A Unified Procedure for Provability and Counter-Model Generation in Minimal Implicational Logic

Jefferson de Barros Santos¹,²
Departamento de Informática
PUC-Rio
Brazil

Bruno Lopes Vieira⁴
Instituto de Computação
UFF
Brazil

Edward Hermann Haeusler³
Departamento de Informática
PUC-Rio
Brazil

Abstract

This paper presents results on the definition of a sequent calculus for Minimal Implicational Propositional Logic (M→) aimed to be used for provability and counter-model generation in this logic. The system tracks the attempts to construct a proof in such a way that, if the original formula is a M→ tautology, the tree structure produced by the proving process is a proof, otherwise, it is used to construct a counter-model using Kripke semantics.

Keywords: theorem proving

1 Introduction

Proof search (validity) in Minimal Implicational Propositional Logic (M→) is a PSPACE-Complete problem as stated by Statman in [14] who also shows that

¹ The authors thank to CNPq and CAPES for supporting this research
² Email: jsantos@inf.puc-rio.br
³ Email: hermann@inf.puc-rio.br
⁴ Email: bruno@ic.uff.br

http://dx.doi.org/10.1016/j.entcs.2016.09.014
1571-0661 © 2016 The Author(s). Published by Elsevier B.V.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).
\(M \to\) polynomially simulates Intuitionistic Propositional Logic (IPL). This simulation can be used to polynomially simulate Classical Logic too, although Classical Logic seems to be in a smaller complexity class\(^5\). This result points out that \(M \to\) is as hard to implement as the most popular propositional logics. Haeusler shows in [7] that \(M \to\) can polynomially simulate not only Classical and Intuitionistic Propositional Logic but also Full Minimal Propositional Logic and any other decidable propositional logic with a Natural Deduction system with the sub-formula property. Because of those features, \(M \to\) can be used as a base tool to study complexity of many other logics.

Our goal here is to present a sequent calculus for \(M \to\) which allows the definition of a unified procedure for provability and counter-model generation in this logic. The calculus is based on a set of rules and in a general strategy for application of the rules in such a way that we can avoid the usage of loop checkers and the necessity of working with different systems for provability and refutation. To the best of our knowledge, this is the first proof calculus for \(M \to\) where validity and counter-model generation are done in a single procedure.

Counter-model generation (using Kripke semantics) is achieved as a consequence of the completeness of the system. We are also developing an interactive theorem prover for \(M \to\) based on the in here proposed calculus. Its source code can be found at https://github.com/jeffsantos/sequent-prover.

## 2 Minimal Implicational Logic

### 2.1 Semantics

The Minimal Implicational Logic (\(M \to\)) is the fragment of Minimal Logic containing only the logical constant \(\to\). Its semantics is the intuitionistic semantics restricted to \(\to\) only. Thus, given a propositional language \(\mathcal{L}\), a \(M \to\) model is a structure \(\langle U, \preceq, V \rangle\), where \(U\) is a non-empty set (worlds), \(\preceq\) is a partial order relation on \(U\) and \(V\) is a function from \(U\) into the power set of \(\mathcal{L}\), such that if \(i, j \in U\) and \(i \preceq j\) then \(V(i) \subseteq V(j)\). Given a model, the satisfaction relationship \(\models\) between worlds in models and formulae is defined as in Intuitionistic Logic, namely:

- \(\langle U, \preceq, V \rangle \models p, p \in \mathcal{L}\), iff, \(p \in V(i)\)
- \(\langle U, \preceq, V \rangle \models \alpha_1 \to \alpha_2\), iff, for every \(j \in U\), such that \(i \preceq j\), if \(\langle U, \preceq, V \rangle \models_j \alpha_1\) then \(\langle U, \preceq, V \rangle \models_j \alpha_2\).

As usual a formula \(\alpha\) is valid in a model \(M\), namely \(M \models \alpha\), if and only if, it is satisfiable in every world \(i\) of the model, namely \(\forall i \in U, M \models_i \alpha\). A formula is a \(M \to\) tautology, if and only if, it is valid in every model.

