# Proceedings of the Workshop on Intuitionistic Modal Logic and Applications (IMLA'08)

Valeria dePaiva Aleks Nanevski
(editors)

23 June, 2008

Technical Report
MSR-TR-2008-90

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
http://www.research.microsoft.com

# On Constructive Linear-Time Temporal Logic

Kensuke Kojima[1] and Atsushi Igarashi[2]

*Graduate School of Informatics*
*Kyoto University*
*Kyoto, Japan*

**Abstract**

In this paper we study a version of constructive linear-time temporal logic (LTL) with the "next" temporal operator. The logic is originally due to Davies, who has shown that the proof system of the logic corresponds to a type system for binding-time analysis via the Curry-Howard isomorphism. However, he did not investigate the logic itself in detail; he has proved only that the logic augmented with negation and classical reasoning is equivalent to (the "next" fragment of) the standard formulation of classical linear-time temporal logic. We give natural deduction and Kripke semantics for constructive LTL with conjunction and disjunction, and prove soundness and completeness. Distributivity of the "next" operator over disjunction "$\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$" is rejected from a computational viewpoint. We also give a formalization by sequent calculus and its cut-elimination procedure.

*Keywords:* constructive linear-time temporal logic, Kripke semantics, sequent calculus, cut elimination

## 1 Introduction

Temporal logic is a family of (modal) logics in which the truth of propositions may depend on time, and is useful to describe various properties of state transition systems. Linear-time temporal logic (LTL, for short), which is used to reason about properties of a fixed execution path of a system, is temporal logic in which each time has a unique time that follows it.

In this paper, we study a constructive propositional LTL with only the "next" temporal operator $\bigcirc$. Our contributions are (1) to give a Kripke semantics and a complete proof system for constructive LTL and (2) to give another formalization by sequent calculus in which cut elimination holds.

Intuitionistic versions of LTL have been already considered in the literature [12,6]. However, a characteristic feature of our version of LTL is that the "distributivity law" $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$, is *not* admitted in our logic, while (to our knowledge) it is admitted in the other formalizations as well as in the classical setting.

[1] Email: kozima@kuis.kyoto-u.ac.jp
[2] Email: igarashi@kuis.kyoto-u.ac.jp

The motivation not to admit the distributive law above comes from the type-theoretic interpretation of $\bigcirc$ operator, first given by Davies [4]. He pointed out that a proof system of LTL can be related to a type system of (multi-level) binding-time analysis, which is used in offline partial evaluation [10] to determine which part of a program can be computed at specialization-time and which is residualized. According to this correspondence, a formula $\bigcirc A$, which means that $A$ holds at the next time, is interpreted as a type of (residual) *code* of type $A$; introduction and elimination rules of $\bigcirc$ are as Lisp-like quasiquotation and unquote, respectively. As a result, $\lambda^{\bigcirc}$ terms can be considered as program-generating programs, such as parser generators or generating extensions, which manipulate code fragments by the quasiquotation mechanism. For example, a parser generator would have a type like $\texttt{parser\_spec} \to \bigcirc(\texttt{string} \to \texttt{syntax\_tree})$. Now, a proof of the distributive law would be considered a function which takes a value of type $\bigcirc(A \vee B)$ and returns a value of type $\bigcirc A \vee \bigcirc B$. While a value of the return type must be of type $\bigcirc A$ or type $\bigcirc B$ with a tag indicating which of the two is actually the case, a value of the argument type is *quoted* code, which will not be executed *until the next time comes*, that is, until the residual code is executed; it is in general impossible to know which value ($A$ or $B$) this code evaluates to *now* (unless a Lisp-like eval function was available). From this observation, we conclude that there is no method to turn a value of type $\bigcirc(A \vee B)$ into a value of type $\bigcirc A \vee \bigcirc B$, and hence $\bigcirc A \vee \bigcirc B$ should be strictly stronger than $\bigcirc(A \vee B)$.

Davies defined a natural deduction system for a constructive LTL with only the "next" operator $\bigcirc$ and implication, derived via the Curry-Howard isomorphism a typed $\lambda$-calculus $\lambda^{\bigcirc}$, which was formally shown to be equivalent to a type system of multi-level binding-time analysis by Glück and Jørgensen [8]. Unfortunately, however, Davies did not investigate his system in detail, from a logical point of view: he proved only that his system augmented with negation and classical reasoning is equivalent to the *classical* LTL, even though the logic can be considered a *constructive* version of LTL. The main aim of this paper is to see how his system is formalized in terms of Kripke semantics and sequent calculus. Davies' original system is an implicational fragment, but we also consider conjunction and disjunction. [3]

The organization of the rest of this paper is as follows. In Section 2, we discuss an implicational fragment: we first review the natural deduction by Davies, give a Kripke semantics, obtained by a natural extension of that of the classical LTL, and finally prove soundness and completeness of the proof system. We also discuss that, unfortunately, a straightforward extension of the semantics to disjunction is not suitable for our interpretation of disjunction. In Section 3 we extend the logic with conjunction and disjunction. We give another Kripke semantics, which does not admit the distributivity law mentioned above, and prove soundness and completeness of the proof system. In Section 4 we define a sequent calculus $\mathrm{LJ}^{\bigcirc}$, which is equivalent to the natural deduction, with its cut elimination procedure. Finally, we give concluding remarks in Section 5.

[3] Precisely speaking, Davies extended $\lambda^{\bigcirc}$ with pairing and natural numbers, but did not consider conjunction or disjunction in his logic.

$$\frac{}{\Gamma, A^n \vdash A^n}\ (\text{Axiom}) \qquad \frac{\Gamma \vdash A \supset B^n \qquad \Gamma \vdash A^n}{\Gamma \vdash B^n}\ (\supset\text{E}) \qquad \frac{\Gamma, A^n \vdash B^n}{\Gamma \vdash A \supset B^n}\ (\supset\text{I})$$

$$\frac{\Gamma \vdash \bigcirc A^n}{\Gamma \vdash A^{n+1}}\ (\bigcirc\text{E}) \qquad \frac{\Gamma \vdash A^{n+1}}{\Gamma \vdash \bigcirc A^n}\ (\bigcirc\text{I})$$

Fig. 1. Derivation Rules of Davies' System.

## 2 Implicational Fragment

In this section, we first recall the natural deduction system by Davies and some of its properties, define a Kripke semantics for it, and prove completeness of Davies' system.

### *2.1 Results by Davies*

The temporal logic Davies considered contains only $\bigcirc$ ("next" operator) and $\supset$ (intuitionistic implication), so the language we consider in this section is constructed from propositional variables using $\supset$ and $\bigcirc$.

A judgment in his system takes the form

$$A_1^{n_1}, \ldots, A_k^{n_k} \vdash B^m$$

where $A_i, B$ are formulas and $n_i, m$ are natural numbers; it is read "$B$ holds at time $m$ under the assumption that $A_i$ holds at time $n_i$ (for $i = 1, \ldots, k$)." In what follows, we use $A, B, C, D$ for formulas, $k, l, m, n$ for natural numbers, $F, G$ for annotated formulas (i.e. formulas with time annotation), and $\Gamma, \Delta$ for sets of annotated formulas. We consider the left-hand side of a judgment a set.

Inference rules of Davies' system are listed in Fig. 1. The rules $\supset$I, $\supset$E, and Axiom are standard. The other two, the introduction and elimination rules for $\bigcirc$ operator, state that $A$ holds at time $n+1$ if and only if $\bigcirc A$ holds at time $n$. This is quite natural since $\bigcirc A$ means that "$A$ holds at the next time." This system is obtained from intuitionistic K, given by Martini and Masini [13] (aside from a few notational differences), whose introduction rule for modality has a side condition that all time annotations in the context must be smaller than $n+1$ (the time annotation of the succedent of the premise).

To show that $\bigcirc$ operator in this system is indeed the "next" operator in linear-time temporal logic, Davies compared his system with $L^{\bigcirc}$, a well-known Hilbert-style proof system of the fragment of classical linear-time temporal logic consisting of only implication, negation and next operators. The axiomatization is given by Stirling, who also proved that $L^{\bigcirc}$ is sound and complete for the standard semantics [19]. The axioms and rules of $L^{\bigcirc}$ are as follows:

**Axioms** • any classical tautology instance
- $\bigcirc\neg A \supset \neg \bigcirc A$
- $\neg \bigcirc A \supset \bigcirc\neg A$
- $\bigcirc(A \supset B) \supset \bigcirc A \supset \bigcirc B$

**Rules** • if $A \supset B$ and $A$ then $B$

- if $A$ then $\bigcirc A$

Davies proved that his system extended by negation and classical reasoning is equivalent to $L^{\bigcirc}$ in the following sense [4]:

**Proposition 2.1** *A judgment $A_1^{n_1}, \ldots, A_k^{n_k} \vdash B^m$ is provable in the extended system if and only if $\bigcirc^{n_1} A_1 \supset \ldots \supset \bigcirc^{n_k} A_k \supset \bigcirc^m B$ has a proof in $L^{\bigcirc}$. In particular, $\cdot \vdash A^0$ is provable if and only if $A$ is a theorem of $L^{\bigcirc}$.*

### *2.2 Kripke Semantics via Functional Frames*

Before discussing the semantics of the implicational fragment, we briefly explain how the usual classical semantics is given in terms of Kripke semantics. Kripke frames we consider are *functional*, in the sense that the accessibility relation $R$ on possible worlds is a map.[4] This condition guarantees that, in a functional frame, the next state of a given state is uniquely determined, hence justifying "linear time".

To give a semantics of constructive LTL, we follow the previous researches on Kripke-style models of intuitionistic modal logics [1,23,3] and augment functional frames by another accessibility relation $\leq$. This additional accessibility represents the "constructive" counterpart, as in the standard semantics of intuitionistic logic.

**Definition 2.2** *An* intuitionistic functional frame *is a triple $\langle W, \leq, R\rangle$ of a nonempty set $W$, a preorder $\leq$ on $W$ and a map $R$ from $W$ to $W$ such that $\leq \circ R = R \circ \leq$ holds. Here $\circ$ stands for a composition of binary relations defined by $x\ R \circ S\ y \iff \exists z.(x\ R\ z\ S\ y)$.*

This notion is an extension of classical functional frames: if $\leq$ is the diagonal relation (that is, $x \leq y$ if and only if $x = y$) in this definition, the frame $\langle W, \leq, R\rangle$ can be identified with a classical functional frame $\langle W, R\rangle$. Hereafter, we simply say functional frame when no confusion arises.

Using functional frames we can define a satisfaction relation on formulas.

**Definition 2.3** *Let $\langle W, \leq, R\rangle$ be a functional frame and $\models$ be a binary relation between $W$ and the set of propositional variables such that $w \leq w'$ and $w \models p$ imply $w' \models p$. We extend $\models$ to formulas by induction with*

- *$w \models A \supset B \iff$ if $w \leq w'$ and $w' \models A$ then $w' \models B$, and*
- *$w \models \bigcirc A \iff$ if $w\ R\ w'$ then $w' \models A$.*

*We also write $w \models A^n$ for $w \models \bigcirc^n A$.*

This definition is one of the standard semantics of intuitionistic modal logics previously considered [23]. As is easily verified by induction on the construction of formulas, this semantics satisfies the monotonicity condition.

**Lemma 2.4** *If $w \leq w'$ and $w \models A$, then $w' \models A$.*

It is not very difficult to see that Davies' system is sound and complete for this semantics. Soundness is proved by straightforward induction on the derivation.

[4] The term "functional" is, to our knowledge, first used by Segerberg [18] (but not in context of semantics of LTL).

Completeness is proved by constructing a functional frame in which validity and provability coincide. We sketch the proof below.

For a set $T$ of formulas, we write $\bigcirc^{-1}T$ for the set $\{A \mid \bigcirc A \in T\}$ and $\bigcirc T$ for $\{\bigcirc A \mid A \in T\}$. Take the set of all theories as $W$, let $\leq$ be a set-inclusion, and $R$ the map which sends each theory $T$ to the theory $\bigcirc^{-1}T$. First we show that this defines a functional frame.

**Lemma 2.5** *The canonical frame $\langle W, \leq, R\rangle$ above is indeed functional.*

**Proof.** Among conditions of being a functional frame, the only nontrivial one is $R \circ \leq \subseteq \leq \circ R$. To show this, take theories $T$ and $S$ with $\bigcirc^{-1}T \subseteq S$ (i.e. $T$ $(R \circ \leq)$ $S$), and let $U$ be the smallest theory containing $T$ and $\bigcirc S$. We are going to show that $U$ satisfies $T \leq U\ R\ S$, i.e. $T \subseteq U$ and $\bigcirc^{-1}U = S$.

Clearly, $T \subseteq U$ holds by definition. It is also easy to see that $S \subseteq \bigcirc^{-1}U$: if $A \in S$, then $\bigcirc A \in \bigcirc S \subseteq U$, and from this $A \in \bigcirc^{-1}U$ follows. For the converse, let $A$ be a formula in $\bigcirc^{-1}U$. Then we have $\bigcirc A \in U$. Since $U$ is the smallest theory containing $T$ and $\bigcirc S$, there exist formulas $A_1, \ldots, A_n \in S$ such that $\bigcirc A_1 \supset \ldots \supset \bigcirc A_n \supset \bigcirc A \in T$. Because $\bigcirc(A \supset B)$ follows from $\bigcirc A \supset \bigcirc B$, we also have $\bigcirc(A_1 \supset \ldots \supset A_n \supset A) \in T$. This implies that $A_1 \supset \ldots \supset A_n \supset A \in \bigcirc^{-1}T \subseteq S$ holds. As $A_i \in S$ from the assumption, we conclude that $A \in S$, as required. □

Let $\models$ be the satisfaction relation defined by: $T \models p$ if and only if $p \in T$. Then it holds that $T \models A$ if and only if $A \in T$ for each formula $A$, which is easily verified by induction on $A$. Finally, if $\Gamma \vdash A^n$ is not provable, take the set $\left\{A \,\middle|\, \Gamma \vdash A^0\right\}$ as $T$. Then $T \models \Gamma$ holds but $T \models A^n$ does not.

### *2.3 A Problem with Disjunction*

The proof strategy above is almost standard, but notice that we took the set of all theories as $W$. When we consider the full system (in particular, disjunction), the same method will not work. In the presence of disjunction, the standard way to prove completeness is to take the set of all *prime* theories.[5] Otherwise, we cannot prove the equivalence of $T \models A$ and $A \in T$ in the last step of the proof above. However, if we give $W$ in this way, there is no natural way to define suitable $R$ because the theory $\bigcirc^{-1}T$ is not necessarily prime even if $T$ is prime.

In fact, functional frames are not appropriate in the presence of disjunction because they would validate the distributivity law $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$, which we reject as discussed in the introduction, under the straightforward interpretation of disjunction:

$$w \models A \vee B \iff \text{if } w \models A \text{ or } w \models B$$

It does not seem easy to adjust the definition of the satisfaction relation to exclude the distributivity law. In fact, since necessity and possibility coincide when $R$ is a (total) map, it may appear natural to adopt the ideas from some of the Kripke semantics for intuitionistic modal logics [22,1], which rejects distributivity

[5] A theory $T$ is said to be prime if $A \vee B \in T$ implies $A \in T$ or $B \in T$.

$$\frac{\Gamma \vdash A \wedge B^n}{\Gamma \vdash A^n}\ (\wedge\mathrm{E1}) \qquad \frac{\Gamma \vdash A \wedge B^n}{\Gamma \vdash B^n}\ (\wedge\mathrm{E2}) \qquad \frac{\Gamma \vdash A^n \qquad \Gamma \vdash B^n}{\Gamma \vdash A \wedge B^n}\ (\wedge\mathrm{I})$$

$$\frac{\Gamma \vdash A^n}{\Gamma \vdash A \vee B^n}\ (\vee\mathrm{I1}) \qquad \frac{\Gamma \vdash B^n}{\Gamma \vdash A \vee B^n}\ (\vee\mathrm{I2})$$

$$\frac{\Gamma \vdash A \vee B^n \qquad \Gamma, A^n \vdash C^n \qquad \Gamma, B^n \vdash C^n}{\Gamma \vdash C^n}\ (\vee\mathrm{E})$$

Fig. 2. Additional Rules for Full NJ$^{\bigcirc}$

$\Diamond(A \vee B) \supset \Diamond A \vee \Diamond B$ of possibility over disjunction by:

$$w \models \Diamond A \iff \forall v.(w \leq v \implies \exists w'.(v\ R\ w' \wedge w' \models A)).$$

Unfortunately, this attempt fails. To falsify the distributivity we also need to have $\leq \circ R \not\subseteq R \circ \leq$, but then, the formula $(\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$ becomes invalid. Indeed, consider a functional frame $\langle W, \leq, R\rangle$ defined by $W = \{a, b, c, d\}$ and $\leq\ = \{(a,b),(a,a),(b,b),(c,c),(d,d)\}$ and $R = \{(a,c),(b,d),(c,c),(d,d)\}$ and the satisfaction relation such that $A$ is true at $c$ and false at $d$, and $B$ is false at $c$. Then, $a \models \bigcirc A \supset \bigcirc B$ holds but $a \models \bigcirc(A \supset B)$ does not.

From the observation above, it seems that the combination of functionality of $R$ and soundness leads to the distributivity. In the next section we give a larger class of frames, by relaxing the functionality condition.

# 3 Full System: Natural Deduction and Kripke Semantics

In the previous section we have seen that the notion of functional frames is too naive to represent the intuitive meaning of the $\bigcirc$ operator we consider. In this section we propose a more suitable class of Kripke frames and a complete proof system.

## *3.1 Natural Deduction*

First we define a natural deduction system NJ$^{\bigcirc}$ extending Davies' system, by adding conjunction and disjunction. Derivation rules for these two connectives are listed in Fig. 2. They are fairly straightforward, but only $\vee$E may be nontrivial. In this rule, the formula being eliminated must have the same time as the succedent of the conclusion. At first sight it may seem strange, but in fact this restriction is essential for our system. Indeed, without this restriction we could prove the distributivity law $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$, which should not be a tautology as mentioned above, as follows:

$$\dfrac{\dfrac{\dfrac{\bigcirc(A \vee B)^0, A^1 \vdash A^1}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A^0}}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A \vee \bigcirc B^0} \quad \dfrac{\dfrac{\bigcirc(A \vee B)^0, B^1 \vdash B^1}{\bigcirc(A \vee B)^0, B^1 \vdash \bigcirc B^0}}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A \vee \bigcirc B^0} \quad \dfrac{\bigcirc(A \vee B)^0 \vdash \bigcirc(A \vee B)^0}{\bigcirc(A \vee B)^0 \vdash A \vee B^1}}{\bigcirc(A \vee B)^0 \vdash \bigcirc A \vee \bigcirc B^0}\ \vee\mathrm{E}$$

In this proof, disjunction being eliminated has time 1 while the time of the succedent is 0. In fact, the problem would occur only if we allowed the time of the succedent

$C$ to be strictly less than that of the disjunction $A \vee B$ being eliminated. (A slight variation of $\vee$E in which $C^n$ is changed to $C^m$ with the side condition $m \geq n$ is provable by using $\bigcirc$I and $\bigcirc$E.)

### *3.2 Kripke Semantics*

As discussed above, the proof system NJ$^{\bigcirc}$ does not seem to prove distributivity law, so we think the logic defined by NJ$^{\bigcirc}$ is more appropriate than that by functional frames. Therefore the next question is what kind of frames correspond to our logic. The answer we give is $\bigcirc$-frames, defined below.

**Definition 3.1** *A $\bigcirc$-frame is a triple $\langle W, \leq, R\rangle$ of a nonempty set $W$, a preorder $\leq$ on $W$ and a binary relation $R$ on $W$ such that*

- $\leq \circ R = R \circ \leq = R$, *and*
- *if $w\ R\ v$ then there exists $w'$ such that $w \leq w'$ and $\forall u \in W.(w'\ R\ u \iff v \leq u)$.*

Note that, here, $R$ is not assumed to be a map. This definition is essentially a special case of Kripke IM-frames considered by Wolter and Zakharyaschev [23]. [6]

Satisfaction relations are defined in the same way as the functional frame semantics in Section 2, but we need to add the following two clauses for disjunction and conjunction.

- $w \models A \vee B \iff w \models A$ or $w \models B$
- $w \models A \wedge B \iff w \models A$ and $w \models B$

This $\bigcirc$-frame semantics is a generalization of the functional one:

**Proposition 3.2** *For an arbitrary functional frame $\mathcal{F} = \langle W, \leq, R\rangle$, there exists a binary relation $R'$ such that the frame $\mathcal{F}' = \langle W, \leq, R'\rangle$ is a $\bigcirc$-frame, and for each satisfaction relation $\models$ on $W$ its extensions on $\mathcal{F}$ and $\mathcal{F}'$ coincide.*

**Proof.** Let $R' = R \circ \leq$ (in other words, $w\ R'\ v$ if and only if $u \leq v$, where $u$ is the image of $R$ at $w$). Then $\leq \circ R' = R' \circ \leq = R'$ is easily verified from $\leq \circ R = R \circ \leq$ and transitivity of $\leq$. The latter part is proved by induction on the formula. □

**Theorem 3.3 (Soundness)** *Suppose that $\Gamma \vdash A^n$ is provable in* NJ$^{\bigcirc}$. *Then for any $\bigcirc$-frame $\langle W, \leq, R\rangle$, satisfaction relation $\models$, and possible world $w \in W$ such that $w \models \Gamma$, it holds that $w \models A^n$.*

**Proof.** Induction on the derivation. □

**Theorem 3.4 (Completeness)** *If $w \models \Gamma$ implies $w \models A^n$ for any $\bigcirc$-frame $\langle W, \leq, R\rangle$, satisfaction relation $\models$, and possible world $w \in W$, then there exists a derivation of $\Gamma \vdash A^n$.*

**Proof.** Basically we proceed in a way similar to the proof in Section 2, but we need some modification. Here we take the set of all *prime* theories as $W$, and define accessibility relation $R$ so that $T\ R\ T'$ holds if and only if $\bigcirc^{-1}T \subseteq T'$.

