (3)	$\cancel{\neg p \Rightarrow \bot}$
$sub(18)$	$\cancel{(10)}$	$\bowtie^{\mathrm{At}}$ (3)	$\cancel{\neg p \Rightarrow p}$

- Iteration 2

$sub(24)$	$\cancel{(11)}$	$\vee(5)(3)$	$\cancel{\cdot\,;\ \neg\neg p \supset p \to \neg p \vee p}$
	(12)	$\vee(8)(7)$	$\neg p, \neg\neg p\,;\ \neg\neg p \supset p, S \to (\neg\neg p \supset p) \vee \neg\neg p$
$sub(21)$	$\cancel{(13)}$	$\supset_{\in}$ (9)	$\cancel{\neg p \Rightarrow \neg\neg p}$
$sub(22)$	$\cancel{(14)}$	$\supset_{\notin}$ (9)	$\cancel{\cdot\,;\ S \to \neg\neg p}$
	(15)	$\bowtie^{\mathrm{At}}$ (6)	$p, \neg\neg p \Rightarrow \bot$
$sub(26)$	$\cancel{(16)}$	$\bowtie^{\vee}$ (3)(5)	$\cancel{\cdot \Rightarrow \neg p \vee p}$
	(17)	$\bowtie^{\mathrm{At}}$ (3)(7)	$\neg p, \neg\neg p \supset p \Rightarrow \bot$
	(18)	$\bowtie^{\mathrm{At}}$ (3)(7)	$\neg p, \neg\neg p \supset p \Rightarrow p$

Example: Anti-Scott principle

- Iteration 3

	(19)	$\supset_{\in}$ (15)	$p, \neg\neg p \Rightarrow \neg p$
	(20)	$\supset_{\notin}$ (15)	$\cdot\,;\, \neg\neg p, \neg\neg p \supset p, S \rightarrow \neg p$
	(21)	$\supset_{\in}$ (17)	$\neg p, \neg\neg p \supset p \Rightarrow \neg\neg p$
	(22)	$\supset_{\notin}$ (17)	$\cdot\,;\, \neg\neg p \supset p, S \rightarrow \neg\neg p$
sub(32)	~~(23)~~	$\supset_{\in}$ (11)	$\cancel{\neg\neg p \supset p\,;\, \cdot \rightarrow H}$

- Iteration 4

	(24)	$\vee$(20)(3)	$\cdot\,;\, \neg\neg p, \neg\neg p \supset p, S \rightarrow \neg p \vee p$
	(25)	$\bowtie^{\mathrm{At}}$ (20)	$\neg\neg p \Rightarrow p$
	(26)	$\bowtie^{\vee}$ (3)(20)	$\neg\neg p \Rightarrow \neg p \vee p$
sub(37)	~~(27)~~	$\bowtie^{\vee}$ (3)(20)(22)	$\cancel{\neg\neg p \supset p \Rightarrow \neg p \vee p}$

- Iteration 5

	(28)	$\supset_{\in}$ (25)	$\neg\neg p \Rightarrow \neg\neg p \supset p$
	(29)	$\supset_{\notin}$ (25)	$\cdot\,;\, S \rightarrow \neg\neg p \supset p$
sub(38)	~~(30)~~	$\supset_{\in}$ (27)	$\cancel{\neg\neg p \supset p \Rightarrow H}$
sub(39)	~~(31)~~	$\supset_{\notin}$ (27)	$\cancel{\cdot\,;\, \cdot \rightarrow H}$
	(32)	$\supset_{\in}$ (24)	$\neg\neg p \supset p\,;\, \neg\neg p, S \rightarrow H$

Example: Anti-Scott principle

- Iteration 6

	(33)	$\vee(29)(22)$	$\cdot\,;\, S \to (\neg\neg p \supset p) \vee \neg\neg p$
$sub(40)$	$\cancel{(34)}$	$\bowtie^{\vee}$ (22)(29)	$\cancel{\cdot \Rightarrow (\neg\neg p \supset p) \vee \neg\neg p}$
	(35)	$\bowtie^{\mathrm{At}}$ (22)(32)	$\neg\neg p \supset p, S \Rightarrow \bot$
	(36)	$\bowtie^{\mathrm{At}}$ (22)(32)	$\neg\neg p \supset p, S \Rightarrow p$
	(37)	$\bowtie^{\vee}$ (3)(20)(22)(32)	$\neg\neg p \supset p, S \Rightarrow \neg p \vee p$

- Iteration 7

(38)	$\supset_{\in}$ (37)	$\neg\neg p \supset p, S \Rightarrow H$
(39)	$\supset_{\not\in}$ (37)	$\cdot\,;\, S \to H$

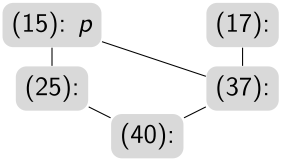
- Iteration 8

(40)	$\bowtie^{\vee}$ (22)(29)(39)	$S \Rightarrow (\neg\neg p \supset p) \vee \neg\neg p$

- Iteration 9 (Goal)

(41)	$\supset_{\in}$ (40)	$S \Rightarrow G$
(42)	$\supset_{\not\in}$ (40)	$\cdot\,;\,\cdot \to G$