### 2.2 Syntax

It is known that Prawitz Natural deduction system for Minimal Logic with only the \(\to\)-rules (\(\to\)-Elim and \(\to\)-Intro) is sound and complete for the \(M \to\) regarding Kripke

---

\(^5\) We remember that we do not know whether \(NP = PSPACE\) or not.
semantics. As a consequence of this, Gentzen’s LJ system ([15, p. 81]) containing only right and left \(\rightarrow\)-rules is also sound and complete. As it is well known the \(\rightarrow\)-left rule of LJ does not preserve invalidity. Figure 1 shows structural and logic rules of an adapted Gentzen’s sequent calculus for \(M^\rightarrow\) based on [16, p. 18, §3]. Basically, we restrict the right side of a sequent to one and only one formula (we are in \(M^\rightarrow\) thus sequents with empty right side does not make sense). This implies that structural rules can only be considered for main formulae on the left side of a sequent.

A central aspect when considering mechanisms for proof search in \(M^\rightarrow\) (and also for IPL) is the application of the \(\rightarrow\)-left rule. Sequent calculus for classical logic (Gentzen’s LK system - [15, p. 81]) ensures that each rule when applied in a bottom-up manner in the proof search reduces the degree of the main formula of the sequent (the formula to which the rule is applied). This implies the termination of the system. For LJ we have the restriction that the right side of a sequent only allows one formula and, as we can reuse a hypothesis in different parts of a proof, the main formula must be available to be used again by the generated premises. Thus, \(\rightarrow\)-left rule has the repetition of the main formula in the premises, a scenario that allows the occurrence of loops in automatic procedures.

\[
\begin{align*}
\Delta, \gamma \Rightarrow \gamma & \quad \text{axiom} \\
\Delta \Rightarrow \gamma & \quad \alpha, \Delta \Rightarrow \gamma \quad \text{weakening} \\
\Gamma, \alpha, \beta, \Delta \Rightarrow \gamma & \quad \alpha, \alpha, \Delta \Rightarrow \gamma \quad \text{contraction} \\
\Gamma, \beta, \alpha, \Delta \Rightarrow \gamma & \quad \Gamma, \alpha, \beta, \Delta \Rightarrow \gamma \quad \text{exchange} \\
\Delta \Rightarrow \alpha & \quad \Delta, \Gamma \Rightarrow \gamma \quad \text{cut} \\
\Delta, \alpha \Rightarrow \beta & \quad \rightarrow\text{right} \\
\Delta \Rightarrow \alpha \Rightarrow \beta & \quad \Delta, \alpha \Rightarrow \beta \Rightarrow \alpha \quad \rightarrow\text{left} \\
\end{align*}
\]

Fig. 1. Rules of Gentzen’s LJ

3 The Sequent Calculus LMT\(\rightarrow\)

In this section we present a sound and complete sequent calculus for \(M^\rightarrow\). We call this system LMT(\(\rightarrow\). We can prove for each rule that if all premises are valid, then the conclusion is also valid and if at least one premise is invalid then the conclusion also is. Besides that, this proof is constructive in the sense that for any sequent we
have an effective way to produce either a proof or a counter-model of it.

We start defining the concept of sequent used in the proposed calculus. A sequent in our system has the following general form:

\[
\{\Delta', \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}\}, \Delta \Rightarrow [p_1, p_2, \ldots, p_n], \varphi
\]

(1)

where \(\varphi\) is a formula in \(\mathcal{L}\) and \(\Delta, \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}\) are bags \(^6\) of formulae. Each \(\Upsilon_i^{p_i}\) represents formulae associated with an atomic formula \(p_i\).

A sequent has two focus areas, one in the left side (curly bracket) and another in the right (square bracket). Curly brackets are used to control the application of the \(\rightarrow\)-left rule and square brackets are used to keep control of formulae that are related to a particular counter-model definition. \(\Delta'\) is a set of formulae and \(p_1, p_2, \ldots, p_n\) is a sequence that does not allow repetition. We call context of the sequent a pair \((\alpha, q)\), where \(\alpha \in \Delta'\) and \(\varphi = q\), where \(q\) is an atomic formula on the right side of the sequent.

The axioms and rules of \(\text{LMT} \rightarrow\) are presented in Figure 2. In each rule, \(\Delta' \subseteq \Delta\).

Rules are inspired by their backward application. In a \(\rightarrow\)-left rule application, the atomic formula, \(q\), on the right side of the conclusion goes to the \([\cdot]\)-area in the left premise. \(\Delta\) formulae in the conclusion are copied to the left premise and marked with a label relating each of them with \(q\). Left premise also has a copy of \(\Delta\) formulae without the \(q\)-label. This is a mechanism to keep track of proving attempts. The form of the restart rule is better understood in the completeness proof on Section 6. A forward reading of rules can be achieved considering the notion of validity, as described Section 5.