[6] It may sound strange that $\bigcirc$ does not distribute over disjunction in $\bigcirc$-frames, when it is known that the distributivity law of $\Diamond$ over disjunction holds in any IM-frame. This is not a contradiction, however, because we regard $\bigcirc$ as necessity $\Box$ rather than possibility $\Diamond$.

$$\frac{(A \text{ is atomic})}{\Gamma, A^n \Rightarrow A^n}\ (\text{Init}) \qquad \frac{\Gamma \Rightarrow F \qquad F, \Delta \Rightarrow G}{\Gamma, \Delta \Rightarrow G}\ (\text{Cut})$$

$$\frac{\Gamma \Rightarrow A^n \qquad \Gamma, B^n \Rightarrow F}{\Gamma, A \supset B^n \Rightarrow F}\ (\supset\text{L}) \qquad \frac{\Gamma, A^n \Rightarrow B^n}{\Gamma \Rightarrow A \supset B^n}\ (\supset\text{R})$$

$$\frac{\Gamma, A^n \Rightarrow F}{\Gamma, A \wedge B^n \Rightarrow F}\ (\wedge\text{L1}) \qquad \frac{\Gamma \Rightarrow A^n \qquad \Gamma \Rightarrow B^n}{\Gamma \Rightarrow A \wedge B^n}\ (\wedge\text{R})$$

$$\frac{\Gamma, B^n \Rightarrow F}{\Gamma, A \wedge B^n \Rightarrow F}\ (\wedge\text{L2}) \qquad \frac{\Gamma \Rightarrow A^n}{\Gamma \Rightarrow A \vee B^n}\ (\vee\text{R1})$$

$$\frac{\Gamma, A^n \Rightarrow C^{n+m} \qquad \Gamma, B^n \Rightarrow C^{n+m}}{\Gamma, A \vee B^n \Rightarrow C^{n+m}}\ (\vee\text{L}) \qquad \frac{\Gamma \Rightarrow B^n}{\Gamma \Rightarrow A \vee B^n}\ (\vee\text{R2})$$

$$\frac{\Gamma, A^{n+1} \Rightarrow F}{\Gamma, \bigcirc A^n \Rightarrow F}\ (\bigcirc\text{L}) \qquad \frac{\Gamma \Rightarrow A^{n+1}}{\Gamma \Rightarrow \bigcirc A^n}\ (\bigcirc\text{R})$$

Fig. 3. Inference Rules of $\text{LJ}^{\bigcirc}$.

The only nontrivial point in the proof is that $\langle W, \leq, R\rangle$ defined above is indeed a $\bigcirc$-frame. The condition $\leq \circ R = R \circ \leq = R$ is not difficult to prove, and we omit the details. Below we prove that the other condition is satisfied. Let $S$ and $T$ be prime theories such that $T\ R\ S$ (i.e. $\bigcirc^{-1}T \subseteq S$). Our goal is to prove that there exists some prime theory $U$ such that $T \subseteq U$ and $\forall V \in W.(\bigcirc^{-1}U \subseteq V \iff S \subseteq V)$. Let $X$ be the set of theories defined by:

$$X = \left\{ U \;\middle|\; U \text{ is a theory such that } \bigcirc^{-1}U = S \text{ and } T \subseteq U \right\}.$$

We are going to show that $X$ is not empty, and its maximal element is a prime theory. For the former, take the smallest theory containing $T$ and $\bigcirc S$ and show that it belongs to $X$. This is done in the same way as in the last section. To prove the latter, let $U \in X$ be a maximal element and suppose $A_1, A_2 \notin U$. Moreover, let $U_0, U_1, U_2$ be the smallest theory containing $A_1 \vee A_2, A_1, A_2$, respectively, and $U$. It is sufficient to prove that $U_0 \neq U$. For $i = 1, 2$ the theory $\bigcirc^{-1}U_i$ is a proper extension of $\bigcirc^{-1}U = S$, so there exists a formula $B_i \in \bigcirc^{-1}U_i \setminus S$. For such $B_1$ and $B_2$, it holds that $\bigcirc(B_1 \vee B_2) \in U_1 \cap U_2 = U_0$ and $B_1 \vee B_2 \notin S = \bigcirc^{-1}U$ (because $S$ is prime). Therefore we obtain $\bigcirc(B_1 \vee B_2) \in U_0 \setminus U$, and this implies $U_0 \neq U$, as required.

The rest of the proof is almost the same as the previous one. □

# 4 Sequent Calculus

In this section we give another formalization $\text{LJ}^{\bigcirc}$ of our logic in the sequent calculus style. After verifying that the system $\text{LJ}^{\bigcirc}$ is equivalent to $\text{NJ}^{\bigcirc}$ previously defined, we give a cut-elimination procedure for $\text{LJ}^{\bigcirc}$.

## *4.1 Formalization*

Sequents of $\text{LJ}^{\bigcirc}$ have the form $\Gamma \Rightarrow F$ where $\Gamma$ is a set of annotated formulas and $F$ is an annotated formula. Inference rules of $\text{LJ}^{\bigcirc}$ are listed in Fig. 3.

Since we regard the left-hand side of a sequent as a set, exchange and contraction rules are not explicitly included. There is not an explicit weakening rule, either—we included weakening implicitly by allowing extra formulas in the left-hand side of the initial sequents. To make the proof of cut elimination theorem simpler, we restricted the right-hand side of the initial sequents to be atomic (but this does not reduce the proof-theoretic strength). Most of the rest of the rules are standard, but we comment on the rule $\vee$L. In this rule, the time of the succedent $C$ must be no less than that of the principal formula $A \vee B$. This corresponds to the issue mentioned in the previous section that we cannot eliminate disjunction with a succedent of an earlier time.

LJ$^{\bigcirc}$ is equivalent to NJ$^{\bigcirc}$ in the following sense:

**Theorem 4.1** *A sequent $\Gamma \Rightarrow F$ is provable in* LJ$^{\bigcirc}$ *if and only if $\Gamma \vdash F$ is provable in* NJ$^{\bigcirc}$.

To prove this it is sufficient to check that all rules of LJ$^{\bigcirc}$ are admissible in NJ$^{\bigcirc}$ and vice versa. For the former part we need the admissibility of weakening and cut in natural deduction:

**Lemma 4.2** (i) *If $\Gamma \vdash F$ is provable, then $\Gamma, \Delta \vdash F$ is also provable.*

(ii) *If $\Gamma \vdash F$ and $F, \Delta \vdash G$ are provable, then $\Gamma, \Delta \vdash G$ is also provable.*

Then, both directions are proved by easy induction, so we omit the details.

### *4.2 Cut Elimination Procedure*

Next we show cut is admissible in the cut-free fragment of LJ$^{\bigcirc}$.

**Theorem 4.3** *If $\Gamma \Rightarrow F$ and $F, \Delta \Rightarrow G$ are provable without cut, then $\Gamma, \Delta \Rightarrow G$ is also provable without cut.*

We sketch the proof below. Consider the cut

$$\dfrac{\mathcal{D}_1 = \dfrac{\vdots}{\Gamma \Rightarrow F}\, R_1 \qquad \mathcal{D}_2 = \dfrac{\vdots}{F, \Delta \Rightarrow G}\, R_2}{\Gamma, \Delta \Rightarrow G}\ \mathrm{Cut}$$

We split this into four cases:

(i) $R_1 \neq \vee$L or $R_2 = $ Init;

(ii) $R_1 = \vee$L and $F$ is not principal in $\mathcal{D}_2$;

(iii) $R_1 = R_2 = \vee$L and $F$ is principal in $\mathcal{D}_2$;

(iv) $R_1 = \vee$L, $F$ is principal in $\mathcal{D}_2$, and $F$ is neither atomic nor disjunction.

The standard cut-elimination procedure works in case (i), but in the other cases, i.e. $R_1 = \vee$L, it is not as obvious. The problem stems from the side condition on the time on the pricipal formula and that on the succedent in $\vee$L. Consider the

most general form of cut with $R_1 = \vee\mathrm{L}$:

$$\dfrac{\dfrac{\Gamma, A^n \Rightarrow C^m \quad \Gamma, B^n \Rightarrow C^m}{\Gamma, A \vee B^n \Rightarrow C^m}\ \vee\mathrm{L} \quad C^m, \Delta \Rightarrow D^l}{\Gamma, A \vee B^n, \Delta \Rightarrow D^l}\ \mathrm{Cut}$$

Applying the standard procedure to this derivation, we would obtain a new derivation

$$\dfrac{\dfrac{\Gamma, A^n \Rightarrow C^m \quad C^m, \Delta \Rightarrow D^l}{\Gamma, A^n, \Delta \Rightarrow D^l}\ \mathrm{Cut} \quad \dfrac{\Gamma, B^n \Rightarrow C^m \quad C^m, \Delta \Rightarrow D^l}{\Gamma, B^n, \Delta \Rightarrow D^l}\ \mathrm{Cut}}{\Gamma, A \vee B^n, \Delta \Rightarrow D^l}\ \vee\mathrm{L}$$

which, however, is not always valid, because it is not necessarily the case that $l \geq n$. So, we split this case into the three subcases, (ii), (iii), and (iv) listed above.

In case (ii) it is easy to reduce the cut into a simpler one: as the cut formula is not principal in $\mathcal{D}_2$, it occurs in all premises of $R_2$, so we just lift the cut into $\mathcal{D}_2$.

In case (iii), we can use the standard procedure above because the condition $n \leq l$ is always met.

The last case is the case (iv), in which $F$ is neither atomic nor disjunction. In this case, first rewrite a given derivation $\mathcal{D}_1$ into another derivation $\mathcal{D}_1'$ of the same sequent such that the new derivation ends with a right rule application. Then, the given cut becomes a principal cut, which is easily reduced into a simpler cut. To do this, all we need is the following lemma:

**Lemma 4.4** *If a sequent $S \equiv \Gamma \Rightarrow F$ has a cut-free derivation $\mathcal{D}$ and $F$ is neither atomic formula nor disjunction, then there exists a cut-free derivation $\mathcal{D}'$ of $S$ such that the last rule used in $\mathcal{D}'$ is a right rule.*

**Proof.** It is sufficient to show that any use of a left rule immediately following a right rule other than the $\vee$-right rules can be replaced by applications of the right rule following the left rule. Intuitively this means that by a conversion like

$$\dfrac{\dfrac{T_1 \quad \ldots \quad T_k}{S'}\ \mathrm{Right}}{S}\ \mathrm{Left} \quad \Longrightarrow \quad \dfrac{\dfrac{T_1}{S_1'}\ \mathrm{Left} \quad \ldots \quad \dfrac{T_k}{S_k'}\ \mathrm{Left}}{S}\ \mathrm{Right}$$

we always obtain a valid derivation from a valid derivation. This is done by straightforward case analysis. □

From the argument above, we obtain the cut-elimination theorem for $\mathrm{LJ}^{\bigcirc}$.

**Theorem 4.5** *If a sequent is provable in $\mathrm{LJ}^{\bigcirc}$, then it has a cut-free proof.*

## 5 Concluding Remarks

In this paper we have defined a Kripke semantics for constructive LTL, a sound and complete natural deduction style proof system, and a sequent calculus which enjoys a cut elimination theorem.

Although the temporal logic we considered is *linear-time*, a naive frame condition of functionality turned out to be insufficient, and we used a larger class of Kripke frames. Compared to other modal logics such as S4 and lax logic, an intuitive meaning of the frame condition we presented is not so clear, but it seems to correspond to the fact that the inverse of axiom **K** is a theorem.

For a cut elimination procedure, we basically followed the standard method. However, to make it work correctly, we may need extra transformations.

In this paper we did not mention algebraic semantics and duality between frames and algebras. Related to these topics, results for constructive S4 and propositional lax logic are given by Alechina et al. [1]. A similar result also holds for our constructive LTL. Let us call a lattice equipped with a unary operation $\bigcirc$ a $\bigcirc$-algebra if it has pseudo-complement $\supset$ and $\bigcirc$ preserves $\supset$. It is fairly easy to see that the $\bigcirc$-algebras derive a semantics of constructive LTL and that $\mathrm{NJ}^{\bigcirc}$ is sound and complete. In a way similar to the classical case we can define translations between $\bigcirc$-frames and $\bigcirc$-algebras. Further investigations are left for future work. On duality for intuitionistic modal logics, Wolter and Zakharyaschev [23] also gave a general result, but it does not directly give rise to duality between $\bigcirc$-frame and some class of algebras. This is because we used Kripke frames while they considered general frames.

In the context of multi-modal and intuitionistic modal logics, a notion of product of Kripke frames and general frames are considered [7,9]. We conjecture that there exists a decomposition of functional frame (and maybe $\bigcirc$-frame) into a product of frames.

Another interesting problem is to consider temporal operators other than $\bigcirc$, such as "always" or "until." It is easy to define a semantics for other temporal operators, so the main interest is how to characterize these operators in terms of proof systems. In relation with this issue, a completeness result for constructive propositional dynamic logic is given by Nishimura [17]. Dynamic logic has operators similar to temporal operators, including "next" operator, so we think there are some relationship between his work and ours.

Since work by Davies and Pfenning [5] and Davies [4] on Curry-Howard correspondence for modal and temporal logic, many type systems for multi-stage languages based on their work have been proposed [2,15,20,21,14,16,24,11]. Those languages typically include not only quasiquotation as in $\lambda^{\bigcirc}$ but also Lisp-like eval and lifting of values to code (also called cross-stage persistence [21]). As a result, their type systems could be seen as quite different modal logics: for example, the distributvity law would be validated if eval, which would have type $\bigcirc A \supset A$, and lifting, which would have type $A \supset \bigcirc A$, are supported in one language. The combination of these language features is motivated by a practical reason, rather than a correspondence with logics; it would also be interesting to investigate how these systems (more precisely, the corresponding logics) are characterized in terms of temporal or modal logics. (One such investigation is the second author's work [24], which tries to capture quasiquotation and eval by linear-time temporal logic with next and always modalities.)

# References


[1] Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and Kripke semantics for constructive S4 modal logic. In L. Fribourg, editor, *Proceedings 15th Int. Workshop on Computer Science Logic, CSL'01, Paris, France, 10–13 Sept. 2001*, volume 2142, pages 292–307. Springer-Verlag, Berlin, 2001.

[2] Zine El-Abidine Benaissa, Eugenio Moggi, Walid Taha, and Tim Sheard. Logical modalities and multi-stage programming. In *Proceedings of Workshop on Intuitionstic Modal Logics and Applications (IMLA'99)*, 1999.

[3] Milan Božić and Kosta Došen. Models for normal intuitionistic modal logics. *Studia Logica*, 43(3):217–245, September 1984.

[4] Rowan Davies. A temporal-logic approach to binding-time analysis. In *Proceedings of IEEE Symposium on Logic In Computer Science (LICS'96)*, pages 184–195, July 1996.

[5] Rowan Davies and Frank Pfenning. A modal analysis of staged computation. *Journal of the ACM*, 48(3):555–604, 2001.

[6] W. B. Ewald. Intuitionistic tense and modal logic. *Journal of Symbolic Logic*, 51(1):166–179, 1986.

[7] Dov M. Gabbay and Valentin B. Shehtman. Products of modal logics, part 1. *Logic Journal of the IGPL*, 6(1):73–146, January 1998.

[8] Robert Glück and Jesper Jørgensen. Efficient multi-level generating extensions for program specialization. In *Proceedings of Programming Languages, Implementations, Logics and Programs (PLILP'95)*, volume 982 of *Lecture Notes in Computer Science*, pages 259–278, 1995.

[9] Yasusi Hasimoto. *Algebras and Frames for Modal Logics*. PhD thesis, School of Information Science, Japan Advanced Institute of Science and Technology, January 2001.

[10] Neil D. Jones, Carsten K. Gomard, and Peter Sestoft. *Partial Evaluation and Automatic Program Generation*. Prentice-Hall, 1993.

[11] Ik-Soon Kim, Kwangkeun Yi, and Cristiano Calcagno. A polymorphic modal type system for Lisp-like multi-staged languages. In *Proceedings of ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL06)*, pages 257–268, Charleston, SC, January 2006.

[12] Patrick Maier. Intuitionistic LTL and a new characterization of safety and liveness. In *Proceedings of Conference of the European Association for Computer Science Logic*, volume 3210 of *Lecture Notes in Computer Science*, pages 295–309. Springer Verlag, 2004.

[13] S. Martini and A. Masini. A computational interpretation of modal proofs. In H. Wansing, editor, *Proof Theory of Modal Logics*. Kluwer, 1994.

[14] Eugenio Moggi and S. Fagorzi. A monadic multi-stage metalanguage. In *Proceedings of Conference on Foundations of Software Science and Computation Structures (FoSSaCS'03)*, volume 2620 of *Lecture Notes in Computer Science*, pages 358–374. Springer Verlag, 2003.

[15] Eugenio Moggi, Walid Taha, Zine El-Abidine Benaissa, and Tim Sheard. An idealized MetaML: Simpler, and more expressive. In *Proceedings of European Symposium on Programming (ESOP'99)*, volume 1576 of *Lecture Notes in Computer Science*, pages 193–207, 1999.

[16] Aleksandar Nanevski and Frank Pfenning. Staged computation with names and necessity. *Journal of Functional Programming*, 15(5):893–939, 2005.

[17] Hirokazu Nishimura. Semantical analysis of constructive PDL. *Publications of the Research Institute for Mathematical Sciences*, 18:847–858, 1982.

[18] Krister Segerberg. Modal logics with functional alternative relations. *Notre Dame Journal of Formal Logic*, 27(4):504–522, October 1986.

[19] Colin Stirling. Modal and temporal logics. In *Handbook of Logic in Computer Science*, pages 477–563. Oxford University Press, Inc., New York, NY, USA, 1992.

[20] Walid Taha and Michael Florentin Nielsen. Environment classifiers. In *Proceedings of ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'03)*, pages 26–37, 2003.

[21] Walid Taha and Tim Sheard. MetaML and multi-stage programming with explicit annotations. *Theoretical Computer Science*, 248:211–242, 2000.

[22] Duminda Wijesekera. Constructive modal logics I. *Annals of Pure and Applied Logic*, 50:271–301, 1990.

[23] Frank Wolter and Michael Zakharyaschev. Intiuitionistic modal logics as fragments of classical bimodal logics. *Logics at work, Essays in honour of Helena Rasiowa*, pages 168–186, 1998.

[24] Yoshihiro Yuse and Atsushi Igarashi. A modal type system for multi-level generating extensions with persistent code. In *Proceedings of 8th ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'06)*, pages 201–212, Venice, Italy, July 2006.

# Constructive rationality implies backward induction for conscientious players

René Vestergaard[a,1] Pierre Lescanne[b,2] Hiroakira Ono[a,3]

[a] *RCIS, JAIST, Nomi, Japan*

[b] *LIP, ENS de Lyon, Lyon, France*

**Abstract**

We formulate precisely and prove formally the proposition that if conscientious players are constructively rational in a sequential game of perfect information, then the backward induction outcome is reached.

*Keywords:* Aumann's Theorem, rationality, backward induction, decidability, type theory, Coq

## 1 Introduction

A celebrated result in economics, hereinafter called *Aumann's Theorem (on Rationality)*, says that "common knowledge of rationality implies backward induction" [1]. The result pertains to extensive-form games of perfect information, i.e., sequentially-playable game trees, and involves epistemic operators. Backward induction is a restricted form of Nash equilibrium, where the usual *perceived optimality* requirement must hold not just for the game as a whole but at all intermediate stages as well. The result has been used to advocate sustained engagement in the resolution of regional conflicts, even if no obvious peace is in sight. The argument says that negotiations foster understanding and that, ultimately, all parties will come to appreciate each other's motives, their appreciation of motives, appreciation of appreciation of motives, etc., at which point a solution will have been reached. Unfortunately, one might say, semantical arguments exist that both validate [1] and contradict [7] the result. It is not clear what connectives and predicates are being

[1] Corresponding author; email: vester@jaist.ac.jp

[2] Email: pierre.lescanne@ens-lyon.fr

[3] Email: ono@jaist.ac.jp

given semantics though, and they obviously differ in the two cases. The technical point of departure is thought to be what is meant by *(substantive) rationality* [3].

We undertake a simple proof-theoretic analysis of Aumann's Theorem and present a proof of the differently motivated but closely related result in the title, in part to help clarify the above issue and make sure that less confusion is possible. Our development uses a new epistemic axiom for K/the knowledge modality, called "decidable not-K-not", where not-K-not is often interpreted as a form of belief. The axiom says that if it has been established that some agent does not know that some proposition is false *and* the truth status of that proposition is otherwise clear, then the proposition does in fact hold. Alternatively, the axiom says that agents may not believe propositions it is within their power to decide to be false — it is this property that gives rise to the titular 'conscientious players', and that points to constructive logic as the right framework for our proof and the preceding proof-theoretic analysis. Our proof does not involve common knowledge, in some sense because of the conscientiousness considerations, and additionally simplifies the requirements on the amount of knowledge that is needed to qualify as 'rational'. We do use general inductive definitions (to formally define *extensive-form games*) but it is not completely clear whether that explains why our proof does not need the fixpoint-defined common-knowledge modality whereas others use it [1,3,7]. The article is supported by a Coq [2] formalisation that contains additional results [9].

## 2 Formalism

A key element of our proof is the ability to make inductive definitions, and to subsequently prove properties about them by structural induction. We now sketch a simple formalism that incorporates this and the other proof concepts we need; it is based on extensible type theory but barely goes beyond first-order intuitionistic logic. The formalism is made extensible by the base language being indexed by a set of *user-specifiable base sorts*, $U$; additions to $U$ are tightly regulated, as we shall see, to avoid introducing inconsistencies.

**Definition 1** *We consider a set* $\mathcal{V}$ *of* variable names*, ranged over by* $x$*; a set* $\mathcal{F}$ *of* function symbols*, ranged over by* $f$*; and a set* $\mathcal{A}$ *of* ad hoc logical symbols*, ranged over by* $a$*. The sets are assumed to be disjoint. Let* $n$ *range over* $\mathcal{V} \cup \mathcal{F}$*.*

**Definition 2** *Consider terms* $\mathrm{T} ::= \mathcal{V} \mid \mathcal{F} \mid \mathrm{T}(\mathrm{T})$*, and let* $t$ *range over* T*.*

The terms may occur inside formulas either by themselves or as arguments to ad hoc logical symbols. (There are further restrictions on the use of terms, see below.)