Example: Anti-Scott principle

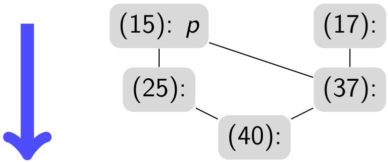


$$
\begin{array}{llll}
(15) & p, \neg\neg p \Rightarrow \bot & (17) & \neg p, \neg\neg p \supset p \Rightarrow \bot \\
(25) & \neg\neg p \Rightarrow p & (37) & \neg\neg p \supset p \Rightarrow \neg p \vee p \\
(40) & S \Rightarrow (\neg\neg p \supset p) \vee \neg\neg p & &
\end{array}
$$

$$G = S \supset ((\neg\neg p \supset p) \vee \neg\neg p) \quad S = H \supset (\neg\neg p \vee \neg p) \quad H = (\neg\neg p \supset p) \supset (\neg p \vee p)$$

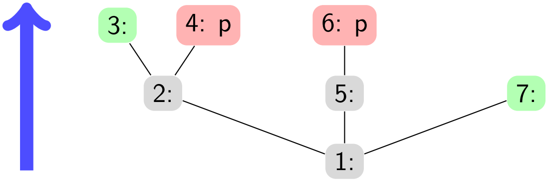
- At the end of the computation DB contains 38 sequents:
  - √ 15 sequents have been deleted by backward subsumption
  - √ 16 sequents are needed to prove the goal
- We have an application of the join rule $\bowtie^{\mathrm{At}}$ with 4 premises.

Example: Anti-Scott principle



The obtained model is minimal in the number of worlds and is *not a tree*, hence it cannot be obtained by standard bottom-up methods.

For instance, using `lsj`, a prover based on the calculus presented in [Ferrari et. al., JAR 2013] we get the following tree-shaped countermodel, which has *minimal height*, but contains some redundancies.



6 is a replica of 4

7 is a replica of 3

Example: Nishimura formulas

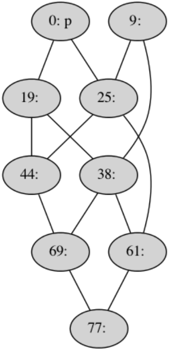
We get very concise models with one-variable Nishimura formulas:

$$\begin{aligned} N_1 &= p & \qquad N_{2n+3} &= N_{2n+1} \vee N_{2n+2} \\ N_2 &= \neg p & \qquad N_{2n+4} &= N_{2n+3} \supset N_{2n+1} \end{aligned}$$

N_9 : equivalent to Anti-Scott principle

Indeed, `frj` yields the standard "tower-like" minimum countermodels.

Countermodel for N_{17}

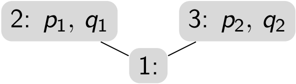


On countermodels

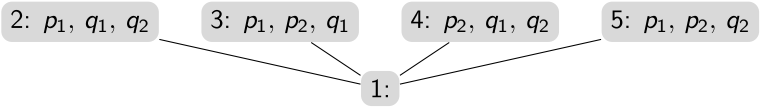
- We can tweak the proof-search strategy so to get countermodels having minimal height
- However, the countermodels might not be minimal. For instance:

$$G \;=\; (p_1 \supset p_2) \vee (p_2 \supset p_1) \vee (q_1 \supset q_2) \vee (q_2 \supset q_1)$$

Minimal Countermodel:



Countermodel $\mathcal{K}$ generated by `frj`:



  - $\mathcal{K}$ has the same height of the minimal countermodel
  - Final worlds of $\mathcal{K}$ have "maximal" forcing (only one prop. var. is not forced), thus we cannot simulate the minimal countermodel

Whenever proof-search in **FRJ**(G) fails, we get a *saturated database* DB for G, namely:

- If a sequent σ is provable in **FRJ**(G), there exists σ' in DB such that σ' subsumes σ

From a saturated database for G, we can immediately extract a derivation of G in **Gbu**(G), a sequent calculus for **IPL**.

- **Gbu**(G) can be viewed as a “focused” variant of the well-known sequent calculus **G3i**, and it is closely related with the calculus presented in

  M. Ferrari, C. Fiorentini, and G. Fiorino. A terminating evaluation-driven variant of G3i. TABLEAUX 2013

Accordingly, a saturated database for G can be understood as a *proof-certificate* of the validity of G in **IPL**.

On saturated database

A dual remark has been issued in

> *S. McLaughlin and F. Pfenning. Imogen: Focusing the polarized inverse method for intuitionistic propositional logic. LPAR 2008.*

The authors introduce a forward (focused) sequent calculus for **IPL**.

If proof-search for a goal G fails, one gets a saturated database $\mathtt{DB}$ for G.

The authors claim that a saturated $\mathtt{DB}$

> *"may be considered a kind of countermodel for the goal sequent".*

But so far no method has been proposed to extract a countermodel from such a saturated $\mathtt{DB}$.

Conclusion

- We have introduced **FRJ**(G), a forward calculus to derive the unprovability of a goal formula G in **IPL** and we have designed and implemented a proof-search procedure:
  - If G is provable in **FRJ**(G), from the derivation we can immediately extract a countermodel for G;
  - otherwise, we get a saturated `DB` which can be exploited to get a sequent-style derivation of G in **IPL**.
    Thus a saturated `DB` can be viewed as a proof-certificate of the validity of G in **IPL**.
- Advantages of forward vs. backward reasoning:
  - derivations are more concise since sequents are reused and not duplicated (forward/backward subsumption tests),
  - countermodels are in general compact and have minimal height
- Future work
  - √ Improve the efficiency of the prover.
  - √ Investigate the applicability of the method to other logics.