4 A Termination Strategy for LMT\(\rightarrow\)

The following is a general strategy to be applied with the rules of \(\text{LMT} \rightarrow\) to generate proofs from an input sequent (a sequent that is candidate to be the conclusion of a proof), that is based on bottom-up application of the rules. From the proposed strategy, we can then state a proposition about termination of the proving process.

A goal sequent is a new sequent in the form of 1, premise of one of the system’s rule, generated by the application of this rule during the proving process. If the goal sequent is an axiom, this branch stops. If it is not and this goal can not be expanded anymore in this branch, then halt and empty the bag of goals. A goal can not be expanded anymore in a branch when we have applied the restarted rule for every atomic formula that appear on the right side over that branch. Otherwise apply the first applicable rule in the following order:

(i) Apply \(\rightarrow\)-right rule if it is possible, i.e., if the formula on the right side of the sequent, outside de \([\cdot]\)-area is not atomic. The premise generated by this application is the new goal of this branch.

(ii) Choose the leftmost formula of a highest degree on the left side of the sequent,

\(^6\) Sets that take repetitions into account: \(\{A, A, B\}\) is not the same set as \(\{A, B\}\)
\[
\begin{align*}
\{\Delta', q\}, \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}, \Delta \Rightarrow [p_1, p_2, \ldots, p_n], q & \quad \text{axiom} \\
\{\Delta', \alpha\}, \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}, \Delta, \alpha \Rightarrow [p_1, p_2, \ldots, p_n], \beta & \quad \text{focus}_\alpha \\
\{\}, \Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i, \Upsilon_{i+1}^{p_{i+1}}, \ldots, \Upsilon_n^{p_n}, \Delta q \Rightarrow [p_1, p_2, \ldots, p_i, \ldots, p_n], q, p_i & \quad \text{restart}_{p_i} \\
\{\Delta', \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_i^{p_i}, \Upsilon_{i+1}^{p_{i+1}}, \ldots, \Upsilon_n^{p_n}, \Delta \Rightarrow [p_1, p_2, \ldots, p_i, \ldots, p_n], q & \quad \rightarrow_{-\text{right}} \alpha \rightarrow \beta \\
\{\Delta', \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}, \Delta \Rightarrow [p_1, p_2, \ldots, p_n], \alpha \rightarrow \beta & \quad \rightarrow_{\text{left}} \alpha \rightarrow \beta \\
\end{align*}
\]

Considering \( \overline{\Upsilon} = \bigcup_{i=1}^{n} \Upsilon_i^{p_i} \) and \( \bar{p} = p_1, p_2, \ldots, p_n \), we have:

\[
\{\alpha \rightarrow \beta, \Delta'\}, \overline{\Upsilon}, \Delta q, \Delta \Rightarrow [\bar{p}, q], \alpha \quad \{\alpha \rightarrow \beta, \Delta'\}, \overline{\Upsilon}, \Delta, \beta \Rightarrow [\bar{p}, q] \\
\{\alpha \rightarrow \beta, \Delta'\}, \overline{\Upsilon}, \Delta \Rightarrow [\bar{p}, q] \quad \rightarrow_{\text{left}} \alpha \rightarrow \beta
\]

Fig. 2. Rules of \( \text{LMT}^{\rightarrow} \)

not labeled yet, i.e., a formula \( \alpha \in \Delta \) that is not occurring in \( \Delta' \), then apply the focus rule. The premise generated by this application is the new goal of this branch.

(iii) If all formulae on the left side have already been focused, choose the first formula \( \alpha \in \Delta' \) such that the context \( (\alpha, q) \) was not yet tried since the last application of a restart rule. We say that a context \( (\alpha, q) \) is already tried when a formula \( \alpha \) on the left was expanded (by the application of \( \rightarrow_{-\text{left}} \) rule) with \( q \) as the formula outside the \([\cdot]\)-area on the right side of the sequent. The premises generated by this application become new goals of the respective new branches.

(iv) Choose the leftmost formula inside the \([\cdot]\)-area that was not chosen before in this branch and apply the restart rule. The premise generated by this application is the new goal of this branch.
Figure 3 shows an attempt proof tree generated by the application of the aforementioned strategy.

**Proposition 4.1** Given that the bag of goals contains only one copy of \{\Delta', \gamma_1^{p_1}, \gamma_2^{p_2}, \ldots, \gamma_n^{p_n}, \Delta \Rightarrow [p_1, p_2, \ldots, p_n], \varphi\} then, based on the aforementioned strategy, LMT→ eventually stops.