**Definition 3** *Let* $\overrightarrow{X}$ *denote* lists *of* $X$*s, let* $\mathtt{F}$ *be the constant* false*, and consider*

$$\mathrm{P} \quad ::= \quad \mathrm{P} \wedge \mathrm{P} \mid \mathrm{P} \vee \mathrm{P} \mid \mathrm{P} \Rightarrow \mathrm{P} \mid \mathtt{F} \mid \forall \mathcal{V} \in U \,.\, \mathrm{P} \mid \mathrm{T} \mid \mathcal{A}(\overrightarrow{\mathrm{T}})$$

*Let* $p$ *range over* formulas P*; write* $\neg p$ *for* $p \Rightarrow \mathtt{F}$ *and* $\mathtt{T}$ *for* $\neg\mathtt{F}$*.*

In order to ensure that terms are used meaningfully, we introduce a notion of sorting with the principal aim that only PROP-sorted terms may occur as formulas, i.e., that terms that occur as formulas are predicates.

$$\frac{}{\Gamma_1, p, \Gamma_2 \vdash^{\Delta} p}\,(Assm)\ \text{ if } \Delta \rhd_f p \qquad \frac{\Gamma \vdash^{\Delta} \mathtt{F}}{\Gamma \vdash^{\Delta} p}\,(E_{\mathtt{F}})$$

$$\frac{\Gamma \vdash^{\Delta} p_l \quad \Gamma \vdash^{\Delta} p_r}{\Gamma \vdash^{\Delta} p_l \wedge p_r}\,(I_\wedge) \qquad \frac{\Gamma \vdash^{\Delta} p_l \wedge p_r}{\Gamma \vdash^{\Delta} p_l}\,(E^l_\wedge) \qquad \frac{\Gamma \vdash^{\Delta} p_l \wedge p_r}{\Gamma \vdash^{\Delta} p_r}\,(E^r_\wedge)$$

$$\frac{\Gamma \vdash^{\Delta} p_l}{\Gamma \vdash^{\Delta} p_l \vee p_r}\,(I^l_\vee) \qquad \frac{\Gamma \vdash^{\Delta} p_r}{\Gamma \vdash^{\Delta} p_l \vee p_r}\,(I^r_\vee) \qquad \frac{\Gamma \vdash^{\Delta} p_l \vee p_r \quad \Gamma, p_l \vdash^{\Delta} p \quad \Gamma, p_r \vdash^{\Delta} p}{\Gamma \vdash^{\Delta} p}\,(E_\vee)$$

$$\frac{\Gamma_1, p_a, \Gamma_2 \vdash^{\Delta} p_b}{\Gamma_1, \Gamma_2 \vdash^{\Delta} p_a \Rightarrow p_b}\,(I_\Rightarrow)\ \text{ if } \Delta \rhd_f p_a \qquad \frac{\Gamma \vdash^{\Delta} p_a \Rightarrow p_b \quad \Gamma \vdash^{\Delta} p_a}{\Gamma \vdash^{\Delta} p_b}\,(E_\Rightarrow)$$

Fig. 1. Intuitionistic propositional provability

$$\frac{\Gamma \vdash^{\Delta} \mathrm{Q}(Zero) \qquad \Gamma, \mathrm{Q}(x) \vdash^{\Delta, x:Nat} \mathrm{Q}(Succ(x))}{\Gamma \vdash^{\Delta} \forall n \in Nat\,.\,\mathrm{Q}(n)}\,(Ind^{\mathrm{Q}}_{Nat}) \qquad \text{if } \begin{cases} \Delta_t(Zero) = Nat, \\ \Delta_t(Succ) = Nat \to Nat, \\ n, x \text{ not used in } \Gamma, \Delta \end{cases}$$

Fig. 2. Structural induction over $Nat$

**Definition 4** *Let* Prop *be a distinct constant; consider* sorts*, ranged over by* $s$*.*

$$\mathrm{S} \;::=\; U \mid \textsc{Prop} \mid \mathrm{S} \to \mathrm{S}$$

**Definition 5** *Let* $\Delta$ *range over pairs* $\langle \Delta_t, \Delta_f \rangle$*, where* $\Delta_t$ *ranges over finite functions from* $\mathcal{V} \cup \mathcal{F}$ *to* S *and* $\Delta_f$ *ranges over finite functions from* $\mathcal{A}$ *to* $\overrightarrow{\mathrm{S}}$*;*[4] *let* $\oplus$ *range over* $\{\wedge, \vee, \Rightarrow\}$*. Define* well-sortedness for terms*,* $\rhd_t$*, and* formulas*,* $\rhd_f$*, thus.*

$$\frac{\Delta \rhd_t t_f : s_a \to s_r \quad \Delta \rhd_t t_a : s_a}{\Delta \rhd_t t_f(t_a) : s_r} \qquad \frac{\Delta_t(n) = s}{\Delta \rhd_t n : s} \qquad \frac{\Delta \rhd_f p}{\Delta \rhd_t p : \textsc{Prop}}$$

$$\frac{\Delta \rhd_f p \quad \Delta_t(x) = s}{\Delta \rhd_f \forall x \in s\,.\,p} \qquad \frac{\overrightarrow{\Delta \rhd_t t_i : s_i} \quad \Delta_f(a) = \overrightarrow{s_i}}{\Delta \rhd_f a(\overrightarrow{t_i})} \qquad \frac{\Delta \rhd_f p_1 \quad \Delta \rhd_f p_2}{\Delta \rhd_f p_1 \oplus p_2} \qquad \frac{}{\Delta \rhd_f \mathtt{F}} \qquad \frac{\Delta \rhd_t t : \textsc{Prop}}{\Delta \rhd_f t}$$

Next, we define provability; the definition is split into multiple parts but they address just one relation. We first consider intuitionistic propositional provability.

**Definition 6** *Let* $\Gamma$ *range over lists of formulas,* $\overrightarrow{\mathrm{P}}$*, and let* $\Delta$ *be as in Definition 5. The propositional part of our provability relation,* $\vdash^{\Delta}$*, is given in Fig. 1. We write* $\varepsilon$ *for empty lists and say that* $p$ *is a* $\vdash^{\Delta}$*-theorem if* $\varepsilon \vdash^{\Delta} p$ *is derivable.*

Appendix A contains example proofs (of the $\vdash$-equivalence of $\neg\neg p$ and $(p \vee \neg p) \Rightarrow p$). The sort set $U$ will contain any user-defined inductive data types, with the defining constructors taken as function symbols, $\mathcal{F}$. For example, a user may define a natural-number sort, with 'zero' and 'successor' constructors.[5]

$$\mathrm{Nat} \;::=\; \mathrm{Zero} : \mathrm{Nat} \mid \mathrm{Succ} : \mathrm{Nat} \to \mathrm{Nat}$$

[4] Formally, $\Delta$ should be set up as a dependently typed list.

[5] Formally, an inductively defined sort may be used only so-called "strictly positively" in the constructors' sorts. For example, $(\mathrm{X} \to \mathrm{X}) \to \mathrm{X}$ is not valid because of the first X: the type would not be well-founded.

$$\frac{\Gamma \vdash^{\Delta} p_0}{\Gamma \vdash^{\Delta} p}\,(comp) \qquad \text{if } \downarrow p = p_0 \text{ and } \Delta \triangleright_f p$$

Fig. 3. Computational reasoning

$$\frac{}{\Gamma \vdash^{\Delta} LEq^{Nat}(t,t)}\,(rInd^1_{LEq^{Nat}}) \quad \text{if } \begin{cases} \Delta \triangleright_t t : \mathrm{Nat} \\ \Delta_t(LEq^{Nat}) = \langle \mathrm{Nat}, \mathrm{Nat} \rangle \end{cases}$$

$$\frac{\Gamma \vdash^{\Delta} LEq^{Nat}(\mathrm{Succ}(t_1), t_2)}{\Gamma \vdash^{\Delta} LEq^{Nat}(t_1, t_2)}\,(rInd^2_{LEq^{Nat}}) \quad \text{if } \begin{cases} \Delta_t(LEq^{Nat}) = \langle \mathrm{Nat}, \mathrm{Nat} \rangle \\ \Delta_t(\mathrm{Succ}) = \mathrm{Nat} \to \mathrm{Nat} \end{cases}$$

Fig. 4. Ad hoc rule induction for $LEq^{Nat}$

**Definition 7** *For Inductively defined sorts, add* structural induction *rules to the provability relation, see Figure 2 in the case of Nat.*

Additionally, we allow for the definition by *structural recursion* of new function symbols over inductively defined sorts.

$$\begin{aligned} \mathrm{IsEven}(\mathrm{Zero}) &= \mathtt{T} \\ \mathrm{IsEven}(\mathrm{Succ}(n)) &= \neg \mathrm{IsEven}(n) \end{aligned}$$

**Definition 8** *Let the* computational reasoning *rule be as given in Figure 3, with* $\downarrow$ *being a not-further-specified form of deterministic computation that includes "exhaustive definition unfolding" of structural-recursive functions.*

With this, we are able to formally prove that, e.g., two is even.

$$\dfrac{\dfrac{\dfrac{}{\mathtt{F} \vdash^{\Delta} \mathtt{F}}\,(Assm)}{\varepsilon \vdash^{\Delta} \mathtt{T}}\,(I_{\Rightarrow})}{\varepsilon \vdash^{\Delta} \mathrm{IsEven}(\mathrm{Succ}(\mathrm{Succ}(\mathrm{Zero})))}\,(comp)$$

Lastly, we allow a user to conservatively extend the considered formalism.

$$\frac{}{LEq^{Nat}(t,t)} \qquad \frac{LEq^{Nat}(\mathrm{Succ}(t_1), t_2)}{LEq^{Nat}(t_1, t_2)}$$

**Definition 9** *For ad hoc logical symbols, include the defining rules as proof rules, see Figure 4, in the case of* $LEq^{Nat}$*: we refer to their use as* rule induction.

Formally, $\vdash$ is an *extensible type theory*. Under minor additional constraints, specifically *dependent typing of* $\Delta$, $\Gamma$, we can guarantee that any so-constructed extension is consistent. The proof of this will typically use a richer, non-extensible type theory that is consistent and contains functions that, e.g., send the definition of *Nat* to its structural-induction and -recursion rules, seen as terms.

## 3 Epistemic Provability

As mentioned, Aumann's Theorem involves epistemic operators, particularly for the *knowledge* of a given agent and the *common knowledge* of the group of agents.

$$\frac{}{\Gamma \vdash^{\Delta} K_a(p) \Rightarrow p}\,(T_{K_a}) \qquad \frac{\varepsilon \vdash^{\Delta} p}{\varepsilon \vdash^{\Delta} K_a(p)}\,(Gen_{K_a}) \qquad \frac{}{\Gamma \vdash^{\Delta} (K_a(p_1 \Rightarrow p_2)) \Rightarrow K_a(p_1) \Rightarrow K_a(p_2)}\,(K_{K_a})$$

Fig. 5. The knowledge modality, $K_a(-)$, for agent $a$

**Definition 10** *Consider a set of* agents, $G \in U$. *The* knowledge modality, $K_a : \textsc{Prop} \to \textsc{Prop}$, *for $a \in G$ is an ad hoc symbol, defined in Fig. 5. (The definition style goes beyond Fig. 4's conservative extensivity.)*

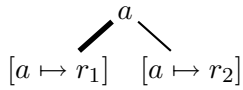
We shall not actively pursue the common-knowledge modality, $C_G$, and it suffices to mention that it can be defined as a fixpoint of knowledges, which means that it includes knowledge of knowledge ad infinitum. In addition to its fixpoint properties, $C_G$ enjoys the same laws as $K_a$, see Fig. 5.

## 4 Extensive-Form Games

Our reason for considering a formalism with support for inductive definitions is that Aumann's Theorem pertains to extensive-form games of perfect information. To economists, such games are expressible as game trees with no restrictions, e.g., on the order in which players move/make choices. To us, game trees are a standard abstract data type that is susceptible to formal treatment in its own right.

**Definition 11** *Let $rwd \in U$ be a sort (for payoffs/rewards) and consider the two-point sort $choice ::= left : choice \mid right : choice$. The inductive sort of* strategies *is $strt ::= Leaf : (G \to rwd) \to strt \mid Node : G \to choice \to strt \to strt \to strt$.*

A (binary) strategy is either a leaf, where a payoff function assigns a payoff to each agent, or it is an internal node owned by some agent, who chooses between two sub-strategies. A game is essentially the same sort, except no choice is recorded in internal nodes. (The binary restriction is not crucial to the considered result.) The following is an example, with $a \in G$ and the *choice* indicated with a boldface line.

(1)



**Definition 12** *Define structural-recursively the function that returns the choice-induced payoff/reward function in a given strategy, $strtRwd : strt \to (G \to rwd)$.*

$$\begin{aligned} strtRwd(Leaf\ rFct) &= rFct \\ strtRwd(Node\ a\ left\ sl\ sr) &= strtRwd(sl) \\ strtRwd(Node\ a\ right\ sl\ sr) &= strtRwd(sr) \end{aligned}$$

A strategy, $s$, is a Nash equilibrium for the underlying game if no agent, $a$, can increase $strtRwd(s)(a)$ by changing (only) $a$'s choices in $s$. A particular form of Nash equilibria, Backward Inductions, accomplishes this by all choices being optimal.

**Definition 13** *Consider the function symbol $LEq : rwd \to rwd \to \textsc{Prop}$ (less-than-or-equal-to on rewards) and the structural-recursive predicate, i.e., function*

*into* PROP*, that identifies Backward Induction strategies,* $BI : strt \to \text{PROP}$.

$$\begin{aligned} BI(Leaf\ rFct) &= \mathtt{T} \\ BI(Node\ a\ left\ sl\ sr) &= BI(sl) \wedge BI(sr) \wedge LEq(strtRwd(sr)(a), strtRwd(sl)(a)) \\ BI(Node\ a\ right\ sl\ sr) &= BI(sl) \wedge BI(sr) \wedge LEq(strtRwd(sl)(a), strtRwd(sr)(a)) \end{aligned}$$

(Needless to say, we can similarly define the function that computes a backward-induction strategy from a given game, thereby proving Kuhn's Theorem: "all extensive-form games of perfect information have Nash equilibria" [4,8].)

# 5 Rationality

Aumann defines rationality informally as follows [1].

> *"Rationality of a player means . . . that no matter where he finds himself — at which vertex — he will not knowingly continue with a strategy that yields him less than he could have gotten with a different strategy."*

The actual definition reads $\bigcap_{v \in V_i} \bigcap_{t_i \in S_i} (\neg K_i[h_i^v(\mathbf{s}; t_i) > h_i^v(\mathbf{s})])$ [1, eq. (3)], with $S_i$ being $i$'s choices and $V_i$ being $i$'s nodes. Stripping off the outer intersection, we are lead to the following predicate, where our $r$ is Aumann's $h_i^v(\mathbf{s})$.

**Definition 14** *Define* $nKns : strt \to G \to rwd \to \text{PROP}$ *by structural recursion.*

$$\begin{aligned} nKns(Leaf\ rFct, a, r) &= \neg K_a(\neg LEq(rFct(a), r) \\ nKns(Node\ a\ c\ sl\ sr, a, r) &= nKns(sl, a, r) \wedge nKns(sl, a, r) \\ nKns(Node\ a'\ left\ sl\ sr, a, r) &= nKns(sl, a, r) \\ nKns(Node\ a'\ right\ sl\ sr, a, r) &= nKns(sr, a, r) \end{aligned}$$

Aumann's outer intersection ranges over one agent's nodes, and rationality of all agents in a strategy is therefore as follows.

**Definition 15** *Define* $Rat : strt \to \text{PROP}$ *by structural recursion.*

$$\begin{aligned} Rat(Leaf\ rFct) &= \mathtt{T} \\ Rat(Node\ a\ c\ sl\ sr) &= Rat(sl) \wedge Rat(sr) \wedge nKns(Node\ a\ c\ sl\ sr, a, strtRwd(Node\ a\ c\ sl\ sr)(a)) \end{aligned}$$

# 6 Aumann's Theorem

Aumann's theorem states that if there is common knowledge of rationality in a given strategy, then that strategy is a backward-induction equilibrium.

$$\forall\ s : strt,\ C_G(Rat(s)) \Rightarrow BI(s)$$

## *6.1 A Consequence*

Consider the *strt*-example in (1), for which the implication in Aumann's Theorem is supposed to hold. Applying *Rat* to this example gives $\mathtt{T} \wedge \mathtt{T} \wedge \neg K_a(\neg LEq(r_1, r_1)) \wedge \neg K_a(\neg LEq(r_2, r_1))$. Applying *BI* gives $\mathtt{T} \wedge \mathtt{T} \wedge LEq(r_2, r_1)$. Aumann's Theorem therefore mandates that

$$C_G(\neg K_a(\mathtt{F}) \wedge \neg K_a(\neg LEq(r_2, r_1))) \ \Rightarrow\ LEq(r_2, r_1)$$

$\neg K_a(\mathtt{F})$ is short for $K_a(\mathtt{F}) \Rightarrow \mathtt{F}$, i.e., it is an instance of $(T_{K_a})$, and $C_G(\neg K_a(\mathtt{F}))$ is therefore provable by the $C_G$-generation rule, see $(Gen_{K_a})$ in Fig. 5. As $C_G$

$$\frac{}{\Gamma \vdash^{\Delta} \mathrm{Dcdbl}(p) \Rightarrow \neg K_a(\neg p) \Rightarrow p}\,(dec\text{-}nKn_a)$$

Fig. 6. Axiom decidable-nKn, with Dcdbl(_) being 'decidable'.

distributes over conjunction, this means that we are looking at the following.

$$C_G(\neg K_a(\neg LEq(r_2, r_1))) \;\Rightarrow\; LEq(r_2, r_1) \tag{2}$$

In other words, we need an axiom T for the combined modality $C_G(\neg K_a(\neg \_))$, with a possible qualification to certain permissible formulas that include $LEq(r_2, r_1)$. We have axiom T for $C_G$, and $\neg K_a(\neg p) \Rightarrow p$ would give us (2), by transitivity of $\Rightarrow$.

### *6.2 Axiom Decidable nKn and Constructive Logic*

We have axiom T for $K$: $(T_{K_a})$, see Fig. 5, including for negated propositions.

$$K_a(\neg p) \;\Rightarrow\; \neg p$$

In long form this is $K_a(\neg p) \;\Rightarrow\; p \;\Rightarrow\; \mathtt{F}$, or equivalently

$$p \;\Rightarrow\; \neg K_a(\neg p) \tag{3}$$

Having $\neg K_a(\neg p) \;\Rightarrow\; p$ thus collapses the derived modality, i.e., we would have $\neg K_a(\neg p) \Leftrightarrow p$. This is clearly not desirable in general as $\neg K_a(\neg \_)$ is thought to be related to epistemic belief. The question we are faced with in (2) is whether the $C_G$-modality qualifies $\neg K_a(\neg \_)$ enough to accept an axiom T for their combination. If we use the interpretation that $\neg K_a(\neg \_)$ is related to belief, or even absence of doubt, it is difficult to see how common knowledge of that fact can impact on the inner proposition, and we have found no compelling proof-theoretic argument either for or against an axiom T for $C_G(\neg K_a(\neg \_))$ (and none can be found in or can be immediately extracted from [1,3,7]). We note, instead, that (2) holds trivially if, in fact, it is the case that $LEq(r_2, r_1)$ holds. Conversely, $\neg K_a(\neg LEq(r_2, r_1))$ cannot be allowed to hold if $\neg LEq(r_2, r_1)$ can be independently established because that would allow us to conclude that also $LEq(r_2, r_1)$ holds, which would leave the considered formalism inconsistent. Consequently, we propose as a general principle that $\neg K_a(\neg p) \Rightarrow p$ holds in case of decidable propositions, $p$, i.e., propositions for which we know whether and which of it and its negation that is provable.

**Definition 16** *Axiom decidable-nKn is defined in Fig. 6.*

Because $\vdash$ is constructive, specifically because it enjoys the *Disjunction Property* ($\varepsilon \vdash^{\Delta} p \vee q$ implies $\varepsilon \vdash^{\Delta} p$ or $\varepsilon \vdash^{\Delta} q$), we have a simple coding of Dcdbl($p$) in the present case: $p \vee \neg p$. We shall take advantage of this in Section 8.2, where we give an alternative account of the axiom and prove that the introduced formalism is consistent. Informally, the axiom asks agents to *not believe in propositions that it is within their power to refute*, which is what restricts access to the axiom to conscientious players. In logical terms, the axiom prevents agents from believing F.

# 7 Rationality, Backward Induction, Conscientiousness

If we consider Aumann's two predicates, we can note that the number of conjuncts will grow faster in *Rat* than in *BI* with bigger strategies. The way induction proofs work, it will suffice for the two predicates to have the same structure/growth rate.

**Definition 17** *Define lRat, aka local rationality, by structural recursion.*

$$\begin{aligned} lRat(Leaf\ rFct) &= \mathtt{T} \\ lRat(Node\ a\ left\ sl\ sr) &= lRat(sl) \wedge lRat(sr) \wedge \neg K_a(\neg LEq(strtRwd(sr)(a), strtRwd(sl)(a))) \\ lRat(Node\ a\ right\ sl\ sr) &= lRat(sl) \wedge lRat(sr) \wedge \neg K_a(\neg LEq(strtRwd(sl)(a), strtRwd(sr)(a))) \end{aligned}$$

Let $\Delta_0$ be the sorting environment constructed so-far.

**Theorem 18** *Assuming LEq is decidable,* $\vdash^{\Delta_0} \forall s \in strt\,.\,lRat(s) \Rightarrow BI(s)$

**Proof** We write infix $\leq$ for *LEq*, and $\overline{c}$ for *choice* complementation. The proof proceeds by structural *strt*-induction in $s$. In the leaf case, the computational-reasoning rule implies that it suffices to prove $\mathtt{T} \Rightarrow \mathtt{T}$. In the node case, the computational-reasoning rule implies that we must prove that the three *lRat*-conjuncts for nodes imply the three *BI*-conjuncts, which we show via $(P_a \Rightarrow P_c) \Rightarrow (Q_a \Rightarrow Q_c) \Rightarrow (R_a \Rightarrow R_c) \Rightarrow P_a \wedge Q_a \wedge R_a \Rightarrow P_c \wedge Q_c \wedge R_c$, called (*33*) below. The first two follow directly by the induction hypotheses. For the third, we case-split on/do structural induction in the choice made and we are straightforwardly done by decidable-nKn and the assumed decidability of $\leq$.

$$\dfrac{\dfrac{\dfrac{}{\ldots}\,(dec\text{-}nKn_a) \quad \dfrac{}{H_i \vdash^{\Delta_0'} Dcdbl\ (r_2 \leq r_1)}\,(dec_{\leq})}{H_i \vdash^{\Delta_0'} \neg K_a(r_2 \not\leq r_1) \Rightarrow r_2 \leq r_1}\,(E_{\Rightarrow}) \quad \dfrac{\dfrac{}{\ldots}\,(dec\text{-}nKn_a) \quad \dfrac{}{H_i \vdash^{\Delta_0'} Dcdbl\ (r_1 \leq r_2)}\,(dec_{\leq})}{H_i \vdash^{\Delta_0'} \neg K_a(r_1 \not\leq r_2) \Rightarrow r_1 \leq r_2}\,(E_{\Rightarrow})}{H_i \vdash^{\Delta_0'} \forall c \in choice\,.\,\neg K_a(r_{\overline{c}} \not\leq r_c) \Rightarrow r_{\overline{c}} \leq r_c)}\,(Ind)^{-}_{choice}$$

$$\dfrac{\dfrac{\dfrac{}{H_i \vdash^{\Delta_0'} lRat\ s_1 \Rightarrow BI\ s_1}\,(A) \quad \dfrac{}{H_i \vdash^{\Delta_0'} lRat\ s_2 \Rightarrow BI\ s_2}\,(A)}{H_i \vdash^{\Delta_0'} lRat\ (Nd\ a\ c\ s_1\ s_2) \Rightarrow BI\ (Nd\ a\ c\ s_1\ s_2)}\,(33)\,(comp) \quad \dfrac{\dfrac{}{\varepsilon \vdash^{\Delta_0''} \mathtt{T} \Rightarrow \mathtt{T}}\,(A)\,(I_{\Rightarrow})}{\varepsilon \vdash^{\Delta_0''} lRat\ (Lf\ rF) \Rightarrow BI\ (Lf\ rF)}\,(comp)}{\varepsilon \vdash^{\Delta_0} \forall s \in strt\,.\,lRat\ s \Rightarrow BI\ s}\,(Ind)^{-}_{strt}$$

□

Needless to say, $Rat(s)$ implies $lRat(s)$. By transitivity of $\Rightarrow$ and axiom T for $C_G$, it therefore follows from the above result that $\vdash^{\Delta_0} \forall s \in strt\,.\,C_G(Rat(s)) \Rightarrow BI(s)$.

