A forward unprovability calculus for Intuitionistic Propositional Logic

Camillo Fiorentini

DI, Univ. degli Studi di Milano, Milano, Italy

Torino, October 8th, 2018

Forward proof-search in refutation calculi

The inverse method has been extensively exploited to prove the *validity* of a goal formula in a specific logic.

Here we follow the dual approach:

We propose forward calculi $\mathbf{C}_G$ to derive the non-validity of a goal formula G in a logic L.

Thus, $\mathbf{C}_G$ is a forward refutation calculus for L.

- We focus on Intuitionistic Propositional Logic (IPL) and we present a forward refutation calculus $\mathbf{FRJ}(G)$ for IPL.

  C. Fiorentini and M. Ferrari. A Forward Unprovability Calculus for Intuitionistic Propositional Logic. TABLEAUX 2017, LNAI, vol. 10501, pp. 114-130, Springer, 2017.

  C. Fiorentini and M. Ferrari. Duality between unprovability and provability in forward proof-search for Intuitionistic Propositional Logic. arXiv:1804.06689, 2018.

Forward refutation in IPL

We present a forward calculus **FRJ**(G) to derive the non-validity of a goal formula G in IPL.

$$G \text{ is provable in } \mathbf{FRJ}(G) \iff G \notin \mathrm{IPL}$$

- If G is provable in **FRJ**(G):
  - √ from the derivation we extract a "small" Kripke countermodel for G, witnessing the non-validity of G in IPL.
- If G is not provable in **FRJ**(G):
  - √ we get a saturated database DB of sequents provable in **FRJ**(G);
  - √ by exploiting it, we build a derivation of G in a standard sequent calculus for IPL, witnessing the validity of G in IPL.

Notation

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

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

- 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 $\beta \Vdash B$

Towards a Forward Refutation Calculus for G

- Sequents have the form

$$\Gamma \Rightarrow A \qquad\qquad \Gamma \cup \{A\} \subseteq \mathrm{Sf}(G)$$

- Soundness

  If $\Gamma \Rightarrow A$ is provable in $\mathbf{FRJ}(G)$, then the sequent $\Gamma \Rightarrow \Delta$ is non-valid, namely:

  $\surd$ the formula $\bigwedge \Gamma \supset A$ is non-valid in IPL

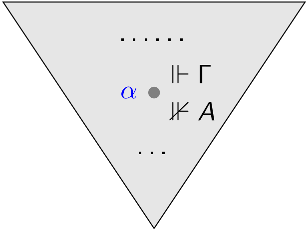
  This means that:

  $\surd$ the formula A is not provable from formulas Γ in IPL

Towards a Forward Refutation Calculus for G

- Soundness (semantic)

  √ if $\Gamma \Rightarrow A$ is provable in $\mathbf{FRJ}(G)$, there exists a world α of a Kripke model such that:



All the formulas in Γ are forced in α
A is not forced in α

- Completeness

  If G is non-valid in IPL, then a sequent of the form

$$\Gamma \Rightarrow G$$

is provable in $\mathbf{FRJ}(G)$. Note that the set Γ might be non-empty

Towards a Forward Refutation Calculus for G

- Axioms

  In standard forward calculi axioms have the form

$$p \vdash p \qquad\qquad p\text{: propositional variable}$$

  Since $\mathbf{FRJ}(G)$ is a refutation calculus, axioms are unprovable sequents (in IPL) only containing propositional variables and $\bot$:

$$p_1, \ldots, p_n \Rightarrow q \qquad q \neq p_1, \ \ldots\ , q \neq p_n$$

$$p_1, \ldots, p_n \Rightarrow \bot$$

  where $p_1, \ldots, p_n$, q are propositional variables.

Towards a Forward Refutation Calculus for G

Rules must preserve unprovability in IPL

- Rule for $R\wedge$ (right and)

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \wedge B}\ R\wedge \quad \downarrow$$

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

- Rule for $L\vee$ (left or)

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

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 Refutation Calculus for G

Tricky task

How to cope with rules having more than one premise?

- Standard forward rule for $R\wedge$

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

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

- Unprovability forward calculus

  Since rules must preserve unprovability in IPL, side formulas must be intersected.