**Proof.**

- \rightarrow\text{-right rule} is applied until we obtain an atomic formula on the right side.
- focus rule is applied until every non-labeled formula become focused. The same formula can not be focused twice, unless a restart rule is applied.
- \rightarrow\text{-left rule} can not be applied more than once to a formula, unless a restart rule is applied.
- between two applications of the restart rule in a branch there is only one possible application of a \rightarrow\text{-left rule} for a context \((\alpha, q)\).
- restart rule is applied only once for each atomic formula that appears on the right side of sequents in a branch. This implies a finite number of application of the restart rule.

\[\square\]

**Observation 4.1** From the proof strategy we can make the following observations about a tree generated during a proving process:

(i) A top sequent is the highest sequent of a branch in the tree.
(ii) In a top sequent of a branch on the form of sequent 1, if \varphi \in \Delta then the top sequent is an axiom and the branch is called a closed branch. Otherwise, we say that the branch is open and \varphi is an atomic formula.
(iii) In every sequent of the tree, \Delta' \subseteq \Delta.
(iv) For \(i = 1, \ldots, n\), \(\gamma_{i-1}^{p_i} \subseteq \gamma_i^{p_i}\).

The proof of completeness of LMT→ is closely related with this strategy and with the way the proof tree is labeled during the proving process. Section 5 presents the soundness proof of LMT→ and Section 6, the completeness proof.
\begin{itemize}
\item \{\Delta', \Upsilon_1^{p_i}, \Upsilon_2^{p_i}, \Upsilon_{i-1}^{p_i}, \ldots, \Upsilon_i^p, \Delta \Rightarrow [p_1, p_2, \ldots, p_{i-1}, p_i], p_k\} (where k = 1, 2, \ldots, i)
\item a sequence of focus, \rightarrow-left and \rightarrow-right
\item \{\}, \Upsilon_1^{p_i}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta \Rightarrow [p_1, p_2, \ldots, p_{i-1}, p_i]
\item a sequence of focus, \rightarrow-left, \rightarrow-right and restart (for each atomic formula in the \llbracket-\text{area})
\item \{\varphi \rightarrow \psi\}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta^{p_i}, \Upsilon_1^{p_i}, \Upsilon_1, \varphi_1, \ldots, \varphi_n \Rightarrow [p_2, \ldots, p_{i-1}, p_i, p_1], p_2\}
\item a sequence of focus, \rightarrow-left and \rightarrow-right
\item \{\varphi \rightarrow \psi\}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta^{p_i}, \Upsilon_1^{p_i}, \Upsilon_1 \Rightarrow [p_2, \ldots, p_{i-1}, p_i], \varphi
\item \{\varphi \rightarrow \psi\}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta^{p_i}, \Upsilon_1 \Rightarrow [p_2, \ldots, p_{i-1}, p_i], p_1
\item \{\varphi \rightarrow \psi\}, \Upsilon_1^{p_i}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta \Rightarrow [p_1, p_2, \ldots, p_{i-1}], p_i
\item \{\Delta', \Upsilon_1^{p_i}, \Upsilon_2^{p_i}, \ldots, \Upsilon_{i-1}^{p_i}, \Delta \Rightarrow [p_1, p_2, \ldots, p_{i-1}], p_i
\item \{\}, \Upsilon_1^{p_i}, \Upsilon_1 \Rightarrow [p_1], p_2
\item a sequence \rightarrow-right
\item \{\varphi \rightarrow \psi\}, \Upsilon_1^{p_i} \Rightarrow [p_1], \varphi
\item \{\varphi \rightarrow \psi\}, \Upsilon_1 \Rightarrow [], p_1
\item \{\}, \varphi \rightarrow \psi \Rightarrow [], p_1
\item \{\} \Rightarrow [], (\varphi \rightarrow \psi) \rightarrow \gamma
\end{itemize}

Fig. 3. General attempt proof tree
5 Soundness of LMT\(\rightarrow\)

In this section we prove the soundness of LMT\(\rightarrow\). A few basic facts and definitions used in the proof follow.

**Definition 5.1** A sequent \(\{\Delta', \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}, \Delta \}\Rightarrow [p_1, p_2, \ldots, p_n], \varphi\) is valid, if and only if, \(\Delta', \Delta \models \varphi\) or \(\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i\), for \(i = 1, \ldots, n\).

**Definition 5.2** We say that a rule is sound, if and only if, in the case of the premises of the sequent are valid sequents, then its conclusion also is.