As a side-remark, we note that the proof will be even simpler if a decision procedure for *LEq* is known. In the case of Nat, the following works, see [9].

$$\begin{aligned} LEq_{dp}(Zero, Succ(n)) &= \mathtt{T} \\ LEq_{dp}(Succ(n), Zero) &= \mathtt{F} \\ LEq_{dp}(Succ(n_1), Succ(n_2)) &= LEq_{dp}(n_1, n_2) \end{aligned}$$

# 8 Discussion

## *8.1 Formalisation*

Coq [2] formalisations of the various results we have discussed are available at http://www.jaist.ac.jp/~vester/Writings/eAumann-abstract-relOrdering.v and

http://www.jaist.ac.jp/~vester/Writings/eAumann-Nat-fctOrdering.v. The developments in this paper directly reflect their Coq counterparts and $\vdash$ is intended as a lightweight calculus of inductive constructions [6]. The formalisation is shallow *and* deep: we borrow Coq's induction mechanisms but re-formalise the other aspects.

### *8.2 Epistemic Knowledge*

According to [1, Proof of Theorem A], Aumann's model validates $\neg K_i(\neg I^v) \Rightarrow I^v$, $\neg K_i(\neg I^v) \Leftrightarrow \neg\neg K_i(I^v)$, and $\neg\neg K_i(I^v) \Leftrightarrow K_i(I^v)$, where $I^v$ means that "the backward-induction choice was made in node $v$", i.e., $I^v$ is short for our $r_2 \leq r_1$-conditions. As we saw, the first of these imply that $\neg K_i(\neg I^v) \Leftrightarrow I^v$. The combination of these equivalences makes it difficult (or trivial!) to understand what is meant by the knowledge and common-knowledge modalities in [1].

For our development, we note that $p \Rightarrow \neg\neg p$ and $\neg p \Leftrightarrow \neg\neg\neg p$ hold intuitionistically, while $\neg\neg p \Rightarrow p$ typically is thought of as only classically valid. However, double-negation elimination does hold intuitionistically for decidable formulas.

**Proposition 19** $\vdash^{p:\textsc{Prop}} (p \vee \neg p) \Rightarrow \neg\neg p \Rightarrow p$.

**Proof** Proposition 21, Appendix A (with the last two rules swapped). □

An interesting consequence is the following.

**Lemma 20** *Let* $\vdash_{\overline{(dec_{nKn_a})}}$ *be* $\vdash$ *without* (*dec-nKn*$_a$)*; adding axiom* (*dec-nKn*$_a$) *to* $\vdash_{\overline{(dec_{nKn_a})}}$ *is equivalent to adding the following axiom.*

$$\frac{}{\Gamma \vdash^{\Delta} \neg K_a(\neg p) \Leftrightarrow \neg\neg p}\,(nKn_a\neg\neg)$$

**Proof** (*dec-nKn*$_a$) follows from ($nKn_a\neg\neg$) according to Proposition 19. For the other direction, we first note that (3) implies $\neg\neg p \Rightarrow \neg K_a(\neg p)$ by contraposition. For $\neg K_a(\neg p) \Rightarrow \neg\neg p$, we note that $\neg\neg p$ is equivalent to $(p \vee \neg p) \Rightarrow p$, see Appendix A, and we are done by swapping $\neg K_a(\neg p)$ and $p \vee \neg p$ in (*dec-nKn*$_a$). □

In other words, adding axiom (*dec-nKn*$_a$) has the formal effect of mandating that $\neg K_a(\neg\_)$ can only hold for propositions that are not explicitly refutable, which i) is the usual intuitionistic reading of double-negation and ii) is reassuringly close to our informal aim. More, adding the axiom i) does not collapse $\neg K_a(\neg p)$ and $p$ in general and ii) is consistent with intuitionistic epistemic logic; in particular, (3) implies that it is logically consistent to add the axiom to standard epistemic logic.

### *8.3 Substantive Rationality vs Structural Recursion*

Aumann [1] states that substantive rationality means that "when deciding what to do at $v$, the player considers the situation *from that point on*: he acts *as if* $v$ is reached." According to Halpern [3], this amounts to a *counterfactual* and, in particular, 'substantive' is formalised by the outer intersection in $\bigcap_{v\in V_i}\bigcap_{t_i\in S_i}(\neg K_i[h_i^v(\mathbf{s};t_i) > h_i^v(\mathbf{s})])$. To us, this means that Aumann's substantive rationality is definable by structural recursion, as done here: 'substantivity' (in

Halpern's interpretation) corresponds to the recursion over all nodes and (for Aumann's stated intentions) to the compositionality of our rationality predicates, i.e., that recursive calls do not depend on the call site; more, 'counter-factuality' corresponds to the fact that our rationality predicates recurse into both sub-strategies of a node of a considered player, meaning that some knowledge will involve choices that are not going to be reached according to the strategy at hand.

# 9 Conclusion

If, indeed, we have re-proved and strengthened Aumann's Theorem (under the reasonable additional assumptions that $LEq$ is decidable and that players check the most basic of facts before forming beliefs), it is noteworthy how relatively inconspicuous our proof (of Theorem 18) is — in particular, the proof is a straightforward structural induction with one subtlety: ($dec\text{-}nKn_a$). If the two results are merely related, an additional proof-theoretic analysis of what is actually meant by Aumann's Theorem and its epistemic connectives and consequences would be instructive. Irrespective of the relationship between the results, our analysis pinpointed axioms T to be of central relevance and, additionally, lead us to Axiom ($dec\text{-}nKn_a$), which seems to have its own compelling logic, in particular but not only in intuitionistic/constructive logic.

# References


[1] Aumann, R. J., *Backward induction and common knowledge of rationality*, Games and Economic Behavior **8** (1995).

[2] Dowek, G., C. Paulin-Mohring et al., *Coq*, http://coq.inria.fr/.

[3] Halpern, J. Y., *Substantive rationality and backward induction*, Games and Economic Behavior **37** (2001), pp. 425–435.

[4] Kuhn, H. W., *Extensive games and the problem of information*, Contributions to the Theory of Games II (1953), reprinted in [5].

[5] Kuhn, H. W., editor, "Classics in Game Theory," Princeton Uni. Press, 1997.

[6] Paulin-Mohring, C., *Inductive definitions in the system Coq: Rules and properties*, in: M. Bezem and J. F. Groote, editors, *Typed Lambda Calculi and Applications, TLCA'93*, Lecture Notes in Computer Science **664** (1993), pp. 328–345.

[7] Stalnaker, R., *Knowledge, belief and counterfactual reasoning in games*, Economics and Philosophy **12** (1996), pp. 133–162.

[8] Vestergaard, R., *A constructive approach to sequential Nash equilibria*, Information Processing Letters **97** (2006), pp. 46–51.

[9] Vestergaard, R., P. Lescanne and H. Ono, *The inductive and modal proof theory of Aumann's theorem on rationality*, Technical Report IS-RR-2006-009, JAIST (2006).

## A "$\vdash \neg\neg p \Leftrightarrow ((p \vee \neg p) \Rightarrow p)$"

**Proposition 21** $\vdash^{p:\textsc{Prop}} \neg\neg p \Rightarrow (p \vee \neg p) \Rightarrow p$

**Proof** We suppress $p : \textsc{Prop}$ in the proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg p, \neg\neg p, p \vee \neg p \vdash \neg p \Rightarrow \mathtt{F}}(A) \quad \dfrac{}{\neg p, \neg\neg p, p \vee \neg p \vdash \neg p}(A)}{\neg p, \neg\neg p, p \vee \neg p \vdash \mathtt{F}}(E_{\Rightarrow})}{\neg p, \neg\neg p, p \vee \neg p \vdash p}(E_{\mathtt{F}}) \\ \vdots \\ \dfrac{}{\neg\neg p, p \vee \neg p \vdash p \vee \neg p}(A) \quad \dfrac{}{p, \neg\neg p, p \vee \neg p \vdash p}(A)}{\neg\neg p, p \vee \neg p \vdash p}(E_{\vee})}{\neg\neg p \vdash (p \vee \neg p) \Rightarrow p}(I_{\Rightarrow})}{\varepsilon \vdash \neg\neg p \Rightarrow (p \vee \neg p) \Rightarrow p}(I_{\Rightarrow})$$

□

**Proposition 22** $\vdash^{p:\textsc{Prop}} ((p \vee \neg p) \Rightarrow p) \Rightarrow \neg\neg p$

**Proof** We suppress $p : \textsc{Prop}$ in the proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg p, (p \vee \neg p) \Rightarrow p \vdash \neg p}(A)}{\neg p, (p \vee \neg p) \Rightarrow p \vdash p \vee \neg p}(I'_{\vee}) \\ \vdots \\ \dfrac{}{\neg p, (p \vee \neg p) \Rightarrow p \vdash (p \vee \neg p) \Rightarrow p}(A)}{\neg p, (p \vee \neg p) \Rightarrow p \vdash p}(E_{\Rightarrow}) \\ \vdots \\ \dfrac{}{\neg p, (p \vee \neg p) \Rightarrow p \vdash p \Rightarrow \mathtt{F}}(A)}{\neg p, (p \vee \neg p) \Rightarrow p \vdash \mathtt{F}}(E_{\Rightarrow})}{(p \vee \neg p) \Rightarrow p \vdash \neg p \Rightarrow \mathtt{F}}(I_{\Rightarrow})}{\varepsilon \vdash ((p \vee \neg p) \Rightarrow p) \Rightarrow \neg\neg p}(I_{\Rightarrow})$$

□

# Reducing Provability to Knowledge in Multi-Agent Systems

Simon Kramer[1]

*Ecole Polytechnique and INRIA*
*Paris, France*

**Abstract**

We construct a reduction of provability to a combination of four kinds of knowledge in multi-agent systems. These kinds are: *individual* knowledge (knowledge of messages), plain *propositional* knowledge (knowledge that a state of affairs is the case), *common* knowledge (propositional knowledge shared in a community of agents), and a new kind of knowledge, namely *adductive* knowledge (propositional knowledge contingent on the adduction of certain individual knowledge, e.g., through *oracle invocation*).

*Keywords:* modal logic, [designated verifier] proofs as sufficient evidence, oracles, multi-agent systems

## 1 Introduction

The concept of formal provability (i.e. as internalised in a formal language) goes back to Gödel (cf. [1, Chapter 16] by S. N. Artëmov); the one of formal knowledge to Hintikka (cf. [2] for a monograph). Provability is strictly stronger than plain propositional knowledge (i.e. the knowledge that a state of affairs is the case): for example, an agent may know that a certain state of affairs is the case *from observation* yet not be able to prove her knowledge to the non-observers for lack of *sufficient evidence* (i.e. proof) that could confirm her knowledge to them.

Notwithstanding, we prove that provability *is* reducible to knowledge — even in multi-agent systems — although of course not to plain propositional knowledge alone, but to a combination of *individual* knowledge (knowledge of messages), plain *propositional* knowledge, *common* knowledge (propositional knowledge shared in a community of agents), and a new kind of knowledge, namely *adductive* knowledge (propositional knowledge contingent on the adduction of certain individual knowledge, e.g., through *oracle invocation*).

Applications of formal provability in *dis*trusted multi-agent systems have been discovered in [3,4], where it is shown that provability is the key to the logical for-

[1] Email: simon.kramer@a3.epfl.ch

malisation of the class of *commitment*-related states of affairs such as electronic contract-signing (including non-repudiation). In *trusted* multi-agent systems (e.g. scientific peer-review), the main application of formal provability is the communicability of propositional knowledge: if an agent, say $a$, has a proof that a state of affairs, say $\phi$, is the case then $a$ can convince any other agent, say $b$, that ($a$ knows that) $\phi$ is the case by communicating that (signed) proof to $b$.

We opine that just as the introduction of Prior's *temporal* logic into computer science by Pnueli has given birth to a generation of *concurrent* [2] systems specification and verification, and as the introduction of Hintikka's *epistemic* logic into computer science by Fagin, Halpern, Moses, and Vardi is giving birth to a generation of *distributed* [3] systems specification and verification, the introduction of Gödel-style *provability* into computer science will give birth to a next generation of *accountable* distributed systems specification and verification. In this opinion, this paper reduces the third generation of systems specification and verification to the second generation at the cost of introducing adductive knowledge.

Finally, we opine that in the age of the Internet, which acts as a generator and amplifier of the virtuality of human relations, accountability, i.e., the possibility of enforcing responsibility for committed acts, is increasingly important.

## 2 Reduction

### *2.1 Definitions*

**Definition 2.1** [Reduction framework] Let $\mathcal{A}$ designate a finite set of *agent names* [4] $a$, $\mathcal{M} \ni M ::= a \mid [M]_a \mid (M, M)$ a set of *messages* $M$ with agent names, signed messages, and message pairs, respectively, and

$$\Phi \ni \phi ::= a \; \mathsf{k} \; M \mid \neg\phi \mid \phi \wedge \phi \mid \forall m(\varphi) \mid \Box\phi \mid \mathsf{K}_a(\phi) \mid \mathsf{K}_a^M(\phi) \mid \mathsf{CK}(\phi)$$

our logical language of propositions (*closed* formulae) $\phi$, where $\varphi$ denotes corresponding unary *open* formulae in which the variable $m$ replaces some occurrences of a message $M$. Our language provides *individual* knowledge ($\mathsf{k}$, pronounced "knows"), negation, conjunction, universal quantification over messages (ranged over by variables $m$), an operator for truth at all future moments in time ($\Box$, pronounced "always"), *plain propositional* knowledge ($\mathsf{K}_a$, pronounced "$a$ knows that"), *adductive propositional* knowledge ($\mathsf{K}_a^M$, pronounced "if $a$ knew $M$ then $a$ would know that"), and *common propositional* knowledge ($\mathsf{CK}$, pronounced "it is common knowledge among the agents that"), respectively.

Then, given $\mathcal{E} \ni \varepsilon ::= \mathtt{Snd}(a, M, b) \mid \mathtt{Rcv}(a, M)$ a set of *communication events* $\varepsilon$ as generated by message sending and receiving actions, respectively, and $\mathcal{E}^*$ the set of *event traces* $E$, the relation of satisfaction $\models \subseteq (\mathcal{E}^* \times \mathbb{N}) \times \Phi$ of our framework is defined in Table 1. There,

- $E\lfloor i$ (resp. $E\rfloor i$) designates the event trace $E$ up to (resp. from) and including the event at position $i$ of $E$

[2] e.g., threads forked by a common process, and processes launched by a common computer

[3] e.g., agent applications, computer clusters, and peer-to-peer systems

[4] Agents are referred to by their (unique) name, and names are transmittable data, i.e., messages.

Table 1
Satisfaction relation

| | | |
|---|---|---|
| $(E,i) \models a \,\mathsf{k}\, M$ | :iff | $E\lfloor i \vdash_a M$ |
| $(E,i) \models \neg\phi$ | :iff | not $(E,i) \models \phi$ |
| $(E,i) \models \phi \wedge \phi'$ | :iff | $(E,i) \models \phi$ and $(E,i) \models \phi'$ |
| $(E,i) \models \forall m(\varphi)$ | :iff | for all $M \in \mathcal{M}$, $(E,i) \models \{m \mapsto M\}(\varphi)$ |
| $(E,i) \models \Box\phi$ | :iff | for all $j \geq i$, $(E,j) \models \phi$ |
| $(E,i) \models \mathsf{K}_a(\phi)$ | :iff | for all $(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E',i') \approx_a (E,i)$ then $(E',i') \models \phi$ |
| $(E,i) \models \mathsf{K}_a^M(\phi)$ | :iff | for all $M' \in \mathcal{M}$, if $(\mathtt{Rcv}(a,M'),1) \models a \,\mathsf{k}\, M$ — *the adduction ...* then $(E\lfloor i \cdot \mathtt{Rcv}(a,M') \cdot E\lfloor i+1, i+1) \models \mathsf{K}_a(\phi)$ |
| $(E,i) \models \mathsf{CK}(\phi)$ | :iff | for all $(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E',i') \approx_\cup^* (E,i)$ then $(E',i') \models \phi$ |

- for all $a \in \mathcal{A}$, $\vdash_a \subseteq \mathcal{E}^* \times \mathcal{M}$:
  - $\mathtt{Rcv}(a,M) \vdash_a M$ (reception implies knowledge)
  - $\mathtt{Snd}(a,M,b) \vdash_a M$ (sending implies knowledge)
  - if $b \in \mathcal{A}$ then $E \vdash_a b$ (agent names are guessable)
  - if $E \vdash_a M$ then $E \vdash_a [M]_a$ (unforgeable signature synthesis)
  - if $E \vdash_a [M]_b$ then $E \vdash_a M$ (signature "analysis")
  - if $E \vdash_a M$ then $E \cdot \varepsilon \vdash_a M$ (monotonicity of individual knowledge)
  - if $E \vdash_a M$ and $E \vdash_a M'$ then $E \vdash_a (M,M')$ (pairing)
  - if $E \vdash_a (M,M')$ then $E \vdash_a M$ and $E \vdash_a M'$ (unpairing)
- for all $a \in \mathcal{A}$, $\approx_a$ designates a standard **S5** epistemic accessibility relation, such that for all $(E,i),(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E,i) \approx_a (E',i')$ then for all $M \in \mathcal{M}$, $(E,i) \models a \,\mathsf{k}\, M$ if and only if $(E',i') \models a \,\mathsf{k}\, M$
  (Indistinguishability of worlds implies identity of individual knowledge.)
- $\approx_\cup^*$ designates the reflexive, transitive closure of $\approx_\cup := \bigcup_{a \in \mathcal{A}} \approx_a$.

Notice that $\phi \in \Phi$ have a Herbrand-style semantics, i.e., logical constants (i.e. agent names) and functional symbols (for signing and pairing) are self-interpreted rather than interpreted in terms of (other, semantic) constants and functions. This design choice is admissible because our individuals (messages) are finite. Hence, substituting (syntactic) messages for message variables into (finite) formulae preserves the finitude of formulae (cf. the semantics of universal quantification).

Further notice that we assume the existence of an unforgeable (proprietary) mechanism for signing messages, which we model with the above signature synthesis and analysis rules. In *trusted* multi-agent systems, such a mechanism is trivially given by the inclusion of the sender name in the sent message. In *dis*trusted multi-agent systems, such a mechanism can be implemented with public-key cryptography.

Furthermore, we macro-define: $\top := a \,\mathsf{k}\, a$, $\bot := \neg\top$, $\phi \vee \phi' := \neg(\neg\phi \wedge \neg\phi')$, $\phi \to \phi' := \neg\phi \vee \phi'$, $\exists m(\varphi) := \neg\forall m(\neg\varphi)$, and $\Diamond\phi := \neg\Box\neg\phi$ ("eventually"); and —

more interestingly — our syntactic construction and conceptual reduction:

$$\begin{array}{rcll} M :_a \phi & := & \mathsf{CK}((a \,\mathsf{k}\, M \rightarrow \mathsf{K}_a(\phi)) \wedge \mathsf{K}_a^M(\phi)) & M \text{ is a proof of } \phi \text{ for } a \\ M : \phi & := & \forall a(M :_a \phi) & M \text{ is a proof of } \phi \\ \mathsf{P}_a(\phi) & := & \exists m((m : \phi) \wedge a \,\mathsf{k}\, m) & a \text{ can prove that } \phi \end{array}$$

$M :_a \phi$ is also pronounced "$M$ is a proof of $\phi$ *for the designated verifier* $a$". In our spirit of *proofs as sufficient evidence*, our definition of designated-verifier proofs stipulates that it be common knowledge among the agents that to the verifier, the *actual* and the *hypothetical* (if received from, e.g., an oracle) knowledge of $M$ be individually necessary and jointly (vacuity!) sufficient for the knowledge of $\phi$.

The hypothetical nature of adductive knowledge is confirmed by the fact that adductive knowledge can be recast as a formula in *conditional logic* (due to Lewis) with knowledge. That is, we could actually macro-define

$$\mathsf{K}_a^M(\phi) \;:=\; a \,\mathsf{k}\, M > \mathsf{K}_a(\phi)$$

where $>$ designates conditional implication. Informally, $\phi > \phi'$ is true in a world by definition if and only if all minimal $\phi$-worlds are $\phi'$-worlds [1, Page 55], where the intuition of minimality in our special case would be the one of a single oracle invocation and sufficient individual knowledge.

**Definition 2.2** [Validity] For all $\phi \in \Phi$, $\phi$ is *valid*, written $\models \phi$, :iff for all $(E, i) \in \mathcal{E}^* \times \mathbb{N}$, $(E, i) \models \phi$.

**Definition 2.3** [Logical consequence] For all $\phi, \phi' \in \Phi$, $\phi'$ is *a logical consequence of* $\phi$, written $\phi \Rightarrow \phi'$, :iff for all $(E, i) \in \mathcal{E}^* \times \mathbb{N}$, if $(E, i) \models \phi$ then $(E, i) \models \phi'$.

### *2.1.1 Generality*

Our reduction is constructed in a fixed framework but without loss of generality in the following sense:

- The *term language* can absorb arbitrary additional data types: our reduction just requires message pairing and (trivial or cryptographic) signing.
- The *formula language* can absorb additional operators such as a next-time operator or branching-time operators. It is the application domain of multi-agent systems, not our reduction, that requires temporal operators because knowledge in multi-agent systems is dynamic due to their intrinsic interactivity.