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

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

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 Refutation 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 $\Gamma \cap \Delta$ is too big, we need a more clever strategy to join sequents.

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

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

- We introduce two kinds of sequent:
  - Regular sequents $\Gamma \Rightarrow C$
  - Irregular sequents $\Sigma\,;\,\Theta \rightarrow C$
- Formulas occurring in the sequents are subformulas of the goal formula G
- In the left, only atoms and implications.
- There are no left rules, but only rules to introduce the connectives $\wedge$, $\vee$, $\supset$ in the right and the multi-premise rules $\bowtie^{\mathrm{At}}$ and $\bowtie^{\vee}$ to join sequents.
- G is *provable* in $\mathbf{FRJ}(G)$ iff there exists an $\mathbf{FRJ}(G)$-derivation of a regular sequent of the form $\Gamma \Rightarrow G$.

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

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

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

- 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.

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

In the wrong $\vee$-rule:

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

Now:

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

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

- Join rules

  Join rules are multi-premise rules allowing the introduction on the right of an atomic formula (rule $\bowtie^{\mathrm{At}}$) or a disjunction (rule $\bowtie^{\vee}$).

- 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.

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

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

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

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

$$\frac{}{\bar{\Gamma}^{\mathrm{At}} \setminus \{F\} \Rightarrow F}\ \mathrm{Ax}{\Rightarrow} \qquad \frac{}{\cdot\, ;\, \bar{\Gamma}^{\mathrm{At}} \setminus \{F\}, \bar{\Gamma}^{\supset} \rightarrow F}\ \mathrm{Ax}{\rightarrow} \qquad F \in \mathcal{V} \cup \{\bot\}$$

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

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

$$\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \supset B}\ {\supset}{\in} \quad A \in \mathcal{C}l(\Gamma) \qquad \frac{\Sigma\, ;\, \Theta, \Lambda \rightarrow B}{\Sigma, \Lambda\, ;\, \Theta \rightarrow A \supset B}\ {\supset}{\in} \qquad \begin{array}{l} \Theta \cap \Lambda = \emptyset \\ A \in \mathcal{C}l(\Sigma \cup \Lambda) \end{array}$$

$$\frac{\Gamma \Rightarrow B}{\cdot\, ;\, \Theta \rightarrow A \supset B}\ {\supset}{\notin} \qquad \begin{array}{l} \Theta \subseteq \mathcal{C}l(\Gamma) \cap \bar{\Gamma} \\ A \in \mathcal{C}l(\Gamma) \setminus \mathcal{C}l(\Theta) \end{array}$$

Let, for $1 \leq j \leq n$, $\sigma_j = \underbrace{\Sigma_j^{\mathrm{At}}, \Sigma_j^{\supset}}_{\Sigma_j}\, ;\, \underbrace{\Theta_j^{\mathrm{At}}, \Theta_j^{\supset}}_{\Theta_j} \rightarrow A_j$ and $\Upsilon = \{A_1, \ldots, A_n\}$

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

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

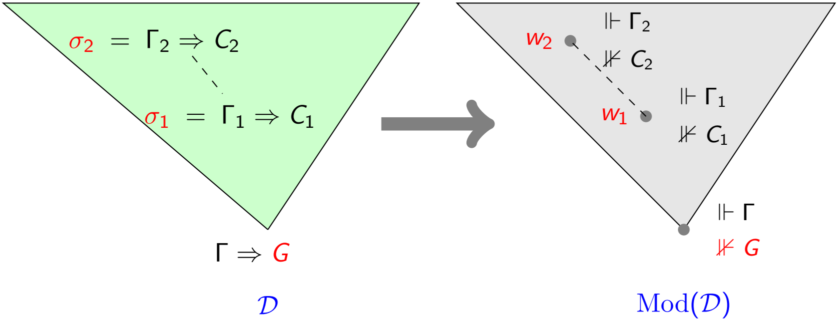
The calculus $\mathbf{FRJ}(G)$

Let G be provable in $\mathbf{FRJ}(G)$.