A calculus is sound, if and only if, each of its rules are sound. We prove the soundness of LMT\(\rightarrow\) by showing that this is the case for each one of its rules.

**Proposition 5.3** Considering validity of a sequent as defined in Definition 5.1, LMT\(\rightarrow\) is sound.

**Proof.** We show that supposing that premises of a rule is valid then, the validity of the conclusion follows. In the sequel we analyze each rule of LMT\(\rightarrow\).

\(\rightarrow\)-left We need to analyze both premises together, thus we have the combinations described below.

- Supposing the left premise is valid because \(\alpha \rightarrow \beta, \Delta', \Delta \models \alpha\) and the right premise is valid because \(\alpha \rightarrow \beta, \Delta', \Delta, \beta \models q\). We also know that \(\alpha \rightarrow \beta \in \Delta\) and \(\Delta' \subseteq \Delta\). In this case, the conclusion holds:

\[
\frac{\alpha \rightarrow \beta \Delta' \Delta}{\frac{\alpha}{\beta}} \frac{\Pi}{q}
\]

- Supposing the left premise is valid because \(\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i\), for \(i = 1, \ldots, n\), the conclusion holds as it is the same. Supposing the left premise is true because \(\Delta \models q\), the conclusion also holds, as \(\Delta q = \Delta\).

- Supposing the right premise is valid because \(\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i\), for \(i = 1, \ldots, n\), then conclusion also holds.

restart Here, we have three cases to evaluate.

- Supposing the premise is valid because \(\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i \models p_i\), then \(\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i\), for \(i = 1, \ldots, n\). The conclusion is also valid.

- Supposing the premise is valid because \(\exists j (\bigcup_{k=i+1}^{j} \Upsilon_k^{p_k}) \models p_j\), for \(j = i + 1, \ldots, n\), then conclusion also holds.
• Supposing the premise is valid because $\Delta^q \models q$, then $\Delta \models q$ and, as $\Delta' \subseteq \Delta$, $\Delta', \Delta \models q$.

→-right

• Supposing the premise is valid because $\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i \models p_i$, then $\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i$, for $i = 1, \ldots, n$. This is also valid in the conclusion.

• Supposing the premise is valid because $\Delta', \Delta, \alpha \models \beta$, then every Kripke model that satisfies $\Delta'$, $\Delta$ and $\alpha$ also satisfies $\beta$. We know that $\Delta' \subseteq \Delta$. Those models also satisfies $\alpha \rightarrow \beta$ and, then, conclusion also holds.

focus

• Supposing the premise is valid because $\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i \models p_i$, then $\exists i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \models p_i$, for $i = 1, \ldots, n$. This is also valid in the conclusion.

• Supposing the premise is valid because $\Delta', \Delta, \alpha \models \beta$, then the conclusion also holds as $\Delta', \Delta, \alpha \models \beta$.

From Proposition 5.3, we conclude that $\text{LMT}^\rightarrow$ only prove tautologies.

6 Completeness of $\text{LMT}^\rightarrow$

By observation 4.1 iii we know that a top sequent of an open branch in an attempt proof tree has the general form bellow, where $q$ is an atomic formula:

$$\{\Delta'\}, \Upsilon_1^{p_1}, \Upsilon_2^{p_2}, \ldots, \Upsilon_n^{p_n}, \Delta \Rightarrow [p_1, p_2, \ldots, p_n], q$$

From Definition 5.1, we can say that a sequent is invalid if and only if $\Delta', \Delta \not\models q$ and $\forall i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \not\models p_i$, for $i = 1, \ldots, n$.

Definition 6.1 We can construct a Kripke counter-model $\mathcal{M}$ that falsifies a top sequent of an open branch. This can be done in the following way:

(i) The model $\mathcal{M}$ has an initial world $w$, i.e., $w$ is not accessible by any other world. In $w$ set every atomic formula inside the $\lbrack \rbrack$-area as false. That is, $\mathcal{M} \not\models_w p_i$, for $i = 1, \ldots, n$.

(ii) Consider a world $w_0$ in $\mathcal{M}$, such that $w \preceq w_0$. By the definition of an invalid sequent, $\Delta', \Delta \not\models q$. $w_0$ will be used to guarantee this. We set $q$ false in $w_0$, i.e., $\mathcal{M} \not\models_{w_0} q$. This implies that $\mathcal{M} \not\models_w q$. We also set every atomic formula that is in $\Delta$ (remember that $\Delta' \subseteq \Delta$) as true, i.e., $\forall p, p \in \Delta, \mathcal{M} \models_{w_0} p$. This is consistent with the values of the same atomic formulae in $w$.

