Forward Proof Search for Intuitionistic Multimodal K Logics

Niels Voorneveld,

niels.voorneveld@cyber.ee

TABLEAUX 2025, Reykjavik, September 27, 2025

This research has been supported by Estonian Research Council, grant No. PRG1780.

Motivation

Formalisation of systems with distributed knowledge and claims.

Modalities can be used to give more context to pieces of knowledge.

- When and where a statement is given
- Who said or hears or believes the statement
- How a statement is communicated.

Intuitionistic logics are inherently constructive and adaptable to computer formalisation following the proofs as types paradigm.

Decidability and Beyond

In practise, good to decide whether a property is provable:

- Tools for completing proofs for logical arguments.
- Checking consequences of assumptions, and dependencies of conclusions.

Decidability and Beyond

In practise, good to decide whether a property is provable:

- Tools for completing proofs for logical arguments.
- Checking consequences of assumptions, and dependencies of conclusions.

There is a difference between decidable and runnable.

- Standard arguments for decidability have exponential blow-up.
- Organizing data structures to facilitate quick proof step searches has many benefits.

Overview

Decidability of multimodal K logics

by adapting Pfennings Cut elimination proof

Forward search technique

using analytic cuts

Multimodal K

Axiom K and Necessity

Suppose given a set of formulas $\mathbb{F}$ closed under a set of unary operations called modalities $\mathbb{M}$.

We write $A_1, \ldots, A_n \vdash B$ to mean: given a sequence of assumptions $A_1, \ldots, A_n$, we can prove the conclusion B.

General rule for modalities satisfying Axiom K and N:

$$\frac{A_1, \ldots, A_n \vdash B}{\mathcal{M}A_1, \ldots, \mathcal{M}A_n \vdash \mathcal{M}B}$$

- Axiom K is the $n \geq 2$ case.
- Necessity is the $n = 0$ case.

Additional Modal Axioms

Axiom types:

- $\forall A \in \mathbb{F}.\mathcal{M}A \vdash A$, ($\mathcal{M}$ is a domain of true knowledge).
- $\forall A \in \mathbb{F}.\mathcal{M}A \vdash \mathcal{N}A$, ($\mathcal{N}$ inherits information from $\mathcal{M}$)
- $\forall A \in \mathbb{F}.\mathcal{M}A \vdash \mathcal{N}\mathcal{R}A$, ($\mathcal{N}$ perceives $\mathcal{M}$ as $\mathcal{R}$)

$\Rrightarrow$ between $\mathbb{M}$ and $\mathbb{M}^*$ (lists over $\mathbb{M}$), where $\mathcal{M} \Rrightarrow \mathcal{N}_1 \ldots \mathcal{N}_n$ asserts the axiom $\forall A \in \mathbb{F}.\mathcal{M}A \vdash \mathcal{N}_1 \ldots \mathcal{N}_n A$.

Properties

Unrestricitve properties of $\Rrightarrow$:

- $\Rrightarrow$ is *reflexive* if for any $\mathcal{M}$, $\mathcal{M} \Rrightarrow \mathcal{M}$.
- $\Rrightarrow$ is *transitive* if $\mathcal{M} \Rrightarrow \alpha\mathcal{N}\beta$ and $\mathcal{N} \Rrightarrow \gamma$ implies $\mathcal{M} \Rrightarrow \alpha\gamma\beta$.

Properties

Unrestricitve properties of $\Rrightarrow$:

- $\Rrightarrow$ is *reflexive* if for any $\mathcal{M}$, $\mathcal{M} \Rrightarrow \mathcal{M}$.
- $\Rrightarrow$ is *transitive* if $\mathcal{M} \Rrightarrow \alpha\mathcal{N}\beta$ and $\mathcal{N} \Rrightarrow \gamma$ implies $\mathcal{M} \Rrightarrow \alpha\gamma\beta$.

Restrictive properties of $\Rrightarrow$ to accommodate decidability:

- $\Rrightarrow$ is *decomposable* if $\forall \mathcal{M}, \mathcal{N} \in \mathbb{M}$ there is a finite set $(\mathcal{M} \ominus \mathcal{N}) \subseteq \mathbb{M}$ s.t.:
  - For any $\mathcal{R} \in (\mathcal{M} \ominus \mathcal{N})$, $\mathcal{M} \Rrightarrow \mathcal{N}\mathcal{R}$.
  - For any non-empty $\alpha \in \mathbb{M}^*$ s.t. $\mathcal{M} \Rrightarrow \mathcal{N}\alpha$, $\exists \mathcal{R} \in \mathcal{M} \ominus \mathcal{N}$ such that $\mathcal{R} \Rrightarrow \alpha$.
- Decomposition is *terminating* if there is a preorder on modalities $\preceq$ s.t.:
  - For any $\mathcal{M}$ the set $\{\mathcal{N} \mid \mathcal{N} \preceq \mathcal{M}\}$ is finite.
  - For any $\mathcal{M}$ and $\mathcal{N}$, and $\mathcal{R} \in (\mathcal{M} \ominus \mathcal{N})$, then $\mathcal{R} \preceq \mathcal{M}$.