- There exists an $\mathbf{FRJ}(G)$-derivation $\mathcal{D}$ of $\Gamma \Rightarrow G$
- From $\mathcal{D}$ we extract a Kripke model $\mathrm{Mod}(\mathcal{D})$ closely related to $\mathcal{D}$.

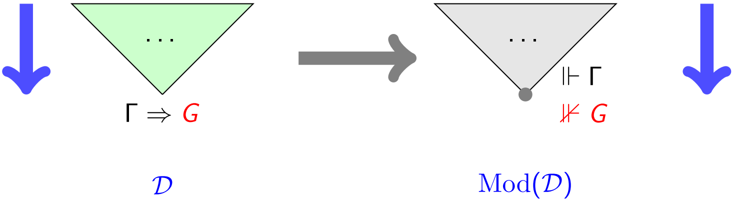
  At the root of $\mathrm{Mod}(\mathcal{D})$ all the formulas in Γ are forced, whereas G is not forced.

Accordingly, $\mathrm{Mod}(\mathcal{D})$ is a countermodel for G.



In forward-proof search, $\mathcal{D}$ is built top-down, starting from axioms.

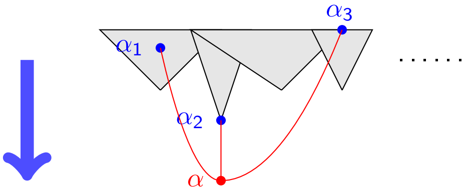
This corresponds to a top-down construction strategy of the countermodel $\mathrm{Mod}(\mathcal{D})$, starting from the top-worlds towards the root.



The calculus **FRJ**(G)

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.



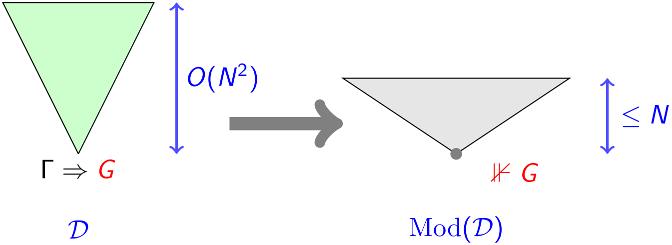
α: new world having the chosen worlds α_1, α_2, α_3 as immediate successors.

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

Let $\mathcal{D}$ be an $\mathbf{FRJ}(G)$-derivation of G and
N the size of G (= number of symbols occurring in G).

Then:

- $\text{height}(\mathcal{D}) = O(N^2)$
- $\text{height}(\text{Mod}(\mathcal{D})) \leq N$



Proof-search

The naive proof-search procedure is not efficient:

- Join rules must be applied to every combination of $n \geq 1$ sequents.
- Too many redundant sequents are generated.

To reduce redundancies:

- ⋆ We introduce a *subsumption* relation between sequents.
- ⋆ We tweak the proof-search procedure so that DB never contains pairs of sequents subsuming each other *(subsumption check)*.

  Indeed, if both σ_1 and σ_2 belong to DB and σ_1 subsumes σ_2, then σ_2 is redundant and can be safely removed.

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/`

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.

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)	~~(0)~~	$\mathrm{Ax}_{\Rightarrow}$	~~$p \Rightarrow \bot$~~
sub(10)	~~(1)~~	$\mathrm{Ax}_{\Rightarrow}$	~~$\cdot \Rightarrow p$~~
	(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

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

- Iteration 2

$sub(24)$	~~(11)~~	$\vee$(5)(3)	~~$\cdot\,;\ \neg\neg p \supset p \rightarrow \neg p \vee p$~~
	(12)	$\vee$(8)(7)	$\neg p, \neg\neg p\,;\ \neg\neg p \supset p, S \rightarrow (\neg\neg p \supset p) \vee \neg\neg p$
$sub(21)$	~~(13)~~	$\supset_{\in}$ (9)	~~$\neg p \Rightarrow \neg\neg p$~~
$sub(22)$	~~(14)~~	$\supset_{\notin}$ (9)	~~$\cdot\,;\ S \rightarrow \neg\neg p$~~
	(15)	$\bowtie^{\mathrm{At}}$ (6)	$p, \neg\neg p \Rightarrow \bot$
$sub(26)$	~~(16)~~	$\bowtie^{\vee}$ (3)(5)	~~$\cdot \Rightarrow \neg p \vee p$~~
	(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)	$\cdot\,; \neg\neg p, \neg\neg p \supset p, S \to \neg p$
	(21)	$\supset_{\in}$ (17)	$\neg p, \neg\neg p \supset p \Rightarrow \neg\neg p$
	(22)	$\supset_{\notin}$ (17)	$\cdot\,; \neg\neg p \supset p, S \to \neg\neg p$
sub(32)	~~(23)~~	$\supset_{\in}$ (11)	~~$\neg\neg p \supset p; \cdot \to H$~~