(iii) By the definition of an invalid sequent, we also need that $\forall i (\bigcup_{k=1}^{i} \Upsilon_k^{p_k}) \not\models p_i$, for
Thus, for each $i, i = 1, \ldots n$ we define a world $w_i$ in $\mathcal{M}$, such that $w \preceq w_i$. We set $\forall p, p \in \mathcal{Y}_i^{p_i}$, $p$ atomic, $\mathcal{M} \models_{w_i} p$. We also set $\mathcal{M} \not\models_{w_i} p_i$.

The general schema of the counter-model generated by the definition 6.1 is

$$
\begin{array}{c}
\mathsf{w} \\
\not\models p_i, i = 1, \ldots n \\
\mathsf{w_n} \\
\cdots \\
\mathsf{w_1} \\
\mathsf{w_0} \\
\forall p, p \in \mathcal{Y}_n^{p_n} \\
\forall p, p \in \mathcal{Y}_i^{p_i} \\
p \text{ atomic} \\
p \text{ atomic} \\
\models p \\
\models p \\
\models p \\
\end{array}
$$

Fig. 4. General schema of counter-models

This schema to construct counter-model allows us to state the following lemma:

**Lemma 6.2** Let $S$ be a top sequent of an open branch in an attempt proof tree generated by the strategy presented in Section 4. Then we can construct a Kripke model $\mathcal{M}$ with a world $u$ where $\mathcal{M} \not\models u S$, using the aforementioned counter-model generation schema.

**Proof.** We can prove this by induction on the degree of formulas in $\Delta$ and in $\mathcal{Y}_i^{p_i}$, for $i = 1, \ldots n$. From definition 6.1 ii we know that every atomic formula in $\Delta$ is true in $w_0$ and that $\not\models_{w_0} q$. From definition 6.1 iii we know that every atomic formula in $\mathcal{Y}_i^{p_i}$ is true in $w_i$ and that $\not\models_{w_i} p_i$. The inductive hypothesis is that every formula in $\Delta$ is true in $w_0$ and that every formula in $\mathcal{Y}_i^{p_i}$ is true in $w_i$.

Thus, we have two cases:

(i) Let $\alpha \rightarrow \beta$ be a formula in $\mathcal{M} \rightarrow$ that is in $\Delta$. We show that $\mathcal{M} \models_{w_0} \alpha \rightarrow \beta$. Consider that $\alpha \equiv (\gamma_1 \rightarrow (\gamma_2 \rightarrow \ldots \rightarrow (\gamma_m \rightarrow q)))$. By the proof strategy, $\gamma_1, \gamma_2, \ldots, \gamma_m$ also are in $\Delta$. The degree of each of these formulae are less than the degree of $\alpha \rightarrow \beta$ and, by the induction hypothesis, all of them are true in $w_0$. This makes $\not\models_{w_0} \alpha$ and $\models_{w_0} \alpha \rightarrow \beta$.

(ii) Let $\alpha \rightarrow \beta$ be a formula in $\mathcal{M} \rightarrow$ that is in $\mathcal{Y}_i^{p_i}$, for $i = 1, \ldots n$. We show that $\mathcal{M} \models_{w_i} \alpha \rightarrow \beta$.

Consider that $\alpha \equiv (\gamma_1 \rightarrow (\gamma_2 \rightarrow \ldots \rightarrow (\gamma_m \rightarrow q)))$. By the proof strategy, $\gamma_1, \gamma_2, \ldots, \gamma_m$ also are in $\mathcal{Y}_i^{p_i}$. The degree of each of these formulae are less than the degree of $\alpha \rightarrow \beta$ and, by the induction hypothesis, all of them are true in $w_i$. This makes $\not\models_{w_i} \alpha$ and $\models_{w_i} \alpha \rightarrow \beta$. 

$\square$
Definition 6.3 A rule is said invertible or double-sound iff the validity of its conclusion implies the validity of its premisses.

In other words, by Definition 6.3 we know that a counter-model for a top sequent of a proof tree which can not be expanded anymore can be used to construct a counter-model to every sequent in the same branch of the tree until the conclusion (root sequent). In the case of \( \rightarrow \)-right rule in our system, not just that if a premiss of the rule has a counter-model then so does the conclusion, but the same counter-model will do. Weich called rules with this property preserving counter model rules [19]. Dyckhoff proposed call them strongly invertible rules (personal communication).