Example: $\Box$

The $\Box$ modality for *necessarily* true facts:

- $\Box A \vdash A$,
- $\Box A \vdash \Box\Box A$,

$\Rrightarrow$ is the total relation between $\{\Box\}$ and $\{\Box\}^*$.

$(\Box \ominus \Box) = \{\Box\}$.

Adding other modalities $\mathbb{M}$:

- $\Box A \vdash \mathcal{M}\Box A$

$(\Box \ominus \mathcal{M}) = \{\Box\}$, and $(\mathcal{M} \ominus \mathcal{N}) = \emptyset$ for any $\mathcal{M}, \mathcal{N} \in \mathbb{M}$

Example: Awareness

We equip $\mathbb{M}$ with a reflexive and transitive relation $\triangleleft$ expressing *awareness*.

The statement $\mathcal{M} \triangleleft \mathcal{N}$ means $\mathcal{M}$ is aware of all knowledge in $\mathcal{N}$, which is asserted with the axiom $\mathcal{N} A \vdash \mathcal{M} \mathcal{N} A$.

$\mathcal{N} \Rrightarrow \alpha\mathcal{N}$ holds when each modality in $\alpha\mathcal{N}$ is aware of the next one.

Note that this is reflexive and transitive.
We define $(\mathcal{M} \ominus \mathcal{N}) = \{\mathcal{M}\}$ if $\mathcal{N} \triangleleft \mathcal{M}$, and otherwise $(\mathcal{M} \ominus \mathcal{N}) = \emptyset$.

Decidability

Modal Weakening

Suppose contexts Γ and Δ are given by sets of formulas.

We write $\Gamma \sqsubseteq \Delta$ if for any formula $A \in \Gamma$:

- $A \in \Delta$, or
- $A = \mathcal{M}B$, and $\mathcal{N}B \in \Delta$ for some $\mathcal{N}$ such that $\mathcal{N} \Rrightarrow \mathcal{M}$.

The resulting calculus should admit a structural weakening property:

If $\Gamma \sqsubseteq \Delta$ then any proof of $\Gamma \vdash A$ gives a proof of $\Delta \vdash A$ of the same shape.

Modal Shift

Given context Γ and modality $\mathcal{M}$, we define the modal shift of Γ by $\mathcal{M}$ as the context:

$$\mathcal{M}^{-1}(\Gamma) = \{A \mid \mathcal{N}A \in \Gamma, \mathcal{N} \Rrightarrow \mathcal{M}\} \cup \{\mathcal{R}A \mid \mathcal{N}A \in \Gamma, \mathcal{R} \in (\mathcal{N} \ominus \mathcal{M})\}$$

- If $\Gamma \sqsubseteq \Delta$, then $\mathcal{M}^{-1}\Gamma \sqsubseteq \mathcal{M}^{-1}\Delta$.
- If $\mathcal{M} \Rrightarrow \mathcal{N}$ then $\mathcal{M}^{-1}\Gamma \sqsubseteq \mathcal{N}^{-1}\Gamma$.
- Suppose $\mathcal{T} \in \mathcal{M} \ominus \mathcal{N}$, then $\mathcal{M}^{-1}\Gamma \sqsubseteq \mathcal{T}^{-1}(\mathcal{N}^{-1}\Gamma)$

Intuitionistic Modal Logic

Formulas of the logic are inductively generated according to the following rules, with a ranging over some set of basic formulas.

$$A, B := a \mid A \wedge B \mid A \vee B \mid A \Rightarrow B \mid \mathcal{M}A \mid \top \mid \bot$$

Provability follows standard intuitionistic derivation rules for sequents, plus:

$$\frac{A_1, \ldots, A_n \vdash B}{\mathcal{M}A_1, \ldots, \mathcal{M}A_n \vdash \mathcal{M}B} \qquad \frac{\mathcal{M} \Rrightarrow \mathcal{N}_1 \ldots \mathcal{N}_n}{\mathcal{M}A \vdash \mathcal{N}_1 \ldots \mathcal{N}_n A}$$