- Iteration 4

	(24)	$\vee$(20)(3)	$\cdot\,; \neg\neg p, \neg\neg p \supset p, S \to \neg p \vee p$
	(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)	~~$\neg\neg p \supset p \Rightarrow \neg p \vee p$~~

- Iteration 5

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

Example: Anti-Scott principle

- Iteration 6

	(33)	$\vee(29)(22)$	$\cdot\,;\, S \to (\neg\neg p \supset p) \vee \neg\neg p$
$sub(40)$	~~(34)~~	$\bowtie^{\vee}$ (22)(29)	~~$\cdot \Rightarrow (\neg\neg p \supset p) \vee \neg\neg p$~~
	(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)	$\supset_{\notin}$ (37)	$\cdot\,;\, S \to H$

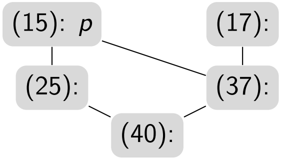
- Iteration 8

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

- Iteration 9 (Goal)

(41) $\supset_{\in}$ (40) $S \Rightarrow G$

Example: Anti-Scott principle

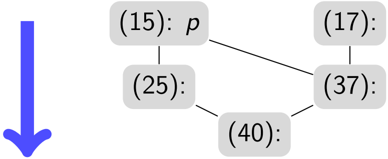


(15)	$p, \neg\neg p \Rightarrow \bot$	(17)	$\neg p, \neg\neg p \supset p \Rightarrow \bot$
(25)	$\neg\neg p \Rightarrow p$	(37)	$\neg\neg p \supset p \Rightarrow \neg p \vee p$
(40)	$S \Rightarrow (\neg\neg p \supset p) \vee \neg\neg p$		

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

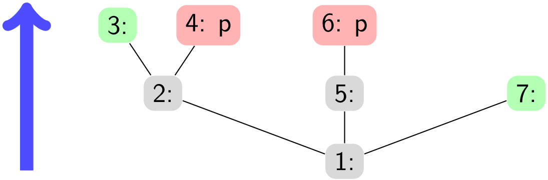
- At the end of the computation `DB` contains 38 sequents:
  - √ 15 sequents have been deleted by (backward) subsumption
  - √ 16 sequents are needed to prove the goal

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

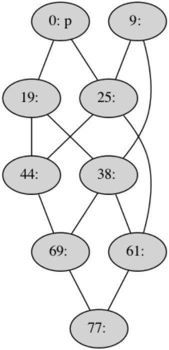
We get very concise models with one-variable Nishimura formulas:

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

N_9 : equivalent to Anti-Scott principle

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

Countermodel for N_{17}

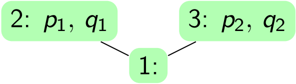


On countermodels

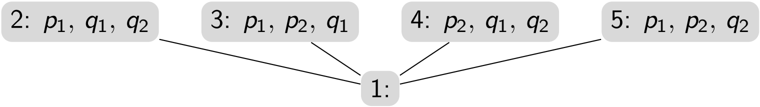
- We can tweak the proof-search strategy so to get countermodels having minimal height
- However, the countermodels might not be minimal. For instance:

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

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

On saturated database

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.

We exploit `DB` to build a sequent derivation of G, so to constructively ascertain the validity of G.

To this aim, we introduce the sequent calculus **Gbu**(G), a "focused" variant of the well-known sequent calculus **G3i**.