## *2.2 Results*

**Theorem 2.4** $\mathsf{P}_a$ *is* ***S4****, the modal system of Gödel's provability modality:*

$\boldsymbol{K}$ $\models \mathsf{P}_a(\phi \rightarrow \phi') \rightarrow (\mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi'))$

$\boldsymbol{T}$ $\models \mathsf{P}_a(\phi) \rightarrow \phi$

$\boldsymbol{4}$ $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\mathsf{P}_a(\phi))$

***N*** *if* $\models \phi$ *then* $\models \mathsf{P}_a(\phi)$.

For transparency, all our proofs are elementary and Fitch-style[5]. They can be checked on a tick-off line-by-line basis.

For simplicity, we will not make a typographical distinction between closed formulae $\phi$ and open formulae $\varphi$ anymore.

**Lemma 2.5** $\models \phi \to \phi'$ *iff* $\phi \Rightarrow \phi'$

**Proof.**

$\models \phi \to \phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, $(E,i) \models \phi \to \phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, $(E,i) \models \neg\phi \vee \phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, $(E,i) \models \neg(\neg\neg\phi \wedge \neg\phi')$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not $(E,i) \models \neg\neg\phi \wedge \neg\phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not $((E,i) \models \neg\neg\phi$ and $(E,i) \models \neg\phi')$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not (not not $(E,i) \models \phi$ and not $(E,i) \models \phi')$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not $((E,i) \models \phi$ and not $(E,i) \models \phi')$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not $(E,i) \models \phi$ or not not $(E,i) \models \phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, not $(E,i) \models \phi$ or $(E,i) \models \phi'$ iff
for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, if $(E,i) \models \phi$ then $(E,i) \models \phi'$ iff
$\phi \Rightarrow \phi'$

□

**Lemma 2.6 (The use of signing)**

$$\models \forall a \forall b \forall m(b \,\mathsf{k}\, [m]_a \to \mathsf{K}_b(a \,\mathsf{k}\, m))$$

**Proof.**

| | | |
|---|---|---|
| 1. | $(E,i) \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 2. | $a, b \in \mathcal{A}$ and $M \in \mathcal{M}$ | hyp. |
| 3. | $(E,i) \models b \,\mathsf{k}\, [M]_a$ | hyp. |
| 4. | $(E',i') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 5. | $(E',i') \approx_b (E,i)$ | hyp. |
| 6. | $(E',i') \models b \,\mathsf{k}\, [M]_a$ | 3, 5, property of $\approx_b$ |
| 7. | $(E',i') \models a \,\mathsf{k}\, [M]_a$ | 6, property of $\mathsf{k}$[6] |
| 8. | $(E',i') \models a \,\mathsf{k}\, M$ | 7, property of $\mathsf{k}$ |
| 9. | if $(E',i') \approx_b (E,i)$ then $(E',i') \models a \,\mathsf{k}\, M$ | 5–8 |
| 10. | for all $(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E',i') \approx_b (E,i)$ then $(E',i') \models a \,\mathsf{k}\, M$ | 4–9 |
| 11. | $(E,i) \models \mathsf{K}_b(a \,\mathsf{k}\, M)$ | 10 |
| 12. | if $(E,i) \models b \,\mathsf{k}\, [M]_a$ then $(E,i) \models \mathsf{K}_b(a \,\mathsf{k}\, M)$ | 3–11 |

[5] http://en.wikipedia.org/wiki/Fitch-style_calculus

[6] unforgeability of signatures (no one else but $a$ can have synthesised $[M]_a$)

| | | |
|---|---|---|
| 13. | $(E,i) \models b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(a \,\mathsf{k}\, M)$ | 12 |
| 14. | for all $a,b \in \mathcal{A}$ and $M \in \mathcal{M}$, $(E,i) \models b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(a \,\mathsf{k}\, M)$ | 2–13 |
| 15. | $(E,i) \models \forall a \forall b \forall m(b \,\mathsf{k}\, [m]_a \rightarrow \mathsf{K}_b(a \,\mathsf{k}\, m))$ | 14 |
| 16. | for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, $(E,i) \models \forall a \forall b \forall m(b \,\mathsf{k}\, [m]_a \rightarrow \mathsf{K}_b(a \,\mathsf{k}\, m))$ | 1–15 |
| 17. | $\models \forall a \forall b \forall m(b \,\mathsf{k}\, [m]_a \rightarrow \mathsf{K}_b(a \,\mathsf{k}\, m))$ | 16 |
| | | □ |

**Lemma 2.7 (The use of signing proofs)**

$$\models \forall a \forall b(\exists m(b \,\mathsf{k}\, [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi)))$$

**Proof.**

| | | |
|---|---|---|
| 1. | $(E,i) \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 2. | $a,b \in \mathcal{A}$ | hyp. |
| 3. | $(E,i) \models \exists m(b \,\mathsf{k}\, [m]_a \wedge m : \phi)$ | hyp. |
| 4. | there is $M \in \mathcal{M}$ s.t. $(E,i) \models b \,\mathsf{k}\, [M]_a \wedge M : \phi$ | 3 |
| 5. | $M \in \mathcal{M}$ and $(E,i) \models b \,\mathsf{k}\, [M]_a \wedge M : \phi$ | hyp. |
| 6. | $(E',i') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 7. | $(E',i') \approx_b (E,i)$ | hyp. |
| 8. | $(E,i) \models b \,\mathsf{k}\, [M]_a$ | 5 |
| 9. | $(E,i) \models M : \phi$ | 5 |
| 10. | $(E',i') \models b \,\mathsf{k}\, [M]_a$ | 7, 8, property of $\approx_b$ |
| 11. | $(E',i') \models \mathsf{K}_b(a \,\mathsf{k}\, M)$ | 10, Lemma 2.6 |
| 12. | $(E',i') \models a \,\mathsf{k}\, M$ | 11, $\mathbf{T}(\mathsf{K})$ |
| 13. | $c \in \mathcal{A}$ | hyp. |
| 14. | $(E,i) \models \forall c(M :_c \phi)$ | 9 |
| 15. | $(E,i) \models M :_c \phi$ | 13, 14 |
| 16. | $(E,i) \models \mathsf{CK}((c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi))$ | 15 |
| 17. | for all $(E'',i'') \in \mathcal{E}^* \times \mathbb{N}$, if $(E'',i'') \approx_\cup^* (E,i)$ then $(E'',i'') \models (c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi)$ | 16 |
| 18. | $(E'',i'') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 19. | $(E'',i'') \approx_\cup^* (E',i')$ | hyp. |
| 20. | $(E'',i'') \approx_\cup^* (E,i)$ | 7, 19, property of $\approx_\cup^*$ |
| 21. | $(E'',i'') \models (c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi)$ | 17, 18, 20 |
| 22. | if $(E'',i'') \approx_\cup^* (E',i')$ then $(E'',i'') \models (c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi)$ | 19–21 |
| 23. | for all $(E'',i'') \in \mathcal{E}^* \times \mathbb{N}$, if $(E'',i'') \approx_\cup^* (E',i')$ then $(E'',i'') \models (c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi)$ | 18–22 |
| 24. | $(E',i') \models \mathsf{CK}((c \,\mathsf{k}\, M \rightarrow \mathsf{K}_c(\phi)) \wedge \mathsf{K}_c^M(\phi))$ | 23 |
| 25. | $(E',i') \models M :_c \phi$ | 24 |
| 26. | for all $c \in \mathcal{A}$, $(E',i') \models M :_c \phi$ | 13–25 |

| | | |
|---|---|---|
| 27. | $(E', i') \models \forall c(M :_c \phi)$ | 26 |
| 28. | $(E', i') \models M : \phi$ | 27 |
| 29. | $(E', i') \models (M : \phi) \wedge a \mathsf{k} M$ | 12, 28 |
| 30. | there is $M \in \mathcal{M}$ s.t. $(E', i') \models (M : \phi) \wedge a \mathsf{k} M$ | 29 |
| 31. | $(E', i') \models \exists m((m : \phi) \wedge a \mathsf{k} m)$ | 30 |
| 32. | $(E', i') \models \mathsf{P}_a(\phi)$ | 31 |
| 33. | if $(E', i') \approx_b (E, i)$ then $(E', i') \models \mathsf{P}_a(\phi)$ | 7–32 |
| 34. | for all $(E', i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E', i') \approx_b (E, i)$ then $(E', i') \models \mathsf{P}_a(\phi)$ | 6–33 |
| 35. | $(E, i) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 34 |
| 36. | $(E, i) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 4–35 |
| 37. | if $(E, i) \models \exists m(b \mathsf{k} [m]_a \wedge m : \phi)$ then $(E, i) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 3–36 |
| 38. | $(E, i) \models \exists m(b \mathsf{k} [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 37 |
| 39. | for all $a, b \in \mathcal{A}$, $(E, i) \models \exists m(b \mathsf{k} [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 2–38 |
| 40. | $(E, i) \models \forall a \forall b(\exists m(b \mathsf{k} [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi)))$ | 39 |
| 41. | for all $(E, i) \in \mathcal{E}^* \times \mathbb{N}$, $(E, i) \models \forall a \forall b(\exists m(b \mathsf{k} [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi)))$ | 1–40 |
| 42. | $\models \forall a \forall b(\exists m(b \mathsf{k} [m]_a \wedge m : \phi) \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi)))$ | 41 |

□

**Proposition 2.8** $\models \mathsf{P}_a(\phi \rightarrow \phi') \rightarrow (\mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi'))$

**Proof.**

| | | |
|---|---|---|
| 1. | $(E, i) \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 2. | $(E, i) \models \mathsf{P}_a(\phi \rightarrow \phi')$ | hyp. |
| 3. | $(E, i) \models \mathsf{P}_a(\phi)$ | hyp. |
| 4. | $(E, i) \models \exists m((m : \phi \rightarrow \phi') \wedge a \mathsf{k} m)$ | 2 |
| 5. | there is $M \in \mathcal{M}$ s.t. $(E, i) \models (M : \phi \rightarrow \phi') \wedge a \mathsf{k} M$ | 4 |
| 6. | $M \in \mathcal{M}$ and $(E, i) \models (M : \phi \rightarrow \phi') \wedge a \mathsf{k} M$ | hyp. |
| 7. | $(E, i) \models \exists m((m : \phi) \wedge a \mathsf{k} m)$ | 3 |
| 8. | there is $M' \in \mathcal{M}$ s.t. $(E, i) \models (M' : \phi) \wedge a \mathsf{k} M'$ | 7 |
| 9. | $M' \in \mathcal{M}$ and $(E, i) \models (M' : \phi) \wedge a \mathsf{k} M'$ | hyp. |
| 10. | $(E, i) \models M : \phi \rightarrow \phi'$ | 6 |
| 11. | $(E, i) \models a \mathsf{k} M$ | 6 |
| 12. | $(E, i) \models M' : \phi$ | 9 |
| 13. | $(E, i) \models a \mathsf{k} M'$ | 9 |
| 14. | $b \in \mathcal{A}$ | hyp. |
| 15. | $(E', i') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 16. | $(E', i') \approx^*_{\cup} (E, i)$ | hyp. |
| 17. | $(E', i') \models (b \mathsf{k} M \rightarrow \mathsf{K}_b(\phi \rightarrow \phi')) \wedge \mathsf{K}_b^M(\phi \rightarrow \phi')$ | 10, 14, 15, 16 |
| 18. | $(E', i') \models (b \mathsf{k} M' \rightarrow \mathsf{K}_b(\phi)) \wedge \mathsf{K}_b^{M'}(\phi)$ | 12, 14, 15, 16 |

19. $(E', i') \models b \mathsf{k} (M, M')$ hyp.
20. $(E', i') \models b \mathsf{k} M$ 19, property of $\mathsf{k}$
21. $(E', i') \models b \mathsf{k} M'$ 19, property of $\mathsf{k}$
22. $(E', i') \models \mathsf{K}_b(\phi \to \phi')$ 17, 20
23. $(E', i') \models \mathsf{K}_b(\phi)$ 18, 21
24. $(E', i') \models \mathsf{K}_b(\phi')$ 22, 23, $\mathbf{K}(\mathsf{K})$
25. if $(E', i') \models b \mathsf{k} (M, M')$ then $(E', i') \models \mathsf{K}_b(\phi')$ 19–24
26. $(E', i') \models b \mathsf{k} (M, M') \to \mathsf{K}_b(\phi')$ 25
27. $M'' \in \mathcal{M}$ hyp.
28. $S = (E' \lfloor i' \cdot \mathtt{Rcv}(b, M'') \cdot E' \rfloor i' + 1, i' + 1)$ hyp.
29. $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} (M, M')$ hyp.
30. $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} M$ 29, property of $\mathsf{k}$
31. $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} M'$ 29, property of $\mathsf{k}$
32. $(E', i') \models \mathsf{K}_b^M(\phi \to \phi')$ 17
33. $S \models \mathsf{K}_b(\phi \to \phi')$ 27, 28, 30, 32
34. $(E', i') \models \mathsf{K}_b^{M'}(\phi)$ 18
35. $S \models \mathsf{K}_b(\phi)$ 27, 28, 31, 34
36. $S \models \mathsf{K}_b(\phi')$ 33, 35, $\mathbf{K}(\mathsf{K})$
37. if $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} (M, M')$ then $S \models \mathsf{K}_b(\phi')$ 29–36
38. if $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} (M, M')$ then $(E' \lfloor i' \cdot \mathtt{Rcv}(b, M'') \cdot E' \rfloor i' + 1, i' + 1) \models \mathsf{K}_b(\phi')$ 28, 37
39. if $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} (M, M')$ then $(E' \lfloor i' \cdot \mathtt{Rcv}(b, M'') \cdot E' \rfloor i' + 1, i' + 1) \models \mathsf{K}_b(\phi')$ 28–38
40. for all $M'' \in \mathcal{M}$, if $(\mathtt{Rcv}(b, M''), 1) \models b \mathsf{k} (M, M')$ then $(E' \lfloor i' \cdot \mathtt{Rcv}(b, M'') \cdot E' \rfloor i' + 1, i' + 1) \models \mathsf{K}_b(\phi')$ 27–39
41. $(E', i') \models \mathsf{K}_b^{(M,M')}(\phi')$ 40
42. $(E', i') \models (b \mathsf{k} (M, M') \to \mathsf{K}_b(\phi')) \wedge \mathsf{K}_b^{(M,M')}(\phi')$ 26, 41
43. if $(E', i') \approx_{\cup}^* (E, i)$ then $(E', i') \models (b \mathsf{k} (M, M') \to \mathsf{K}_b(\phi')) \wedge \mathsf{K}_b^{(M,M')}(\phi')$ 16–42
44. for all $(E', i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E', i') \approx_{\cup}^* (E, i)$ then $(E', i') \models (b \mathsf{k} (M, M') \to \mathsf{K}_b(\phi')) \wedge \mathsf{K}_b^{(M,M')}(\phi')$ 15–43
45. $(E, i) \models \mathsf{CK}((b \mathsf{k} (M, M') \to \mathsf{K}_b(\phi')) \wedge \mathsf{K}_b^{(M,M')}(\phi'))$ 44
46. $(E, i) \models (M, M') :_b \phi'$ 45
47. for all $b \in \mathcal{A}$, $(E, i) \models (M, M') :_b \phi'$ 14–46
48. $(E, i) \models \forall b((M, M') :_b \phi')$ 47
49. $(E, i) \models (M, M') : \phi'$ 48
50. $(E, i) \models a \mathsf{k} (M, M')$ 11, 13
51. $(E, i) \models ((M, M') : \phi') \wedge a \mathsf{k} (M, M')$ 49, 50

52. there is $M'' \in \mathcal{M}$ s.t. $(E,i) \models (M'' : \phi') \wedge a \mathsf{k} M''$ 51
53. $(E,i) \models \exists m((m : \phi') \wedge a \mathsf{k} m)$ 52
54. $(E,i) \models \mathsf{P}_a(\phi')$ 53
55. $(E,i) \models \mathsf{P}_a(\phi')$ 8–54
56. $(E,i) \models \mathsf{P}_a(\phi')$ 5–55
57. if $(E,i) \models \mathsf{P}_a(\phi)$ then $(E,i) \models \mathsf{P}_a(\phi')$ 3–56
58. $(E,i) \models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi')$ 57
59. if $(E,i) \models \mathsf{P}_a(\phi \rightarrow \phi')$ then $(E,i) \models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi')$ 2–58
60. for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, if $(E,i) \models \mathsf{P}_a(\phi \rightarrow \phi')$ then $(E,i) \models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi')$ 1–59
61. $\mathsf{P}_a(\phi \rightarrow \phi') \Rightarrow \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi')$ 60, Definition 2.3
62. $\models \mathsf{P}_a(\phi \rightarrow \phi') \rightarrow (\mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\phi'))$ 61, Lemma 2.5

□

**Proposition 2.9** $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{K}_a(\phi)$

**Proof.**

1. $(E,i) \in \mathcal{E}^* \times \mathbb{N}$ hyp.
2. $(E,i) \models \mathsf{P}_a(\phi)$ hyp.
3. $(E,i) \models \exists m((m : \phi) \wedge a \mathsf{k} m)$ 2
4. there is $M \in \mathcal{M}$ s.t. $(E,i) \models (M : \phi) \wedge a \mathsf{k} M$ 3
5. $M \in \mathcal{M}$ and $(E,i) \models (M : \phi) \wedge a \mathsf{k} M$ hyp.
6. $(E,i) \models M : \phi$ 5
7. $(E,i) \models a \mathsf{k} M$ 5
8. $(E,i) \models a \mathsf{k} M \rightarrow \mathsf{K}_a(\phi)$ 6, $\mathbf{T}(\mathsf{CK})$
9. $(E,i) \models \mathsf{K}_a(\phi)$ 7, 8
10. $(E,i) \models \mathsf{K}_a(\phi)$ 4–9
11. if $(E,i) \models \mathsf{P}_a(\phi)$ then $(E,i) \models \mathsf{K}_a(\phi)$ 2–10
12. for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, if $(E,i) \models \mathsf{P}_a(\phi)$ then $(E,i) \models \mathsf{K}_a(\phi)$ 1–11
13. $\mathsf{P}_a(\phi) \Rightarrow \mathsf{K}_a(\phi)$ 12, Definition 2.3
14. $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{K}_a(\phi)$ 13, Lemma 2.5

□

**Proposition 2.10** $\models \mathsf{P}_a(\phi) \rightarrow \phi$

**Proof.**

1. $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{K}_a(\phi)$ Proposition 2.9
2. $\models \mathsf{K}_a(\phi) \rightarrow \phi$ $\mathbf{T}(\mathsf{K})$
3. $\models \mathsf{P}_a(\phi) \rightarrow \phi$ 1, 2

□

**Proposition 2.11** $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\mathsf{P}_a(\phi))$

**Proof.**

| | | |
|---|---|---|
| 1. | $(E,i) \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 2. | $(E,i) \models \mathsf{P}_a(\phi)$ | hyp. |
| 3. | $(E,i) \models \exists m((m:\phi) \wedge a \,\mathsf{k}\, m)$ | 2 |
| 4. | there is $M \in \mathcal{M}$ s.t. $(E,i) \models (M:\phi) \wedge a \,\mathsf{k}\, M$ | 3 |
| 5. | $M \in \mathcal{M}$ and $(E,i) \models M:\phi \wedge a \,\mathsf{k}\, M$ | hyp. |
| 6. | $b \in \mathcal{A}$ | hyp. |
| 7. | $(E',i') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 8. | $(E',i') \approx^*_{\cup} (E,i)$ | hyp. |
| 9. | $(E,i) \models M:\phi$ | 5 |
| 10. | $(E',i') \models b \,\mathsf{k}\, [M]_a$ | hyp. |
| 11. | $(E,i) \models b \,\mathsf{k}\, [M]_a$ | 8, 10, property of $\approx^*_{\cup}$ |
| 12. | $(E,i) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 9, 11, Lemma 2.7 |
| 13. | $(E',i') \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 8, 12, property of $\approx^*_{\cup}$ |
| 14. | if $(E',i') \models b \,\mathsf{k}\, [M]_a$ then $(E',i') \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 10–13 |
| 15. | $(E',i') \models b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 14 |
| 16. | $M' \in \mathcal{M}$ | hyp. |
| 17. | $(\mathtt{Rcv}(b,M'),1) \models b \,\mathsf{k}\, [M]_a$ | hyp. |
| 18. | $(\mathtt{Rcv}(b,M'),1) \models \mathsf{K}_b(a \,\mathsf{k}\, [M]_a)$ | 17, Lemma 2.6 |
| 19. | $(\mathtt{Rcv}(b,M'),1) \models a \,\mathsf{k}\, [M]_a$ | 18, $\mathbf{T}(\mathsf{K})$ |
| 20. | not $(\mathtt{Rcv}(b,M'),1) \models a \,\mathsf{k}\, [M]_a$ | property of $\mathsf{k}$ [7] |
| 21. | false | 19, 20 |
| 22. | $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M') \cdot E'\rfloor i'+1, i'+1) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 21 |
| 23. | if $(\mathtt{Rcv}(b,M'),1) \models b \,\mathsf{k}\, [M]_a$ then $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M') \cdot E'\rfloor i'+1, i'+1) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 17–22 |
| 24. | for all $M' \in \mathcal{M}$, if $(\mathtt{Rcv}(b,M'),1) \models b \,\mathsf{k}\, [M]_a$ then $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M') \cdot E'\rfloor i'+1, i'+1) \models \mathsf{K}_b(\mathsf{P}_a(\phi))$ | 16–23 |
| 25. | $(E',i') \models \mathsf{K}_b^{[M]_a}(\mathsf{P}_a(\phi))$ | 24 |
| 26. | $(E',i') \models (b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))) \wedge \mathsf{K}_b^{[M]_a}(\mathsf{P}_a(\phi))$ | 15, 25 |
| 27. | if $(E',i') \approx^*_{\cup} (E,i)$ then $(E',i') \models (b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))) \wedge \mathsf{K}_b^{[M]_a}(\mathsf{P}_a(\phi))$ | 8–26 |
| 28. | for all $(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E',i') \approx^*_{\cup} (E,i)$ then $(E',i') \models (b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))) \wedge \mathsf{K}_b^{[M]_a}(\mathsf{P}_a(\phi))$ | 7, 27 |
| 29. | $(E,i) \models \mathsf{CK}((b \,\mathsf{k}\, [M]_a \rightarrow \mathsf{K}_b(\mathsf{P}_a(\phi))) \wedge \mathsf{K}_b^{[M]_a}(\mathsf{P}_a(\phi)))$ | 28 |
| 30. | $(E,i) \models [M]_a :_b \mathsf{P}_a(\phi)$ | 29 |
| 31. | for all $b \in \mathcal{A}$, $(E,i) \models [M]_a :_b \mathsf{P}_a(\phi)$ | 6–30 |
| 32. | $(E,i) \models \forall b([M]_a :_b \mathsf{P}_a(\phi))$ | 31 |
| 33. | $(E,i) \models [M]_a : \mathsf{P}_a(\phi)$ | 32 |