Gentzen's sequent calculus adaptation

Standard (note, contraction and commutativity are structural):

$$\frac{}{\Gamma, a \vdash a}(\text{Var}) \qquad \frac{}{\Gamma \vdash \top}(\top\text{R}) \qquad \frac{}{\Gamma, \bot \vdash A}(\bot\text{L})$$

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

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee\text{R1}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee\text{R2}) \qquad \frac{\Gamma, A \vee B, A \vdash C \qquad \Gamma, A \vee B, B \vdash C}{\Gamma, A \vee B \vdash C}(\vee\text{L})$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}(\Rightarrow\text{R}) \qquad \frac{\Gamma, A \Rightarrow B \vdash A \qquad \Gamma, A \Rightarrow B, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}(\Rightarrow\text{L})$$

Additions:

$$\frac{\Gamma, \mathcal{M}A, A \vdash B \qquad \mathcal{M} \Rrightarrow \cdot}{\Gamma, \mathcal{M}A \vdash B}(\text{ModL}) \qquad \frac{\mathcal{M}^{-1}\Gamma \vdash A}{\Gamma \vdash \mathcal{M}A}(\text{Mod})$$

Properties Overview

Identity theorem: For every $A \in \mathbb{F}$, and Γ we can prove $\Gamma, A \vdash A$.

Extending the subformula relation with $\preceq$, creating $\preceq$ on formulas.

- Subformula property: Any formula used in a proof of a sequent s is a subformula of a formula in s,
- hence the sequent calculus is decidable.

The sequent calculus admits cuts, so provability is equivalent to provability in the aforementioned intuitionistic multimodal K logic.

Cut Elimination

Adapting Pfenning's cut elimination proof [1]: Suppose $\mathsf{D} = \frac{\mathsf{D}_1 \ldots \mathsf{D}_n}{\Gamma \vdash A}$ and $\mathsf{E} = \frac{\mathsf{E}_1 \ldots \mathsf{E}_m}{\Gamma, A \vdash B}$, we construct a proof $\mathsf{F} = \frac{\mathsf{F}_1 \ldots \mathsf{F}_k}{\Gamma \vdash B}$, by mutual induction on A, D and E.

Example, New case 3: By example, supposing $\mathcal{N}^{-1}(\mathcal{M}A)) = \mathcal{R}A, A$

$$\mathsf{D} = \cfrac{\cfrac{\mathsf{D}_1}{\mathcal{M}^{-1}\Gamma \vdash A}\,(\text{d1})}{\Gamma \vdash \mathcal{M}A}\,(\text{Mod}) \qquad \mathsf{E}\ \cfrac{\cfrac{\mathsf{E}_1}{\mathcal{N}^{-1}(\Gamma, \mathcal{M}A) \vdash B}\,(\text{e1})}{\Gamma, \mathcal{M}A \vdash \mathcal{N}B}\,(\text{Mod})$$

$$\cfrac{\cfrac{\mathsf{D}_1''}{\mathcal{N}^{-1}\Gamma \vdash A}\,(\text{d1}) \quad \cfrac{\cfrac{\cfrac{\mathsf{D}_1'}{\mathcal{R}^{-1}(\mathcal{N}^{-1}\Gamma) \vdash A}\,(\text{d1})}{\mathcal{N}^{-1}\Gamma \vdash \mathcal{R}A}\,(\text{Mod}) \quad \cfrac{\mathsf{E}_1}{\mathcal{N}^{-1}\Gamma, \mathcal{R}A, A \vdash B}\,(\text{e1})}{\mathcal{N}^{-1}\Gamma, A \vdash B}\,(\text{IH-E})}{\mathcal{N}^{-1}\Gamma \vdash B}\,(\text{IH-A})$$

Forward Proof Search

Proof Search Bottlenecks

There is a large practical gap between *decidable* and *runnable*.

In what order should we unfold formulas in the context?

$$\frac{\Gamma, A \vee B, A \vdash C \qquad \Gamma, A \vee B, B \vdash C}{\Gamma, A \vee B \vdash C}(\vee\mathrm{L}) \qquad \frac{\Gamma, A \Rightarrow B \vdash A \qquad \Gamma, A \Rightarrow B, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}(\Rightarrow\mathrm{L}) \qquad \frac{\mathcal{M}^{-1}\Gamma \vdash A}{\Gamma \vdash \mathcal{M}A}(\mathrm{Mod})$$

- We change to a top-down approach, *accumulating* relevant true sequents.
- The *inverse method* can be applied to the sequent calculus.
- We attempt further optimization by changing the calculus to deal with computationally cumbersome derivation rules, like $\vee$L and Mod.