$\surd$ **Gbu**(G) can be viewed as the dual calculus of **FRJ**(G)

$\surd$ **Gbu**(G) is closely related with the calculus presented in

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

On saturated database

- **G3i**

$$\frac{}{\Gamma, p \vdash p}\,\mathrm{Ax}_1 \qquad \frac{}{\bot, \Gamma \vdash C}\,\mathrm{Ax}_2$$

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

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{A \vee B, \Gamma \vdash C}\,L\vee \qquad \frac{\Gamma \vdash A_k}{\Gamma \vdash A_1 \vee A_2}\,R\vee \qquad k = 0, 1$$

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

- **Gbu**(G) = **G3i** + labelled sequents (two kinds of sequents)
  + side conditions on some rule applications

On saturated database

- In **G3i**, bottom-up proof search is not terminating.
  Indeed, **G3i** allows for unbounded applications of rule $L\supset$ of this kind:

$$
\dfrac{\dfrac{\dfrac{\vdots}{A\supset B,\Gamma\vdash C} \qquad B,\Gamma\vdash C}{A\supset B,\Gamma\vdash C}\,L\supset \qquad B,\Gamma\vdash C}{A\supset B,\Gamma\vdash C}\,L\supset \qquad \uparrow
$$

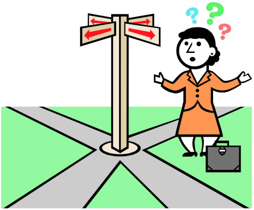
- In **Gbu**(G) the number of applications of rule $L\supset$ is bounded by the size of the root sequent.

  Hence, bottom-up proof-search in **Gbu**(G) is terminating

On saturated database

In **Gbu**(G) bottom-up proof-search in general requires backtracking:

$$\frac{\cdots}{A_1 \supset B_1\,,\,\ldots\,,\,A_n \supset B_n \vdash p}\ L\supset ??$$



- We have to choose the main formula $A_j \supset B_j$ of $L\supset$ application.
- If we take the wrong way, we have to backtrack and try another choice.

On saturated database

Example

$$\frac{\cdots}{p_1,\ p_1 \supset p_2,\ p_3 \supset p_4 \vdash p_2}\ L\supset ??$$

We can choose $p_1 \supset p_2$ or $p_3 \supset p_4$.

- If we choose $p_3 \supset p_4$, proof search fails since the left-most premise is not provable:

$$\frac{\overset{\text{UNPROVABLE}}{p_1,\ p_1 \supset p_2,\ p_3 \supset p_4 \vdash p_3} \qquad p_1,\ p_1 \supset p_2,\ p_4 \vdash p_2}{p_1,\ p_1 \supset p_2,\ p_3 \supset p_4 \vdash p_2}\ L\supset$$

- To build a derivation, we have to backtrack and try the other way

$$\frac{\dfrac{}{p_1,\ p_1 \supset p_2,\ p_3 \supset p_4 \vdash p_1}\ \mathrm{Ax} \qquad \dfrac{}{p_1,\ p_2,\ p_3 \supset p_4 \vdash p_2}\ \mathrm{Ax}}{p_1,\ p_1 \supset p_2,\ p_3 \supset p_4 \vdash p_2}\ L\supset$$

On saturated database

However, we can exploit the $\mathtt{DB}$ obtained at the end of proof-search to avoid backtracking and choose the right path.

To sum up:

- If G is valid in IPL, forward proof-search in $\mathbf{FRJ}(G)$ fails.
- At the end of proof-search we obtain a saturated database $\mathtt{DB}$.
- We can exploit $\mathtt{DB}$ to deterministically construct a sequent derivation of G in $\mathbf{Gbu}(G)$:

  whenever a backtrack point occurs, ask $\mathtt{DB}$ *the right way.*

Thus a saturated $\mathtt{DB}$ can be viewed as a proof-certificate of the validity of G.

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 $\mathtt{DB}$.

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

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

But so far this issue has not been investigated.

Conclusion

- **FRJ**(G) is a forward calculus to derive the unprovability of a goal formula G in IPL:
  - √ 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 (subsumption tests)
  - √ countermodels are in general compact and have minimal height