[7] there is not a single event for $a$ (only a single one for $b$)

| | | |
|---|---|---|
| 34. | $(E,i) \models a \mathsf{k} M$ | 5 |
| 35. | $(E,i) \models a \mathsf{k} [M]_a$ | 34, property of $\mathsf{k}$ |
| 36. | $(E,i) \models ([M]_a : \mathsf{P}_a(\phi)) \wedge a \mathsf{k} [M]_a$ | 33, 35 |
| 37. | there is $M' \in \mathcal{M}$ s.t. $(E,i) \models (M' : \mathsf{P}_a(\phi)) \wedge a \mathsf{k} M'$ | 36 |
| 38. | $(E,i) \models \exists m((m : \mathsf{P}_a(\phi)) \wedge a \mathsf{k} m)$ | 37 |
| 39. | $(E,i) \models \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 38 |
| 40. | $(E,i) \models \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 4–39 |
| 41. | if $(E,i) \models \mathsf{P}_a(\phi)$ then $(E,i) \models \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 2–40 |
| 42. | for all $(E,i)$, if $(E,i) \models \mathsf{P}_a(\phi)$ then $(E,i) \models \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 1–41 |
| 43. | $\mathsf{P}_a(\phi) \Rightarrow \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 42, Definition 2.3 |
| 44. | $\models \mathsf{P}_a(\phi) \rightarrow \mathsf{P}_a(\mathsf{P}_a(\phi))$ | 43, Lemma 2.5 |

□

**Proposition 2.12** *if* $\models \phi$ *then* $\models \mathsf{P}_a(\phi)$

**Proof.**

| | | |
|---|---|---|
| 1. | $\models \phi$ | hyp. |
| 2. | $(E,i) \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 3. | $b \in \mathcal{A}$ | hyp. |
| 4. | $(E',i') \in \mathcal{E}^* \times \mathbb{N}$ | hyp. |
| 5. | $(E',i') \models \mathsf{K}_b(\phi)$ | 1, $\mathbf{N}(\mathsf{K})$ |
| 6. | $(E',i') \models b \mathsf{k} a \rightarrow \mathsf{K}_b(\phi)$ | 5 |
| 7. | $M \in \mathcal{M}$ | hyp. |
| 8. | $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M) \cdot E'\rfloor i'+1, i') \models \mathsf{K}_b(\phi)$ | 1, $\mathbf{N}(\mathsf{K})$ |
| 9. | if $(\mathtt{Rcv}(b,M),1) \models b \mathsf{k} a$ then $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M) \cdot E'\rfloor i'+1, i') \models \mathsf{K}_b(\phi)$ | 8 |
| 10. | for all $M \in \mathcal{M}$, if $(\mathtt{Rcv}(b,M),1) \models b \mathsf{k} a$ then $(E'\lfloor i' \cdot \mathtt{Rcv}(b,M) \cdot E'\rfloor i'+1, i') \models \mathsf{K}_b(\phi)$ | 7–9 |
| 11. | $(E',i') \models \mathsf{K}_b^a(\phi)$ | 10 |
| 12. | $(E',i') \models (b \mathsf{k} a \rightarrow \mathsf{K}_b(\phi)) \wedge \mathsf{K}_b^a(\phi)$ | 6, 11 |
| 13. | if $(E',i') \approx_{\cup}^* (E,i)$ then $(E',i') \models (b \mathsf{k} a \rightarrow \mathsf{K}_b(\phi)) \wedge \mathsf{K}_b^a(\phi)$ | 12 |
| 14. | for all $(E',i') \in \mathcal{E}^* \times \mathbb{N}$, if $(E',i') \approx_{\cup}^* (E,i)$ then $(E',i') \models (b \mathsf{k} a \rightarrow \mathsf{K}_b(\phi)) \wedge \mathsf{K}_b^a(\phi)$ | 4–13 |
| 15. | $(E,i) \models \mathsf{CK}((b \mathsf{k} a \rightarrow \mathsf{K}_b(\phi)) \wedge \mathsf{K}_b^a(\phi))$ | 14 |
| 16. | $(E,i) \models a :_b \phi$ | 15 |
| 17. | for all $b \in \mathcal{A}$, $(E,i) \models a :_b \phi$ | 3–16 |
| 18. | $(E,i) \models \forall b(a :_b \phi)$ | 17 |
| 19. | $(E,i) \models a : \phi$ | 18 [8] |
| 20. | $(E,i) \models a \mathsf{k} a$ | property of $\mathsf{k}$ |
| 21. | $(E,i) \models a : \phi \wedge a \mathsf{k} a$ | 19, 20 |

[8] any datum proves a logical triviality (i.e., a tautology), in particular an agent's name

| | | |
|---|---|---|
| 22. | there is $M \in \mathcal{M}$ s.t. $(E,i) \models M : \phi \wedge a \mathsf{k} M$ | 21 |
| 23. | $(E,i) \models \exists m(m : \phi \wedge a \mathsf{k} m)$ | 22 |
| 24. | $(E,i) \models \mathsf{P}_a(\phi)$ | 23 |
| 25. | for all $(E,i) \in \mathcal{E}^* \times \mathbb{N}$, $(E,i) \models \mathsf{P}_a(\phi)$ | 2–24 |
| 26. | $\models \mathsf{P}_a(\phi)$ | 25 |
| 27. | if $\models \phi$ then $\models \mathsf{P}_a(\phi)$ | 1–26 |

□

## 3 Conclusion

We have provided a construction that reduces provability to knowledge in multi-agent systems, thanks to the introduction of a new kind of knowledge, namely *adductive knowledge*. Our resulting *epistemic* definition of proofs is *declarative*, as opposed to operational, in the sense that the definition is formulated in terms of *what* (knowledge) proofs effect in agents, as opposed to how proofs do so. In particular, our definition reflects the effect of mathematical (in the social sense) proofs: if my peer knew my proof of the statement $\phi$ then she would know that $\phi$ is true. (Notice the different kinds of knowledge and the conditional mode!) In contrast, the *traditional* definition of proofs is *operational*, in the sense that it defines proofs in terms of the deductive operations that are used to construct them. Declarative definitions of proofs have numerous advantages over their operational counterparts: (1) generality—abstractness w.r.t. how, (2) succinctness—1 declarative formula as opposed to 1 operational proof system, (3) intuitiveness—concreteness w.r.t. what.

An alternative idea for reducing provability to knowledge in distrusted multi-agent settings was presented in [3,4]. There, the reduction involved a universal quantification over *adjoint* worlds that amounted to a *weak-second*-order universal quantification over (finite sets of) messages, and did not use common knowledge. Whereas in the reduction here, the quantification is a universal *first*-order one over messages, and common knowledge *is* used.

We plan to relate the idea of [3,4] to the idea presented here, and to concretise our ideas on *interactive* provability, i.e., provability in (possibly game-based) *interactive computation*, as sketched in [3, Chapter 5].

**Acknowledgements**

I thank Andrey Rybalchenko for our stimulating discussions on accountable distributed systems.

## References

[1] Blackburn, P., J. van Benthem and F. Wolter, editors, "Handbook of Modal Logic," Studies in Logic and Practical Reasoning **3**, Elsevier, 2007.

[2] Fagin, R., J. Y. Halpern, Y. Moses and M. Y. Vardi, "Reasoning about Knowledge," MIT Press, 1995.

[3] Kramer, S., "Logical Concepts in Cryptography," Ph.D. thesis, Ecole Polytechnique Fédérale de Lausanne (2007), http://library.epfl.ch/en/theses/?nr=3845.

[4] Kramer, S., *Cryptographic Protocol Logic: Satisfaction for (timed) Dolev-Yao cryptography*, Journal of Logic and Algebraic Programming (invited submission, accepted for publication).

# A Modal Sequent Calculus for Propositional Separation Logic

Neelakantan R. Krishnaswami [1]

*Computer Science Department*
*Carnegie Mellon University*
*Pittsburgh, USA*

**Abstract**

In this paper, we give a sequent calculus for separation logic. Unlike the logic of bunched implications, this calculus does not have a tree-shaped context – instead, we use labelled deduction to control when hypotheses can and cannot be used. We prove that cut-elimination holds for this calculus, and show that it is sound with respect to the provability semantics of separation logic.

*Keywords:* Separation logic, sequent calculus, cut-elimination, hybrid logic, labelled deduction

## 1 Introduction

Separation logic [11] is an extension of Hoare logic, designed to make it easier to reason about the behavior of programs making use of aliased mutable state.

In ordinary Hoare logic, a predicate describes a set of program states (in our case, heaps), and a conjunction like $A \wedge B$ holds of a state when that state holds of $A$ and also holds of $B$. Unfortunately, aliasing is quite difficult to treat – if $x$ and $y$ are pointer variables, we need to explicitly state whether they alias or not. So as the number of variables in a program grows, the number of aliasing conditions grows quadratically. Worse still, this defeats modular proof, since as soon as we put a subprogram into a larger one, we need to add aliasing assertions describing possible interference between the subprogram and the larger program.

The key innovation in separation logic is to extend the logic of pre- and post-conditions with the *spatial* connectives $A * B$ and $A -\!\!* B$. Intuitively, we take $A * B$ to hold of a program state when the state can be divided into two *disjoint* parts, one of which holds of $A$ and the other of which holds of $B$. Since the meaning of the connective enforces disjointness, we do not need to write aliasing conditions

[1] Email: neelk@cs.cmu.edu

| | |
|---|---|
| Propositions | $A ::= \top \mid A \wedge B \mid A \to B \mid \bot \mid A \vee B \mid I \mid A * B \mid A -\!\!* B \mid P$ |
| Worlds | $\omega ::= \alpha \mid \epsilon \mid \omega \cdot \omega$ |
| World Contexts | $\Omega ::= \cdot \mid \Omega, \alpha$ |
| Equality Contexts | $\Xi ::= \cdot \mid \Xi, \omega = \omega'$ |
| Hypothetical Contexts | $\Gamma ::= \cdot \mid \Gamma, A[\omega]$ |

Fig. 1. Syntax

explicitly. As in ordinary Hoare logic, separation logic has a rule of consequence:

$$\frac{P \vdash P' \qquad \{P'\}c\{Q'\} \qquad Q \vdash Q'}{\{P\}c\{Q\}}$$

However, the fact that we have a novel logic means that the entailment relation $P \vdash P'$ is also novel – so we need rules to reason about the entailment relation. This is most commonly done in a Hilbert-style deduction system, where axiom schemata are given that allow direct reasoning about entailment, without context-changing operations. However, such schemes are somewhat cumbersome to work with in practice, and it is desirable to have a sequent calculus or natural deduction system.

Our contributions in this paper are:

- First, we present a sequent calculus for separation logic that does not use bunched contexts. Instead, we interpret separation logic as a modal logic, and give a labelled deduction system that uses hybrids/labels to control when hypotheses can be used.
- Second, we prove that cut is an admissible rule for this calculus.
- Third, we show that this calculus is sound with respect to the semantics of separation logic – that is, any tautology provable in this calculus is true in the model.

## 2 The Sequent Calculus

Our logic is the propositional fragment of separation logic. We have $\top$ as truth, $A \wedge B$ as conjunction, $A \to B$ as implication, $\bot$ as falsehood, $A \vee B$ as disjunction, $A * B$ as separating conjunction, $I$ as the unit to the separating conjunction, and $A -\!\!* B$ as the magic wand (i.e., adjoint to separating conjunction). We do not include the points-to connective $e \mapsto e'$, but we do add atomic formulas $P$. The grammar of propositions is given in Figure 1.

The main idea in this calculus is to move from a judgement of truth to a judgement that determines truth at a particular world. So our judgement does not provide a proof that $A$ is true, but rather a proof that $A[\omega]$, which shows that $A$

| | |
|---|---|
| World Well-formedness | $\Omega \vdash \omega : \mathsf{world}$ |
| Equality Context Well-formedness | $\Omega \vdash \Xi\ \mathsf{ok}$ |
| Context Well-formedness | $\Omega \vdash \Gamma\ \mathsf{ok}$ |
| World Equality | $\Omega; \Xi \vdash \omega \equiv \omega'$ |
| Proposition Provability | $\Omega; \Xi; \Gamma \vdash A[\omega]$ |

Fig. 2. Catalog of Judgements

$$\frac{\omega \equiv \omega' \in \Xi \qquad \Omega \vdash \Xi\ \mathsf{ok}}{\Omega; \Xi \vdash \omega \equiv \omega'}\ \textsc{EHyp} \qquad \frac{\Omega; \Xi \vdash \omega \equiv \omega'}{\Omega; \Xi \vdash \omega' \equiv \omega}\ \textsc{ESym}$$

$$\frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \Xi\ \mathsf{ok}}{\Omega; \Xi \vdash \omega \equiv \omega}\ \textsc{ERefl} \qquad \frac{\Omega; \Xi \vdash \omega \equiv \omega' \qquad \Omega; \Xi \vdash \omega' \equiv \omega''}{\Omega; \Xi \vdash \omega \equiv \omega''}\ \textsc{ETrans}$$

$$\frac{\Omega; \Xi \vdash \omega_1 \equiv \omega_2 \qquad \Omega; \Xi \vdash \omega_1' \equiv \omega_2'}{\Omega; \Xi \vdash \omega_1 \cdot \omega_2 \equiv \omega_1' \cdot \omega_2'}\ \textsc{ECat} \qquad \frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot \epsilon \equiv \omega}\ \textsc{EUnit}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot \omega' \equiv \omega' \cdot \omega}\ \textsc{EComm}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world} \qquad \Omega \vdash \omega'' : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot (\omega' \cdot \omega'') \equiv (\omega \cdot \omega') \cdot \omega}\ \textsc{EAssoc}$$

Fig. 3. World Equality

holds at a world $\omega$. Likewise, we change the context from a multiset $A_1, \ldots, A_n$ to a multiset of located hypotheses $\Gamma = A_1[\omega_1], \ldots, A_n[\omega_n]$.

The world annotations themselves are not structureless. They are expressions formed from world variables $\alpha$, concatenation $\omega \cdot \omega'$, and unit $\epsilon$. We give an equality judgement for worlds $\Omega; \Xi \vdash \omega \equiv \omega'$ in Figure 3. This axiomatizes an equivalence relation (i.e., reflexive, transitive, symmetric) which makes the concatenation $\omega \cdot \omega'$ into an associative and commutative operation that has $\epsilon$ as a unit. The free world variables are in $\Omega$, and a novelty of this equality judgement is that it allows the use of the hypothetical equalities found in the context $\Xi$. $\Omega$ is a set of variables, and $\Xi$ is a multiset of equality hypotheses.

Finally, we come to the primary judgement of this calculus, the provability judgement $\Omega; \Xi; \Gamma \vdash A[\omega]$. This can be read as, "in a world variable context $\Omega$, when the equations in $\Xi$ hold, then $A$ is provable at a world $\omega$, under the hypotheses in $\Gamma$."

We catalog all the judgements of the system in Figure 2, and give the auxilliary well-formedness judgments in Figure 4.

Below, we give the inference rules for our separation logic calculus. The hypothesis rule Hyp allows us to conclude that an atomic proposition $P$ holds at $\omega$ when

$P$ can be found at $\omega'$ in the context, and the two worlds are equal.

The intuitionistic rules for $\top$, $A \wedge B$, $A \to B$, $\bot$, and $A \vee B$ all exactly follow the structure of the usual rules of the intuitionistic sequent calculus – the only difference is that we push around an extra world annotation $\omega$. This corresponds to the fact that in the Kripke semantics of separation logic (given at the start of section 4), we never look at the exact shapes of a heap, except in the semantics of the spatial connectives.

The world annotations start to come into play with the spatial connectives. For example, in the EmpR rule, we are allowed to introduce $I$ at $\omega$, whenever we can show that $\omega$ equals the empty world $\epsilon$. Likewise, reading the left rule from bottom to top, the hypothesis that $I[\omega]$ holds lets us add the assumption that $\omega \equiv \epsilon$.

$$\frac{\Omega; \Xi \vdash \omega \equiv \omega' \qquad \Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok}}{\Omega; \Xi; \Gamma, P[\omega] \vdash P[\omega']}\ \textsc{Hyp}$$

$$\frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok}}{\Omega; \Xi; \Gamma \vdash \top[\omega]}\ \textsc{TrueR} \qquad \text{(No TrueL)}$$

$$\frac{\Omega; \Xi; \Gamma \vdash A_1[\omega] \qquad \Omega; \Xi; \Gamma \vdash A_2[\omega]}{\Omega; \Xi; \Gamma \vdash A_1 \wedge A_2[\omega]}\ \textsc{AndR} \qquad \frac{\Omega; \Xi; \Gamma, A[\omega], B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \wedge B[\omega] \vdash C[\omega']}\ \textsc{AndL}$$

$$\frac{\Omega; \Xi; \Gamma, A[\omega] \vdash B[\omega]}{\Omega; \Xi; \Gamma \vdash A \to B[\omega]}\ \textsc{ImpR}$$

$$\frac{\Omega; \Xi; \Gamma, A \to B[\omega] \vdash A[\omega] \qquad \Omega; \Xi; \Gamma, A \to B[\omega], B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \to B[\omega] \vdash C[\omega']}\ \textsc{ImpL} \qquad \text{(No FalseR)}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma, \bot[\omega]\ \mathsf{ok} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega; \Xi; \Gamma, \bot[\omega] \vdash C[\omega']}\ \textsc{FalseL} \qquad \frac{\Omega; \Xi; \Gamma \vdash A[\omega]}{\Omega; \Xi; \Gamma \vdash A \vee B[\omega]}\ \textsc{OrR1}$$

$$\frac{\Omega; \Xi; \Gamma \vdash B[\omega]}{\Omega; \Xi; \Gamma \vdash A \vee B[\omega]}\ \textsc{OrR2} \qquad \frac{\Omega; \Xi; \Gamma, A[\omega] \vdash C[\omega'] \qquad \Omega; \Xi; \Gamma, B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \vee B[\omega] \vdash C[\omega']}\ \textsc{OrL}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok} \qquad \Omega; \Xi \vdash \epsilon \equiv \omega}{\Omega; \Xi; \Gamma \vdash I[\omega]}\ \textsc{EmpR} \qquad \frac{\Omega; \Xi, \epsilon \equiv \omega; \Gamma, I[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, I[\omega] \vdash C[\omega']}\ \textsc{EmpL}$$

$$\frac{\Omega; \Xi; \Gamma \vdash A[\omega_1] \qquad \Omega; \Xi; \Gamma \vdash B[\omega_2] \qquad \Omega; \Xi \vdash \omega \equiv \omega_1 \cdot \omega_2}{\Omega; \Xi; \Gamma \vdash A * B[\omega]}\ \textsc{StarR}$$

$$\frac{\Omega, \alpha, \beta; \Xi, \omega = \alpha \cdot \beta; \Gamma, A * B[\omega], A[\alpha], B[\beta] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A * B[\omega] \vdash C[\omega']}\ \textsc{StarL}$$

$$\frac{\Omega, \alpha; \Xi; \Gamma, A[\alpha] \vdash B[\omega'] \qquad \Omega, \alpha; \Xi \vdash \omega \cdot \alpha \equiv \omega'}{\Omega; \Xi; \Gamma \vdash A \mathrel{-\!\!*} B[\omega]}\ \textsc{WandR}$$

$$\frac{\begin{array}{c}\Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega] \vdash A[\omega''] \\ \Omega; \Xi \vdash \omega \cdot \omega'' \equiv \omega_1 \qquad \Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega], B[\omega_1] \vdash C[\omega']\end{array}}{\Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega] \vdash C[\omega']}\ \textsc{WandL}$$

The rules for $A * B$ are similar, but a little more complicated. In the StarR rule, we can show that $A * B$ holds at $\omega$ whenver we can find a world $\omega_1$ that $A$ holds in, and a world $\omega_2$ that $B$ holds in, such that $\omega$ equals their concatenation – exactly in analogy to the Kripke semantics for the separating conjunction.

The left rule for separating conjunction is the most complex rule in this calculus. If we have $A * B$ as a hypothesis at $\omega$ in the conclusion, then in the premise we can extend the context with two new worlds $\alpha$ and $\beta$, such that $A$ holds at $\alpha$, $B$ holds at $\beta$, and that $\alpha \cdot \beta \equiv \omega$. The analogy to the Kripke semantics is interesting. In the Kripke semantics for separation logic, if a heap (an element of a partial commutative monoid) $h$ satisfies $A * B$, then there is a splitting of $h$ into $h_1$ and $h_2$ such that $h_1$ satisfies $A$ and $h_2$ satisfies $B$. Note that $h_1$ and $h_2$ are existentially quantified in the Kripke semantics. Because we have a separating conjunction as a hypothesis, we have this existential on the left-hand side of an implication. So we can essentially treat the existential as a universal, via the equivalence $(\exists x.P(x)) \supset Q \equiv \forall x.\ P(x) \supset Q$.

Finally we come to the right and left rules for the magic wand $A \mathrel{-\!\!*} B$. The right rule WandR tells us that we can prove that $A \mathrel{-\!\!*} B$ holds at $\omega$, whenever we can show that if $A$ holds at a new world $\alpha$, then $B$ holds at a world equivalent to $\omega \cdot \alpha$. This is in exact analogy to the Kripke semantics. The left rule tells us that if have a wand hypothesis $A \mathrel{-\!\!*} B$ at $\omega$, and can find a proof that $A$ holds at $\omega'$, then we can also assume that $B$ holds at a world equivalent to $\omega \cdot \omega'$ while proving $C$.

$$\frac{\alpha \in \Omega}{\Omega \vdash \alpha : \mathsf{world}}\ \textsc{WHyp} \qquad \frac{}{\Omega \vdash \epsilon : \mathsf{world}}\ \textsc{WEps} \qquad \frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega \vdash \omega \cdot \omega' : \mathsf{world}}\ \textsc{WCat}$$

$$\frac{}{\Omega \vdash \cdot\ \mathsf{ok}}\ \textsc{EqOkNil} \qquad \frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega \vdash \Xi, \omega \equiv \omega'\ \mathsf{ok}}\ \textsc{EqOkCons}$$

$$\frac{}{\Omega \vdash \cdot\ \mathsf{ok}}\ \textsc{CtxOkNil} \qquad \frac{\Omega \vdash \Gamma\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world}}{\Omega \vdash \Gamma, A[\omega]\ \mathsf{ok}}\ \textsc{CtxOkCons}$$

Fig. 4. Auxilliary Judgements

## 3 Proof Theory

Since we only allow the hypothesis rule at atomic propositions, we need to prove that the identity principle holds for this calculus.