Forward Proof Search

We start with two sets of formulas:

- A set of *questions* or *goals* $?A$ we are interested in proving.
- A set of *answers* or *assumptions* $!A$ we can use.

The forward proof search proceeds in two phases:

- Initiation phase: We recursively generate basic sequents for proving goals, and using assumptions, whilst adding more subformulas to $?A$ and $!A$.
- Accumulation phase: We use further derivation techniques to find more provable sequents, centered around the analytic cut rule.

Modal Sequents

Modal multi-consequent sequents:

$$|_{id}\, \Gamma \Vdash \Delta \qquad \text{and} \qquad \Phi \,|_{\mathcal{M}}\, \Gamma \Vdash \Delta,$$

the latter representing $\bigwedge \Phi \Rightarrow \mathcal{M}\,(\bigwedge \Gamma \Rightarrow \bigvee \Delta)$

Modal Sequents

Modal multi-consequent sequents:

$$|_{id}\ \Gamma \Vdash \Delta \qquad\qquad \text{and} \qquad\qquad \Phi\ |_{\mathcal{M}}\ \Gamma \Vdash \Delta,$$

the latter representing $\bigwedge \Phi \Rightarrow \mathcal{M}\,(\bigwedge \Gamma \Rightarrow \bigvee \Delta)$

Suppose $\triangledown : (\mathbb{M} \cup \{id\}) \times (\mathbb{M} \cup \{id\}) \rightarrow \mathcal{P}_{\text{fin}}(\mathbb{M} \cup \{id\})$ s.t. $\mathcal{M} \triangledown \mathcal{N}$ forms a (terminating) basis of modalities $\{\mathcal{R} \mid \mathcal{M} \Rrightarrow \mathcal{R}, \mathcal{N} \Rrightarrow \mathcal{R}\}$. The cut-rule is then:

$$\frac{\Phi\ |_{\mathcal{M}}\ \Gamma, A \Vdash \Delta \qquad \Phi'\ |_{\mathcal{N}}\ \Gamma' \Vdash \Delta', A \qquad \mathcal{R} \in \mathcal{M} \triangledown \mathcal{N}}{\Phi, \Phi'\ |_{\mathcal{R}}\ \Gamma \cup \Gamma' \Vdash \Delta \cup \Delta'}$$

Forward Search Rules

Initiation:

$$\frac{?\top}{\Vdash \top} \qquad \frac{!\bot \qquad ?A}{\bot \Vdash A}$$

$$\frac{!(A \wedge B)}{A \wedge B \Vdash A \qquad A \wedge B \Vdash B \qquad !A \qquad !B} \qquad \frac{?(A \wedge B)}{A, B \Vdash A \wedge B \qquad ?A \qquad ?B}$$

$$\frac{!(A \vee B)}{A \vee B \Vdash A, B \qquad !A \qquad !B} \qquad \frac{?(A \vee B)}{A \Vdash A \vee B \qquad B \Vdash A \vee B \qquad ?A \qquad ?B}$$

$$\frac{!(A \Rightarrow B)}{A, A \Rightarrow B \Vdash B \qquad ?A \qquad !B} \qquad \frac{?(A \Rightarrow B)}{B \Vdash A \Rightarrow B \qquad !A \qquad ?B}$$

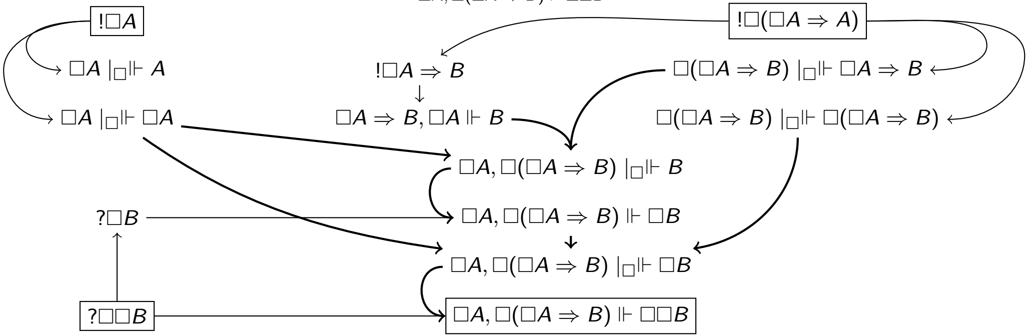
Accumulation:

$$\frac{\Phi \mid_{\mathcal{M}} \Gamma, A \Vdash \Delta \qquad \Phi' \mid_{\mathcal{N}} \Gamma' \Vdash \Delta', A \qquad \mathcal{R} \in \mathcal{M} \nabla \mathcal{N}}{\Phi \cup \Phi' \mid_{\mathcal{R}} \Gamma \cup \Gamma' \Vdash \Delta \cup \Delta'}$$

$$\frac{\Phi \mid_{\mathcal{M}} \Gamma, A \Vdash A \Rightarrow B}{\Phi \mid_{\mathcal{M}} \Gamma \Vdash A \Rightarrow B} \qquad \frac{\Phi \mid_{\mathcal{N}} \cdot \Vdash A \qquad ?\mathcal{M}A \qquad \mathcal{N} \Rrightarrow \mathcal{M} \text{ or } \mathcal{N} = id}{\Phi \Vdash \mathcal{M}A}$$