Lemma 6.4 The rules of LMT\( \rightarrow \) are invertible.

Proof. We show that the rules of LMT\( \rightarrow \) are invertible when considering a proof tree labeled in the schema presented in Section 3. We prove that from the existence of a Kripke model that makes a premise of the rule invalid then, conclusion is also invalid.

\( \rightarrow \)-right If the premise is invalid, then there is a Kripke model \( \mathcal{M} \) where \( \Delta', \Delta, \alpha \not\models \beta \) and \( \forall i \left( \bigcup_{k=1}^{i} \Upsilon_{k}^{p_i} \right) \not\equiv p_i \), for \( i = 1, \ldots, n \) from a given world \( u \). Thus, in the conclusion we have:

- By the definition of semantics of Section 2.1, there have to be a world \( v, u \preceq v \), in the model \( \mathcal{M} \) where \( \Delta', \Delta, \alpha \) are satisfied and where \( \beta \) is not. Thus, in \( v \), \( \alpha \rightarrow \beta \) cannot hold.
- By the model \( \mathcal{M} \), for each \( i \), exists a world \( v_i, u \preceq v_i \), where \( \models_{v_i} \Upsilon_{i}^{p_i} \) and \( \not\models_{v_i} p_i \).
- Thus, the conclusion is also invalid.

\( \rightarrow \)-left Considering that one of the premises of \( \rightarrow \)-left are not valid, the conclusion also is. Thus, we have to evaluate both cases:

- If the right premise is invalid then there is a Kripke model \( \mathcal{M} \) where \( \alpha \rightarrow \beta, \Delta', \Delta, \beta \not\models q \) and \( \forall i \left( \bigcup_{k=1}^{i} \Upsilon_{k}^{p_i} \right) \not\equiv p_i \), for \( i = 1, \ldots, n \) from a given world \( u \). Thus, in the conclusion we have:
  - By the model \( \mathcal{M} \), there have to be a world \( v, u \preceq v \), in the model where \( \alpha \rightarrow \beta, \Delta', \Delta, \beta \) are satisfied and where \( q \) is not.
  - By the model \( \mathcal{M} \), for each \( i \), exists a world \( v_i, u \preceq v_i \), where \( \models_{v_i} \Upsilon_{i}^{p_i} \) and \( \not\models_{v_i} p_i \).
  - Thus, the conclusion is invalid too.

- If the left premise is invalid then there is a Kripke model \( \mathcal{M} \) where \( \alpha \rightarrow \beta, \Delta' \not\models \alpha \) and \( \forall i \left( \bigcup_{k=1}^{i} \Upsilon_{k}^{p_i} \right) \not\equiv p_i \), for \( i = 1, \ldots, n \), and \( \Delta' \not\models q \) from a given world \( u \). Thus, in the conclusion we have:
  - By the model \( \mathcal{M} \), there have to be a world \( v, u \preceq v \), in the model where
\[ \alpha \rightarrow \beta, \Delta' \] are satisfied and where \( \alpha \) is not.

- By the model \( M \), for each \( i \), exists a world \( v_i, u \preceq v_i, \) where \( \models_{v_i} T_{p_i} \) and \( \not\models_{v_i} p_i \).

- We also know by \( M \) that there is a world \( v_q, u \preceq v_q, \) where \( \models_{v_q} \Delta' \) and \( \not\models_{v_q} q \). We also have that \( \Delta' \subseteq \Delta \) and that \( \alpha \rightarrow \beta \in \Delta \). Therefore, \( \models_{v_q} \Delta' \) and \( \models_{v_q} \alpha \rightarrow \beta \).

- Thus, the conclusion can not be valid.

**focus** If we have a model that invalidates the premise, this model also invalidates the conclusion as the sequents in the premise and in the conclusion are the same despite the repetition of the focused formula \( \alpha \).

**restart** If the restart premise is invalid, then there is a Kripke model \( M \) and a world \( u \) from which \( \Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i \not\models p_i \) and \( \forall j (\bigcup_{k=1}^{j} \Upsilon_{p_k}^j) \models p_j \), for \( j = i+1, \ldots, n \), and \( \Delta' \not\models q \). Thus, in the conclusion we have:

- By the model \( M \), there have to be a world \( v, u \preceq v, \) in the model where \( \Upsilon_1, \Upsilon_2, \ldots, \Upsilon_i \) are satisfied and where \( p_i \) is not. Each \( \Upsilon_k \) has the same formulae as \( \Upsilon_{p_k}^j \) and, by the restart condition, we know that \( \not\models p_k, \) for \( k = 1, \ldots, i. \)

- By the model \( M \), for each \( j \), exists a world \( v_j, u \preceq v_j, \) where \( \models_{v_j} \Upsilon_{p_j}^j \) and \( \not\models_{v_j} p_j \).