**Theorem 3.1 (Identity)** *If* $\Omega \vdash \Xi$ ok, $\Omega \vdash \Gamma$ ok, *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega; \Xi; \Gamma, A[\omega] \vdash A[\omega']$.

The proof is a straightforward induction on the proposition $A$.

Next, we can show that weakening holds for this calculus. Equivalent weakening rules hold (when they make sense) for all of the other judgements. However, for conciseness we will only state the theorems for the case of the main provability judgement.

**Theorem 3.2 (Weakening)** *We have that:*

(i) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$, *then* $\Omega, \alpha; \Xi; \Gamma \vdash A[\omega'']$.

(ii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$ *and* $\Omega \vdash \omega : \mathsf{world}$, *and* $\Omega \vdash \omega' : \mathsf{world}$ *then we have that* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash A[\omega'']$.

(iii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$ *and* $\Omega \vdash \omega : \mathsf{world}$, *then* $\Omega; \Xi; \Gamma, B[\omega'] \vdash A[\omega'']$.

Next, we give a contraction principle for this calculus. As before, a similar contraction principle holds for the other judgements.

**Theorem 3.3 (Contraction)** *We have that:*

(i) *If* $\Omega; \Xi, \omega \equiv \omega', \omega \equiv \omega'; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash C[\omega'']$.

(ii) *If* $\Omega; \Xi; \Gamma, A[\omega], A[\omega'] \vdash C[\omega'']$ *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega, \alpha; \Xi; \Gamma, A[\omega] \vdash C[\omega'']$.

We do not give explicit theorems for Exchange, because we have been treating the contexts as multisets.

Finally, we can show that the cut rule is admissible in this calculus. We have two substitution principles for the world variable and world equation contexts, and a true cut principle for the provability judgement. (And once again, we elide the substitution principles for the other judgements in this calculus.)

**Theorem 3.4 (Admissibility of Cut)** *We have that:*

(i) *If* $\Omega \vdash \omega : \mathsf{world}$ *and* $\Omega, \alpha; \Xi; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi[\omega/\alpha]; \Gamma[\omega/\alpha] \vdash C[\omega''[\omega/\alpha]]$.

(ii) *If* $\Omega; \Xi \vdash \omega \equiv \omega'$ *and* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi; \Gamma \vdash C[\omega'']$.

(iii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega]$, *and* $\Omega; \Xi; \Gamma, A[\omega'] \vdash C[\omega'']$, *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega; \Xi; \Gamma \vdash C[\omega'']$

The first two cases are just structural inductions over the derivation. The interesting case is the third case, which we prove with a structural cut admissibility argument in the style of Pfenning [8]. We do a induction on the size of the type $A$, lexicographically prior to a simultaneous induction on the sizes of the two provability derivations.

## 4 Soundness of the Calculus

In this section, we show that our sequent calculus is sound with respect to the Kripke semantics of separation logic, in the sense that the provable tautologies of our calculus are all equal to true in the semantics.

First, recall the Kripke semantics of separation logic. We write $h$ for a heap (a finite function from locations to values; the whole set of heaps is written $H$) [2]; the predicate $h\#h'$ holds when the domains of $h$ and $h'$ are disjoint; $e$ is the empty heap; and $h \cdot h'$ is the union of two heaps, which is defined when the domains are disjoint. Since we include atoms in our propositional language, this satisfaction relation is also indexed by a function $\gamma \in \text{Atom} \to \mathcal{P}(H)$ to interpret the atoms.

$$
\begin{array}{lll}
h \models_\gamma \top & \text{iff always} \\
h \models_\gamma A \wedge B & \text{iff } h \models_\gamma A \text{ and } h \models_\gamma B \\
h \models_\gamma A \to B & \text{iff if } h \models_\gamma A \text{ then } h \models_\gamma B \\
h \models_\gamma \bot & \text{iff never} \\
h \models_\gamma A \vee B & \text{iff } h \models_\gamma A \text{ or } h \models_\gamma B \\
h \models_\gamma I & \text{iff } h = e \\
h \models_\gamma A * B & \text{iff } \exists h_1, h_2. h = h_1 \cdot h_2 \text{ and } h_1 \models_\gamma A \text{ and } h_2 \models_\gamma B \\
h \models_\gamma A -\!\!* B & \text{iff } \forall h'. \text{ if } h' \models_\gamma A \text{ and } h\#h' \text{ then } h \cdot h' \models_\gamma B \\
h \models_\gamma P & \text{iff } h \in \gamma(P)
\end{array}
$$

Now, we can give interpretation functions for the world expressions and the propositions. We will take a world expression as denoting a particular heap, and since world expressions may have free variables the interpretation will be a mapping from the free world variables to a heap. This can just follow the structure of the world expression – note that since heap concatenation is partial, the interpretation function for worlds is also necessarily partial. We will write $\omega \downarrow \eta$ to mean that the interpretation of $\omega$ is defined under the substitution $\eta$.

$$
\begin{array}{ll}
[\![\epsilon]\!]\eta & = e \\
[\![\alpha]\!]\eta & = \eta(\alpha) \\
[\![\omega \cdot \omega']\!]\eta & = [\![\omega]\!]\eta \cdot [\![\omega']\!]\eta
\end{array}
$$

We will also need an interpretation of propositions, which we will take to be the set of heaps satisfying the proposition.

$$[\![A]\!]\gamma = \{h \mid h \models_\gamma A\}$$

To show soundness, we first show that the equality judgement is sound.

**Lemma 4.1 (Soundness of Equality)** *If we have that:*

- $\Omega; \Xi \vdash \omega \equiv \omega'$,
- $\omega_i \downarrow \eta$, *and* $\omega_i' \downarrow \eta$, *and* $[\![\omega_i]\!]\eta = [\![\omega_i']\!]\eta$ *for every* $\omega_i \equiv \omega_i'$ *in* $\Xi$, *and*
- $\omega \downarrow \eta$ *or* $\omega' \downarrow \eta$

*then we know that* $\omega \downarrow \eta$ *and* $\omega' \downarrow \eta$ *and* $[\![\omega]\!]\eta = [\![\omega']\!]\eta$

[2] In fact, the following section does not depend specifically on heaps. The algebraic structure we need is a separation algebra [3], which is just a partial commutative monoid.

The proof is a routine induction on the equality judgement. Armed with this lemma, we can give a soundness theorem for the sequent calculus:

**Theorem 4.2 (Soundness of the Sequent Calculus)** *If we have that:*

- $\Omega; \Xi; \Gamma \vdash A[\omega]$,
- $\eta \in \Omega \to H$,
- $\gamma \in Atom \to \mathcal{P}(H)$
- $\omega_i \downarrow \eta$, *and* $\omega_i' \downarrow \eta$, *and* $[\![\omega_i]\!]\eta = [\![\omega_i']\!]\eta$ *for every* $\omega_i \equiv \omega_i'$ *in* $\Xi$, *and*
- $\omega_j \downarrow \eta$ *and* $[\![\omega_j]\!]\eta \in [\![A_j]\!]\gamma$ *for every* $A_j[\omega_j]$ *in* $\Gamma$,

*then we can conclude that if* $\omega \downarrow \eta$, *then* $[\![\omega]\!]\eta \in [\![A]\!]\gamma$ *holds.*

The proof follows from an induction on the structure of the derivation. As an immediate corollary, it follows that if we can derive $\alpha; \cdot; \cdot \vdash A[\alpha]$, then $A$ is a true proposition of separation logic.

### *4.1 (In)Completeness*

While our calculus is sound, it is not even remotely complete with respect to the semantics. First, the set of heaps forms a boolean algebra, which means that the semantics validates the law of the excluded middle. Since we have an intuitionistic calculus, we cannot prove this. This problem might be rectified by extending the sequent calculus with multiple conclusions, to support classical reasoning.

However, this is not sufficient. Our equality judgement only allows us to make positive judgements about equality – and for completeness, we will need some way to reason from *inequality*. Concretely, suppose we add the points-to assertion $e \mapsto v$, which asserts that we have a one-element heap with location $e$ pointing to value $v$. Now, consider the separation logic assertion $(x \mapsto -) * (x \mapsto -)$. This formula must entail false, because we know that the same pointer cannot be in two disjoint heaps and hence the formula is unsatisfiable. Such a deduction is not possible unless we have a way of deducing inequalities from world expressions.

## 5 Future and Related Work

### *5.1 Future Work*

There are a number of directions to proceed from here. First, for practical use it is necessary to add support for the points-to predicate, perhaps by extending the language of worlds to refer more explicitly to the contents of a heap. This is an interesting question even though it is known [4] that the points-to predicate and equality are sufficient to make judging validity undecidable – there might still be proof-theoretically well-behaved systems (in the sense of admitting cut-elimination) that contain points-to.

Doing this is a fairly delicate operation. One of the key features of separation logic that simplifies reasoning is that we do not normally need to track the aliasing of worlds. The calculus we have presented supports this property: even though heaps only have a partial notion of concatenation, we never need to track whether

two world expressions are catenable or not. Retaining this property and at the same time allowing the controlled use of this knowledge in proofs (for example, if we know $x \mapsto u * y \mapsto v$, we want to be able to deduce that $x \neq y$) is tricky. In particular, the fact that these facts are inequalities is difficult to handle intuitionistically, since inequality is a derived connective.

Finally, in program proofs using separation logic, it is typical to identify and make use of special classes of formulas (such as the pure propositions, whose truth does not depend on the heap; or the precise propositions, which unambiguously identify a piece of state) which satisfy additional axioms. It would be interesting to see if we can extend this calculus with modalities corresponding to those classes.

### *5.2 Related Work*

Pym's original work on bunched implications [9,7] includes a natural deduction and sequent calculus for BI with a branching, tree-structured context. Even though the metatheory is very elegant, actually writing proofs in this calculus is quite complicated. This leads Hoare calculi that use separation logic to typically take the drastic step of abolishing the context altogether. A collection of tautologies of separation logic are given, and proofs done via Hilbert-style reasoning with them. Whenever this becomes too inconvenient, semantic arguments are used. While unquestionably effective, these proofs are often clumsy to read and write.

This is also a problem Bean [1] sought to address, by giving a Fitch-style presentation of natural deduction for BI, called the ribbon calculus. This calculus extends the scoping rules of the regular Fitch style into the second dimension, with a (literally!) spatial scoping principle for the $*$ and $-\!\!*$ connectives. While visually appealing, two-dimensional contexts are tricky to mechanize.

We sought to take a middle ground, and retain a context that is a traditional multiset. Our hope is that this will allow writing relatively natural proofs, without having to resort to metatheoretic arguments in common program proofs, while still being amenable to machine checking.

Agostino and Gabbay [5] proposed labelled deduction as a general methodology for extending the methods for classical theorem proving to cope with intuitionistic and substructural logics. In his doctoral thesis, Simpson [12] shows how to use a labelled calculus to give a proof theory for modal logic, in which the labels are drawn from the Kripke semantics of modal logic.

Galmiche and Mery [6] describe a tableaux method for theorem proving in propositional BI. This work contains the key idea of using monoidal labels to control where BI formulas can and cannot be used. However, they must enrich this structure with an extra preorder structure in order to prevent the provability of formulas like $(A \wedge I) \to (A * A)$, which is not a valid formula of BI. However, we observed that all such anomalies are true theorems of separation logic, which permits us to leave out this preorder structure and simplify our calculus.

Braüner and de Paiva [2] present a natural deduction system for a hybrid propositional logic with a satisfaction operator $a : A$, which is a proposition that asserts that $A$ holds at the world $a$.

Reed [10] integrates a hybrid logic with monoidal labels into the dependent type

theory LF. The context in his system is not explicitly labelled; instead, there is a preorder on worlds, and hypotheses implicitly exist at the least world. Hypotheses are restricted to particular worlds via a hybrid "@" modality. This system can express many substructural types, including a substantial fragment of bunched logic, including the magic wand. However, it cannot fully model the separating conjunction. This is because Reed system leaves out explicit equality hypotheses, in order to make world equality decidable – without the hypothetical equalities, world equality is checkable via ACU unification. In our system, we make the opposite tradeoff: the StarL rule can introduce new hypothetical equalities, which greatly complicates the problem of deciding equality.

# References


[1] Julian Michael Lewis Bean. *Ribbon Proofs – A Proof System for the Logic of Bunched Implications*. PhD thesis, Queen Mary University of London, January 2006.

[2] Torben Braüner and Valeria de Paiva. Intuitionistic hybrid logic. *Journal of Applied Logic*, 4(3):231–255, 2006.

[3] Cristiano Calcagno, Peter W. O'Hearn, and Hongseok Yang. Local action and abstract separation logic. In *LICS*, pages 366–378. IEEE Computer Society, 2007.

[4] Cristiano Calcagno, Hongseok Yang, and Peter W. O'Hearn. Computability and complexity results for a spatial assertion language for data structures. In *APLAS*, pages 289–300, 2001.

[5] Marcello D'Agostino and Dov M. Gabbay. A generalization of analytic deduction via labelled deductive systems. part i: Basic substructural logics. *J. Autom. Reasoning*, 13(2):243–281, 1994.

[6] Didier Galmiche and Daniel Méry. Semantic labelled tableaux for propositional bi. *J. Log. Comput.*, 13(5):707–753, 2003.

[7] Peter W. O'Hearn and David J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[8] Frank Pfenning. Structural cut elimination: I. intuitionistic and classical logic. *Inf. Comput.*, 157(1-2):84–141, 2000.

[9] D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002. Errata and Remarks maintained at: http://www.cs.bath.ac.uk/~pym/BI-monograph-errata.pdf.

[10] Jason Reed. Hybridizing a logical framework. *Electronic Notes in Theoretical Computer Science*, 174(6):135–148, 2007.

[11] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *LICS*, pages 55–74. IEEE Computer Society, 2002.

[12] Alex Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, December 1993.

or with entcsmacro.sty for your meeting. Both can be found at the ENTCS Macro Home Page.

# Calculi for an Intuitionistic Hybrid Modal Logic

Didier Galmiche and Yakoub Salhi [1]

*LORIA UMR 7503 - Université Henri Poincaré*
*Campus Scientifique, BP 239*
*54506 Vandœuvre-les-Nancy, France*

Abstract

In this paper we study proof-search in an intuitionistic hybrid modal logic (for places), denoted $IHML^P$, whose modalities allow us to validate properties taking into account the notion of *place*. In this context we propose different sequent calculi for this logic and also tableau rules in the perspective of proof-search and countermodel generation. As this logic can be seen as an instance of *Hybrid IS5* we can derive new calculi and procedures for this logic. Finally we define a terminating calculus for the $\Box$-free fragment of $IHML^P$ and then propose a decision procedure with countermodel generation.

*Keywords:* Intuitionistic modal logic, sequent calculus, proof-search, semantics, countermodels.

## 1 Introduction

In order to model heterogeneous environments, among them distributed systems, recent works provide logical foundations tuned to programming in such environments, like an intuitionistic modal logic with an operational interpretation of logical proofs as distributed programs [9]. Such a logic allows us to deal with systems seen as a set of different nodes, called *places*, that may have different properties and may contain different resources. It has been recently enriched with the disjunctive connective $\vee$ and the constant $\bot$ in order to obtain an intuitionistic hybrid modal logic (for places) [4], denoted here $IHML^P$, that is suitable for reasoning about distribution of resources. In this context we can mention related works based on separation logics [13] and resource logics like BI [12] and their extensions with modalities [1,11]. Our general aim consists in studying such modal logics dealing with notions of *locations* or *places* in both perspectives of expressiveness and proof and countermodel search.

Here we aim at focusing on the modal logic $IHML^P$ for which several results have been proposed in [4]: two semantics, namely a Kripke semantics and a birelational semantics, both proved sound and complete; the finite model property w.r.t. birelational semantics and then decidability of the logic. The formulae in this logic include names, called *places* and assertions are associated with places and validated in places. A key point is that we are not

[1] Email: galmiche@loria.fr , salhi@loria.fr

only interested in whether a formula is true but also in where a formula is true. Therefore modalities allow us to express a property to be validated in a specific place $p$ (@p), or in a unspecified place ($\Diamond$) or in any place ($\Box$). As the first modality internalizes the model in the logic, this modal logic can also be classified as a hybrid logic [2].
In this paper we aim at studying this logic in the perspective of proof and countermodel search by defining sequent calculi as an alternative to existing natural deduction systems. A first contribution consists of a sequent calculus for $IHML^P$ and its refinements in which contraction and weakening rules are absorbed in the axioms and logical rules. We prove the cut-elimination property and then the soundness and completeness of this calculus. From these results we derive a multi-conclusioned calculus for $IHML^P$ and then tableaux rules for this logic in which the so-called COPY rule is absorbed. As this logic can be seen as the hybridisation of the intuitionistic modal system $IS5$ [3] we can deduce, from our results, new calculi and decision procedures for this logic. Another contribution is the definition of a terminating calculus for the $\Box$-free fragment of $IHML^P$. Its completeness proof provides a way to build countermodels in case of non-validity. Moreover we show, for this fragment, the finite model property w.r.t. the Kripke semantics and thus derive the same result for IS5 without $\Box$.

## 2 An Intuitionistic Modal Logic

In this section, we summarize the key notions about an hybrid intuitionistic modal logic (of places) that we denote $IHML^P$ [4]. It is designed to reason about places with assertions of the form $(G \ \mathsf{at} \ p)$ meaning that the formula $G$ is valid at place $p$. In such an assertion $G$ does not contain any occurrence of the construct $\mathsf{at}$ but use modalities $@p$, one for each place, to cast the meta-linguistic $\mathsf{at}$ at the language level. The logic also has other modalities for reasoning about properties valid at different locations. It corresponds to the logic introduced in [9] enriched with the connectives $\vee$ and $\bot$.
The set of *pure formulae*, denoted $\mathsf{Form}(\mathsf{PL})$, is defined inductively from a set of propositional *variables*, denoted $\mathsf{Var}$, with $\bot$ constant and from a countable set of *places* $\mathsf{PL}$: $\mathcal{F} ::= V \mid \bot \mid \mathcal{F} \wedge \mathcal{F} \mid \mathcal{F} \vee \mathcal{F} \mid \mathcal{F} \supset \mathcal{F} \mid \mathcal{F} @ p \mid \Box \mathcal{F} \mid \Diamond \mathcal{F}$ where $V \in \mathsf{Var}$ and $p \in \mathsf{PL}$.
The assertions of the form $G \ \mathsf{at} \ p$ are called *sentences*. The sequents are of the following form: $\Gamma;\Delta \vdash^P G \ \mathsf{at} \ p$. $\Gamma$ is a finite multiset of *pure formulae* called the *global context*, and contains assumptions that are valid everywhere; $\Delta$ is a finite multiset of *sentences* called the *local context*, and contains assumptions that are valid locally; $G \ \mathsf{at} \ p$ is a sentence called the *conclusion* and $P$ is a finite set of places.
Let us mention that $P + q$ denotes the disjoint union of $P$ and $\{q\}$ and that $PL(S)$ denotes the set of places that appear in the syntactic object $S$.
The sequent $\Gamma;\Delta \vdash^P G \ \mathsf{at} \ p$ is said to be defined iff the set of places $PL(\Gamma) \cup PL(\Delta) \cup PL(G \ \mathsf{at} \ p)$ is a subset of $P$. It has been proved in [4] that for $P = PL(\Gamma) \cup PL(\Delta) \cup PL(G \ \mathsf{at} \ p)$, if $P \subseteq P'$ then $\Gamma;\Delta \vdash^P G \ \mathsf{at} \ p$ is valid iff $\Gamma;\Delta \vdash^{P'} G \ \mathsf{at} \ p$ is valid. Therefore, by assuming that $P$ is finite, there is no loss of generality.

A birelational semantics, similar to the one proposed in [14], have been defined in [4]. It allows to show the finite model property and the decidability of this logic. In this paper, we focus on the Kripke semantics that is similar to the one given for the intuitionistic system IS5 knowing that the logic corresponds to $IS5$ extended with the @ operator [3].

$$\frac{}{A \text{ at } p \vdash^P A \text{ at } p}\ [ID] \qquad \frac{}{\bot \text{ at } p \vdash^P G \text{ at } p'}\ [\bot]$$

$$\frac{\Gamma;\Delta \vdash^P G \text{ at } p'}{\Gamma;\Delta, A \text{ at } p \vdash^P G \text{ at } p'}\ [W_L^1] \qquad \frac{\Gamma;\Delta \vdash^P G \text{ at } p'}{\Gamma, A;\Delta \vdash^P G \text{ at } p'}\ [W_L^2]$$

$$\frac{\Gamma;\Delta, A \text{ at } p, A \text{ at } p \vdash^P G \text{ at } p'}{\Gamma;\Delta, A \text{ at } p \vdash^P G \text{ at } p'}\ [C_L] \qquad \frac{\Gamma, A;\Delta, A \text{ at } p \vdash^P G \text{ at } p'}{\Gamma, A;\Delta \vdash^P G \text{ at } p'}\ [COPY]$$

$$\frac{\Gamma;\Delta \vdash^P A \text{ at } p \qquad \Gamma;\Delta, A \text{ at } p \vdash^P G \text{ at } p'}{\Gamma;\Delta \vdash^P G \text{ at } p'}\ [CUT_1] \qquad \frac{\Gamma;\Delta \vdash^{P+q} A \text{ at } q \qquad \Gamma, A;\Delta \vdash^P G \text{ at } p'}{\Gamma;\Delta \vdash^P G \text{ at } p'}\ [CUT_2]$$

Figure 1. Axioms and Structural Rules of $SC_1^@$

**Definition 2.1** [Kripke model] $\mathcal{K} \equiv (K, \leqslant, \{P_k\}_{k\in K}, \{I_k\}_{k\in K})$ is a *Kripke model* iff
- $K$ is a non-empty set partially ordered by $\leqslant$;
- for every $k \in K$, $P_k$ is a set of places such that for all $k \leqslant l$, $P_k \subseteq P_l$;
- for every $k \in K$, $I_k : \mathsf{Var} \to 2^{P_k}$ is such that for all $k \leqslant l$ and $V \in \mathsf{Var}$ we have $I_k(V) \subseteq I_l(V)$.
The set of places $\bigcup_{k\in K} P_k$ is denoted by $Pls(\mathcal{K})$.

**Definition 2.2** [Kripke semantics] Let $\mathcal{K} \equiv (K, \leqslant, \{P_k\}_{k\in K}, \{I_k\}_{k\in K})$ be a Kripke model, $k \in K$, $p \in P_k$ and a pure formula $A$ with $PL(A) \subseteq P_k$, we define $(k,p) \vDash A$ as follows:
$(k,p) \vDash X$ iff $p \in I_k(X)$ for $X \in \mathsf{Var}$;
$(k,p) \vDash \bot$ never;
$(k,p) \vDash A \wedge B$ iff $(k,p) \vDash A$ and $(k,p) \vDash B$;
$(k,p) \vDash A \vee B$ iff $(k,p) \vDash A$ or $(k,p) \vDash B$;
$(k,p) \vDash A \supset B$ iff for all $l \geqslant k$, if $(l,p) \vDash A$ then $(l,p) \vDash B$;
$(k,p) \vDash A@q$ iff $q \in P_k$ and $(k,q) \vDash B$;
$(k,p) \vDash \Box A$ iff for all $l \geqslant k$ and for all $q \in P_l$, $(l,q) \vDash A$;
$(k,p) \vDash \Diamond A$ iff there exists $q \in P_k$, $(k,q) \vDash A$.