Example Search

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\Box A, A, \Box(\Box A \Rightarrow B), \Box A \Rightarrow B \vdash \Box A}\,(\mathrm{Id}) \qquad \dfrac{}{\Box A, A, \Box(\Box A \Rightarrow B), \Box A \Rightarrow B, B \vdash B}\,(\mathrm{Id})}{\Box A, A, \Box(\Box A \Rightarrow B), \Box A \Rightarrow B \vdash B}\,(\Rightarrow\mathrm{L})}{\Box A, A, \Box(\Box A \Rightarrow B), \Box A \Rightarrow B \vdash \Box B}\,(\mathrm{Mod})}{\Box A, \Box(\Box A \Rightarrow B) \vdash \Box\Box B}\,(\mathrm{Mod})
$$



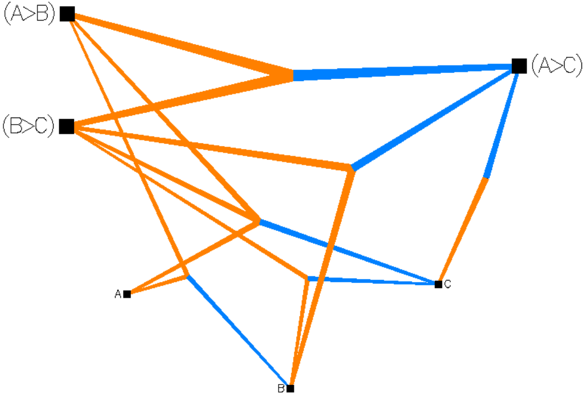
Final Remarks

Haskell Implementation

```
----------from-----------
!  B{a}((<b>=><c>))
!  B{a}((B{a}(<c>)=><d>))
------we can derive------
?  (B{a}(<b>)=>B{a}(<d>))
```

```
Lambda B{a}(<b>)
| Lock B{a}
| >| Apply
| >| | Key [B{a}]
| >| | <| Use B{a}((B{a}(<c>)=><d>))
| >| | Lock B{a}
| >| | >| Apply
| >| | >| | Key [B{a},B{a}]
| >| | >| | <<| Use B{a}((<b>=><c>))
| >| | >| | Key [B{a},B{a}]
| >| | >| | <<| Use B{a}(<b>)
```

Visualization Attempt



Logic Extensions

Add *Consistency axioms* $\mathcal{M}\bot \Rightarrow \bot$:

1. For decidability, include the rule: $\frac{\mathcal{M}^{-1}\Gamma \vdash \bot}{\Gamma \vdash A}$
2. For forward proof search, assert $?\mathcal{M}\bot$, $?\bot$, and $\mathcal{M}\bot \Vdash \bot$.

Add *Unitality axioms* of the form $X \Rightarrow \mathcal{M}X$:

1. For decidability, add Γ to $\mathcal{M}^{-1}\Gamma$.
2. For forward proof search, let $A \Vdash \mathcal{M}A$ whenever $?\mathcal{M}A$.

Further Work

To create countermodels via formulating Kripke worlds based on sets of assumptions. See [2] for countermodels in related multimodal logics.

To export generated proofs to modal dependent type theory [3].

Selected References I

[1] Frank Pfenning. "Structural Cut Elimination: I. Intuitionistic and Classical Logic". In: *Information and Computation* 157.1 (2000), pp. 84–141. ISSN: 0890-5401. DOI: `10.1006/inco.1999.2832`.

[2] Deepak Garg, Valerio Genovese, and Sara Negri. "Countermodels from Sequent Calculi in Multi-Modal Logics". In: *2012 27th Annual IEEE Symposium on Logic in Computer Science*. 2012, pp. 315–324. DOI: `10.1109/LICS.2012.42`.

[3] Lars Birkedal et al. "Modal dependent type theory and dependent right adjoints". In: *Mathematical Structures in Computer Science* 30 (2018), pp. 118 –138. DOI: `10.1017/S0960129519000197`.

The End

Time for questions