- We also know by \( M \) that there is a world \( v_q, u \preceq v_q, \) where \( \models_{v_q} \Delta' \) and \( \not\models_{v_q} q. \)

- We also have that \( \Delta' \subseteq \Delta \). Therefore, \( \models_{v_q} \Delta' \).

- Thus, the conclusion is invalid.

Now we can state a proposition about completeness of \( \text{LMT}^{\rightarrow} \):

**Proposition 6.5** \( \text{LMT}^{\rightarrow} \) is complete regarding the proof strategy presented in Section 3

**Proof.** It follows direct from Proposition 4.1 (the process always terminates) and Lemmas 6.4 and 6.2 above. \( \square \)

## 7 An automatic theorem prover for \( \text{M}^{\rightarrow} \)

Based on the aforementioned system, we developed a theorem prover for \( \text{M}^{\rightarrow} \) (its source code can be found at https://github.com/jeffsantos/sequent-prover). Figure 5 shows a fragment of the proof tree generated by this prover for the formula:

\[ (((A \rightarrow C) \rightarrow A) \rightarrow A) \rightarrow C, \]

a formula that is shown in [2] to need to use the assumption \( (((A \rightarrow C) \rightarrow A) \rightarrow A) \rightarrow C \) at least twice to be proved in \( \text{M}^{\rightarrow} \). As presented in [6] this formula is used as the base to define a family of formulae in \( \text{M}^{\rightarrow} \) with no bounds on the use of assumptions. Figure 5 shows the expansion of the left branch of the final proof.
8 Related Work

A common way to control the proof search procedure in $M \rightarrow$ (and in IPL) is by the definition of routines for loop verification as proposed in [17]. Loop checkers are very expensive procedures, although they are effective to guarantee termination in automatic provers for $M \rightarrow$ (and other logics with the same characteristic). The work in [9] and in [10] are examples of techniques that can be used to minimize the performance problems that can arise with the usage of such procedures.

To avoid the use of loop checkers, Dyckhoff [3] proposed a terminating contraction-free sequent calculus for IPL, named LJT, using a technique based on the work of Vorob’ev [18] in the 50s. Pinto and Dyckhoff, in [13], extended this work showing a method to generate counter-examples in this system. They proposed two calculi, one for proof search and another for counter-model generation, forming a way to decide about the validity or not of formulae in IPL. A characteristic of their systems is that the sub-formula property does not hold on them. In [5], a similar approach is presented using systems where the sub-formula property holds. They also proposed a single decision procedure for IPL which guarantee minimal depth counter-model.

Focused sequent calculi appeared initially in the Andreoli’s work on linear logic ([1]). The author identified a subset of proofs from Gentzen style sequent calculus, which are complete and tractable. Liang and Miller [12] proposed the focused sequent calculi LJF where they used a mapping of IPL into linear logic and adapted the Andreoli’s system to work with the image. Dyckhoff and Lengrand [4] presented the focused system LJQ that work direct in IPL. Focusing is used in their system as a way to implement restrictions in the $\rightarrow$-left rule as proposed by [18] and [11]. The work of Dyckhoff and Lengrand follows from the calculus with the same name presented in [8]. In our approach, focusing is used as a technique to guarantee the completeness of the system and to produce the counter-model from a failed proof search process.

9 Conclusion and Future Work

We presented here the definition of a unified procedure (the LMT$\rightarrow$ system) to generate Kripke counter-models from trees generated by unsuccess proving processes for $M \rightarrow$.

Regarding the LMT$\rightarrow$ system, we know that the size of the generated counter-model still takes into account every possible combination of sub-formulae yielding Kripke models with quite a lot worlds. There are still work to be done in order to produce smaller models.

On the theorem prover side, our research has a lot of work to be done. Further work includes the implementation of user strategies that can be combined with the built-in prover strategy to customize the way the prover conducts the proving process. Interface and user interaction with the system are other options to improve.
Acknowledgment

We would like to thank Roy Dyckhoff for all revisions, critics and suggestions.

References

Fig. 5. Partial proof tree for $(((A \rightarrow C) \rightarrow A) \rightarrow (A \rightarrow C)) \rightarrow C$