Let us remind that the relation $\vDash$ satisfies the Kripke monotonicity property, i.e., if $l \geqslant k$ then $(k,p) \vDash A$ implies $(l,p) \vDash A$ [4]. We write $k \vDash \Gamma;\Delta$ for $\Gamma$ a global context and $\Delta$ a local context iff for every $A \in \Gamma$ and $p \in P_k$, $(k,p) \vDash \Box A$; and for every $B$ at $q \in \Delta$, and $q \in P_k$, $(k,q) \vDash B$. The sequent $\Gamma;\Delta \vdash^P C$ at $p$ is valid in the Kripke model $\mathcal{K} = (K, \leqslant, \{P_k\}_{k\in K}, \{I_k\}_{k\in K})$ iff $PL(\Gamma) \cup PL(\Delta) \cup PL(C) \cup \{p\} \subseteq P$; and for every $k \in K$ such that $P \subseteq P_k$, if $k \vDash \Gamma;\Delta$ then $(k,p) \vDash C$. We say that $\Gamma;\Delta \vdash^P A$ at $p$ is valid iff it is valid in every Kripke model.

## 3 Sequent Calculi for $IHML^P$

In this section, we define a first sequent calculus $SC_1^@$ for $IHML^P$. It is obtained by extending a calculus for the fragment without $\vee$ and $\bot$ [8]. Axioms and structural rules are given in Figure 1 and logical rules are given in Figure 2. Let $\mathcal{S}$ be a sequent $(\Gamma;\Delta \vdash^P G \text{ at } p)$ we write $\rhd_{SC_1^@} \mathcal{S}$ to express that $\mathcal{S}$ is derivable in $SC_1^@$.

**Theorem 3.1 (Soundness)** *Let $\mathcal{S}$ be a sequent, if $\rhd_{SC_1^@} \mathcal{S}$ then $\mathcal{S}$ is valid.*

**Proof** For every rule, we suppose that its premises are valid in every Kripke model, and we prove that its conclusion is valid in every Kripke model. Here, we show only the case

$$\frac{\Gamma;\Delta,A \text{ at } p,B \text{ at } p \vdash^P C \text{ at } p'}{\Gamma;\Delta,A\wedge B \text{ at } p \vdash^P C \text{ at } p'}\ [\wedge_L] \qquad \frac{\Gamma;\Delta\vdash^P A \text{ at } p \qquad \Gamma;\Delta\vdash^P B \text{ at } p}{\Gamma;\Delta\vdash^P A\wedge B \text{ at } p}\ [\wedge_R]$$

$$\frac{\Gamma;\Delta\vdash^P A \text{ at } p}{\Gamma;\Delta\vdash^P A\vee B \text{ at } p}\ [\vee_{R_1}] \qquad \frac{\Gamma;\Delta\vdash^P B \text{ at } p}{\Gamma;\Delta\vdash^P A\vee B \text{ at } p}\ [\vee_{R_2}] \qquad \frac{\Gamma;\Delta,A \text{ at } p\vdash^P C \text{ at } p' \qquad \Gamma;\Delta,B \text{ at } p\vdash^P C \text{ at } p'}{\Gamma;\Delta,A\vee B \text{ at } p\vdash^P C \text{ at } p'}\ [\vee_L]$$

$$\frac{\Gamma;\Delta\vdash^P A \text{ at } p \qquad \Gamma;\Delta,B \text{ at } p\vdash^P C \text{ at } p'}{\Gamma;\Delta,A\supset B \text{ at } p\vdash^P C \text{ at } p'}\ [\supset_L] \qquad \frac{\Gamma;\Delta,A \text{ at } p\vdash^P B \text{ at } p}{\Gamma;\Delta\vdash^P A\supset B \text{ at } p}\ [\supset_R]$$

$$\frac{\Gamma;\Delta,A \text{ at } p\vdash^P C \text{ at } p''}{\Gamma;\Delta,A@p \text{ at } p'\vdash^P C \text{ at } p''}\ [@_L] \qquad \frac{\Gamma;\Delta\vdash^P A \text{ at } p}{\Gamma;\Delta\vdash^P A@p \text{ at } p'}\ [@_R]$$

$$\frac{\Gamma,A;\Delta\vdash^P C \text{ at } p'}{\Gamma;\Delta,\Box A \text{ at } p\vdash^P C \text{ at } p'}\ [\Box_L] \qquad \frac{\Gamma;\Delta\vdash^{P+q} A \text{ at } q}{\Gamma;\Delta\vdash^P \Box A \text{ at } p}\ [\Box_R]$$

$$\frac{\Gamma;\Delta,A \text{ at } q\vdash^{P+q} C \text{ at } p'}{\Gamma;\Delta,\Diamond A \text{ at } p\vdash^P C \text{ at } p'}\ [\Diamond_L] \qquad \frac{\Gamma;\Delta\vdash^P A \text{ at } p}{\Gamma;\Delta\vdash^P \Diamond A \text{ at } p'}\ [\Diamond_R]$$

Figure 2. Logical Rules of $SC_1^@$

of $[\Box_R]$ rule. Let $\mathcal{K}$=$(K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a countermodel of $\Gamma\vdash^P \Box A$ at $p$. Then, $\exists k_0\in K$ such that $P\subseteq P_{k_0}$, $k_0\vDash\Gamma;\Delta$ and $(k_0,p)\nvDash\Box A$. Thus, $\exists l_0\geqslant k_0$ and $\exists p_0\in P_{l_0}$ such that $(l_0,p_0)\vDash A$, and from the Kripke monotonicity, $l_0\vDash\Gamma;\Delta$. Let $\mathcal{K}'$=$(K,\leqslant,\{P_k\cap\{q\}\}_{k\in K},\{I'_k\}_{k\in K})$ where for every $A\in\mathsf{Var}$, $I'_k(A)=I_k(A)\cap\{q\}$ if $p_0\in I_k(A)$ and $I'_k(A)=I_k(A)$ otherwise. In $\mathcal{K}'$, the new place $q$ duplicated $p_0$. Hence for all formulae $\mathcal{F}$, $(l_0,p_0)\vDash\mathcal{F}$ if and only if $(l_0,q)\vDash\mathcal{F}$. It is easy to show that $\mathcal{K}'$ is a Kripke model. Since $q$ duplicating $p_0$, we have $l_0\vDash\Gamma;\Delta$ and $(l_0,q)\vDash A$ in $\mathcal{K}'$. Therefore, $\mathcal{K}'$ is a countermodel of $\Gamma;\Delta\vdash^{P+q} A$ at $q$. As $\Gamma;\Delta\vdash^{P+q}A$ at $q$ is valid, we get a contradiction and we deduce that $\Gamma\vdash^P\Box A$ at $p$ is valid. □

**Theorem 3.2 (Completeness)** *Let $\mathcal{S}$ be a sequent, if $\mathcal{S}$ is valid then $\rhd_{SC_1^@}\mathcal{S}$.*

**Proof** We consider the validity through the natural deduction system introduced in [8] and extended in [4]. Let $\mathcal{S}=\Gamma;\Delta\vdash^P G$ at $p'$. We suppose that $\mathcal{S}$ is derivable in the natural deduction system, and we prove by induction on the depth of the given derivation in the natural deduction system that $\rhd_{SC_1^@}\mathcal{S}$. We only prove it when the derivation ends with $\Diamond$-elimination:

$$\frac{\Gamma;\Delta\vdash^P \Diamond A \text{ at } p \qquad \Gamma;\Delta,A \text{ at } q\vdash^{P+q} G \text{ at } p'}{\Gamma;\Delta\vdash^P G \text{ at } p'}\ [\Diamond_E]$$

By induction hypothesis, we have derivations for $\Gamma;\Delta\vdash^P\Diamond A$ at $p$ and $\Gamma;\Delta,A$ at $q\vdash^{P+q}$ $G$ at $p'$. Then, by using $[\Diamond_L]$ and $[CUT_1]$, we obtain a derivation for $\Gamma;\Delta\vdash^P G$ at $p'$:

$$\dfrac{\Gamma;\Delta\vdash^P \Diamond A \text{ at } p \qquad \dfrac{\Gamma;\Delta,A \text{ at } q\vdash^{P+q} G \text{ at } p'}{\Gamma;\Delta,\Diamond A \text{ at } p\vdash^P G \text{ at } p'}\ [\Diamond_L]}{\Gamma;\Delta\vdash^P G \text{ at } p'}\ [CUT_1]$$

□

**Theorem 3.3 (Cut-elimination)** *Let $\mathcal{S}$ be a sequent. If $\mathcal{S}$ has a proof in $SC_1^@$ then $\mathcal{S}$ has a proof in $SC_1^@$ without using the cut rules.*

**Proof** See Appendix A. □

By using the approach of [15], we provide another calculus $SC_2^@$ in which the contraction and weakening rules are *absorbed* in the axioms and logical rules. This version allows us to improve proof-search in our calculus. It is obtained by replacing the axioms by $\frac{}{\Gamma;\Delta,A \text{ at } p \vdash^P A \text{ at } p}\ [ID]$ and $\frac{}{\Gamma;\Delta,\bot \text{ at } p \vdash^P G \text{ at } p'}\ [\bot]$ and the rule $[\supset_L]$ by the following rule

$$\frac{\Gamma;\Delta,A \supset B \text{ at } p \vdash^P A \text{ at } p \qquad \Gamma;\Delta,B \text{ at } p \vdash^P C \text{ at } p'}{\Gamma;\Delta,A \supset B \text{ at } p \vdash^P C \text{ at } p'}\ [\supset_L]\ .$$

**Theorem 3.4 (Soundness)** *Let $\mathcal{S}$ be a sequent, if $\rhd_{SC_2^@}\mathcal{S}$ then $\mathcal{S}$ is valid.*

**Proof** By using Kripke semantics like in the proof of Theorem 3.1. □

**Theorem 3.5 (Completeness)** *Let $\mathcal{S}$ be a sequent, if $\rhd_{SC_1^@}\mathcal{S}$ then $\rhd_{SC_2^@}\mathcal{S}$.*

**Proof** We start by proving that:
1. If $\rhd_{SC_2^@}\Gamma;\Delta,A \text{ at } p,A \text{ at } p \vdash^P G \text{ at } p'$ then $\rhd_{SC_2^@}\Gamma;\Delta,A \text{ at } p \vdash^P G \text{ at } p'$;
2. If $\rhd_{SC_2^@}\Gamma;\Delta \vdash^P G \text{ at } p'$ then $\rhd_{SC_2^@}\Gamma;\Delta,A \text{ at } p \vdash^P G \text{ at } p'$;

It is done by structural induction on both the derivation of the assumption and $A$. Then, by structural induction over the given derivation, we can easily prove the result. Here, we consider for 1. the case when the derivation of the assumption ends with $[\supset_L]$ rule:

$$\frac{\dfrac{\mathcal{D}_1}{\Gamma;\Delta,A \supset B \text{ at } p,A \supset B \text{ at } p \vdash^P A \text{ at } p} \quad \dfrac{\mathcal{D}_2}{\Gamma;\Delta,A \supset B \text{ at } p,B \text{ at } p \vdash^P G \text{ at } p'}}{\Gamma;\Delta,A \supset B \text{ at } p,A \supset B \text{ at } p \vdash^P G \text{ at } p'}\ [\supset_L]$$

From $\rhd_{SC_2^@}\Gamma;\Delta,A \supset B \text{ at } p,A \supset B \text{ at } p \vdash^P A \text{ at } p$, by induction hypothesis, we have $\rhd_{SC_2^@}\Gamma;\Delta,A \supset B \text{ at } p \vdash^P A \text{ at } p$. Then, we show, by induction on the depth of the given derivation, that if $\rhd_{SC_2^@}\Gamma;\Delta,A \supset B \text{ at } p \vdash^P G \text{ at } p'$ then $\rhd_{SC_2^@}\Gamma;\Delta,B \text{ at } p \vdash^P G \text{ at } p'$. Thus, $\rhd_{SC_2^@}\Gamma;\Delta,B \text{ at } p,B \text{ at } p \vdash^P G \text{ at } p'$ and by induction hypothesis we deduce that $\rhd_{SC_2^@}\Gamma;\Delta,B \text{ at } p \vdash^P G \text{ at } p'$. Therefore, $\rhd_{SC_2^@}\Gamma;\Delta,A \supset B \text{ at } p \vdash^P G \text{ at } p'$. □

Let us give the following example of proof in order to illustrate the use of this sequent calculus.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{A \supset B,A;A \text{ at } q \vdash^{\{p,q\}} A \text{ at } q \quad A \supset B,A;A \text{ at } q,B \text{ at } q \vdash^{\{p,q\}} B \text{ at } q}{A \supset B,A;A \text{ at } q,A \supset B \text{ at } q \vdash^{\{p,q\}} B \text{ at } q}\ [COPY]}{A \supset B,A;A \text{ at } q \vdash^{\{p,q\}} B \text{ at } q}\ [COPY]}{A \supset B,A;\vdash^{\{p,q\}} B \text{ at } q}\ [\Box_R]}{A \supset B,A;\vdash^{\{p\}} \Box B \text{ at } p}\ [\Box_L]}{A \supset B;\Box A \text{ at } p \vdash^{\{p\}} \Box B \text{ at } p}\ [\supset_R]}{A \supset B;\vdash^{\{p\}} \Box A \supset \Box B \text{ at } p}$$

## 4 Tableaux Rules for $HIML^p$

In this section, we propose a multi-conclusioned variant of $SC_2^@$ calculus and then derive from it a tableau rules. A multi-conclusioned sequent has the form $\Gamma;\Delta \vdash^P \Pi$, where $\Gamma$ and $\Delta$ are respectively the global and local contexts and $\Pi$ is a multiset of sentences.

**Definition 4.1** Let $\mathcal{K}$=$(K, \leqslant, \{P_k\}_{k\in K}, \{I_k\}_{k\in K})$ be a Kripke model. The sequent $\Gamma;\Delta\vdash^P \Pi$ is *valid in* $\mathcal{K}$ iff $PL(\Gamma)\cup PL(\Delta)\cup PL(\Pi)\subseteq P$ and for every $k\in K$ such that $P\subseteq P_k$, if $k\vDash\Gamma;\Delta$ then there exists $G$ at $p\in\Pi$ such that $(k,p)\vDash G$. The sequent $\Gamma;\Delta\vdash^P\Pi$ is *valid* iff it is valid in every Kripke model.

The multi-conclusioned version $SC^{@}_{2m}$ is obtained by adding a multiset $\Pi$ of sentences to the right part of the sequents in each rule of $SC^{@}_{2}$ except $[\vee_{R_1}]$, $[\vee_{R_2}]$, $[\supset_R]$ and $[\Diamond_R]$. For example, the rule $[\wedge_R]$ is transformed into:

$$\frac{\Gamma;\Delta\vdash^P A \text{ at } p,\Pi \qquad \Gamma;\Delta\vdash^P B \text{ at } p,\Pi}{\Gamma;\Delta\vdash^P A\wedge B \text{ at } p,\Pi}\ [\wedge_R]$$

We replace $[\vee_{R_1}]$, $[\vee_{R_2}]$, $[\supset_R]$ and $[\Diamond_R]$ by the following three rules:

$$\frac{\Gamma;\Delta\vdash^P A \text{ at } p, B \text{ at } p,\Pi}{\Gamma;\Delta\vdash^P A\vee B \text{ at } p,\Pi}\ [\vee_R] \qquad \frac{\Gamma;\Delta, A \text{ at } p\vdash^P B \text{ at } p}{\Gamma;\Delta\vdash^P A\supset B \text{ at } p,\Pi}\ [\supset_R] \qquad \frac{\Gamma;\Delta\vdash^{\{p_1,\ldots,p_n\}} A \text{ at } p_1,\ldots,A \text{ at } p_n,\Pi}{\Gamma;\Delta\vdash^{\{p_1,\ldots,p_n\}} \Diamond A \text{ at } p,\Pi}\ [\Diamond_R]$$

**Theorem 4.2 (Soundness)** *If* $\rhd_{SC^{@}_{2m}}\Gamma;\Delta\vdash^P\Pi$ *then* $\Gamma;\Delta\vdash^P\Pi$ *is valid.*

**Proof** The proof is similar to the one of Theorem 3.1, by using the Kripke semantics and Definition 4.1. □

**Theorem 4.3 (Completeness)** *If* $\Gamma;\Delta\vdash^P\Pi$ *is valid then* $\rhd_{SC^{@}_{2m}}\Gamma;\Delta\vdash^P\Pi$.

**Proof** We can see that a multi-conclusioned sequent $\Gamma;\Delta\vdash^P A_1 \text{ at } p_1,\ldots,A_n \text{ at } p_n$ is valid iff $\Gamma;\Delta\vdash^P A_1@p_1\vee\ldots\vee A_n@p_n \text{ at } p$, where $p\in P$, is valid. Thus, we can show that if $\rhd_{SC^{@}_{2}}\Gamma;\Delta\vdash^P A_1@p_1\vee\ldots\vee A_n@p_n \text{ at } p$ then $\rhd_{SC^{@}_{2m}}\Gamma;\Delta\vdash^P A_1 \text{ at } p_1,\ldots,A_n \text{ at } p_n$. The proof is done by structural induction on the given derivation of the assumption. We must prove the weakening property: if $\rhd_{SC^{@}_{2m}}\Gamma;\Delta\vdash^P\Pi$ then $\rhd_{SC^{@}_{2m}}\Gamma;\Delta\vdash^P\Pi, A \text{ at } p$. □

Having defined this multi-conclusioned calculus we derive a tableau calculus appropriate for proof-search because of the control of the COPY rule.

**Definition 4.4** A *signed formula* is an expression of the form $S\,A$ where $S\in\{F,T\}$ and $A$ is a pure formula.

**Definition 4.5** A *tableau node* is an expression of the form $M_1;M_2;PL$ where $M_1$ is a multiset of pure formulae, $M_2$ is of the form $\{(S\,A,p)\mid S\,A \text{ is a signed formula and } p \text{ is a place}\}$ and $PL$ is a set of places.
A *tableau* is tree whose nodes are tableau nodes. The rules of branch expansion are displayed in Figure 3.

A tableau node $M_1;M_2,VP$ is said to be *closed* if $M_2$ contains occurrences of both $(TA,p)$ and $(FA,p)$, or if $M_2$ contains $(T\bot,p)$. A branch is closed if it contains a closed tableau node. A tableau is closed if it only contains closed branches.

**Theorem 4.6 (Soundness and completeness)** *Let* $\mathcal{S}=\Gamma;\Delta\vdash^P\Pi$ *be a multi-conclusion sequent.* $\mathcal{S}$ *is valid iff there is a closed tableau with the initial tableau node* $\Gamma;M;P$, *where* $M=\{T(A,p)\mid A \text{ at } p\in\Delta\}\cup\{T(B,q)\mid B\in\Gamma \text{ and } q\in P\}\cup\{F(G,p)\mid G \text{ at } p\in\Pi\}$.

$$\frac{M_1;M_2,(T(A\wedge B),p);P}{M_1;M_2,(TA,p),(TB,p);P}\ [T\wedge] \qquad \frac{M_1;M_2,(F(A\wedge B),p);P}{M_1;M_2,(FA,p);P \mid M_1;M_2,(FB,p);P}\ [F\wedge]$$

$$\frac{M_1;M_2,(T(A\vee B),p);P}{M_1;M_2,(TA,p);P \mid M_1;M_2,(TB,p);P}\ [T\vee] \qquad \frac{M_1;M_2,(F(A\vee B),p);P}{M_1;M_2,(FA,p),(FB,p);P}\ [F\vee]$$

$$\frac{M_1;M_2,(T(A\supset B),p);P}{M_1;M_2,(T(A\supset B),p),(FA,p);P \mid M_1;M_2,(TB,p);P}\ [T\supset] \qquad \frac{M_1;M_2,(F(A\supset B),p);P}{M_1;(M_2)_T,(TA,p),(FB,p);P}\ [F\supset]$$

$$\frac{M_1;M_2,(T(A@p'),p);P}{M_1;M_2,(TA,p');P}\ [T@] \qquad \frac{M_1;M_2,(F(A@p'),p);P}{M_1;M_2,(FA,p');P}\ [F@]$$

$$\frac{M_1;M_2,(T(\Box A),p);P}{M_1,A;M_2,(TA,p_1),\ldots,(TA,p_K);P}\ [T\Box] \qquad \frac{M_1;M_2,(F(\Box A),p);P}{M_1;M_2,(TM_1,q),(FA,q);P+q}\ [F\Box]$$

$$\frac{M_1;M_2,(T(\Diamond A),p);P}{M_1;M_2,(TM_1,q),(TA,q);P+q}\ [T\Diamond] \qquad \frac{M_1;M_2,(F(\Diamond A),p);P}{M_1,A;M_2,(FA,p_1),\ldots,(FA,p_K);P}\ [F\Diamond]$$

Where $\{p_1,\ldots,p_k\}=P$ and $(TM_1,q)=\{(TF,q)\mid F\in M_1\}$.

Figure 3. The Tableau rules

**Proof** Soundness and completeness of this tableau method come from $SC^{@}_{2m}$ system. Intuitively, in this method, we associated the application of the COPY rule to the application of the rules where there is an introduction of a new place, i.e., the $[F\Box]$ and $[T\Diamond]$ rules. Because of a given pure formula $A\in\Gamma$ and a given place $q$, a single copy $A$ at $q$, in the local context, in a derivation is enough. Since we do not use the COPY rule for the places in $P$, we copy the pure formulae of the global context with the places in $P$ in the initial tableau node. □

## 5 A Terminating Calculus for the □-free Fragment

In this section, we propose a terminating calculus, called $SCT^{@}$, for the □-free fragment of this logic by using the approach used in [6] for intuitionistic logic.

We start by defining a particular class of Kripke models by using a structure called *Kripke trees*. For this, we use a similar approach to that given in [7].

**Definition 5.1** A *node* is a set $\mathcal{N}=\{(p_1,S^{p_1}_{\mathcal{N}}),\ldots,(p_n,S^{p_n}_{\mathcal{N}})\}$ where $\forall i\in 1..n$, $p_i$ is a place and $S^{p_i}_{\mathcal{N}}$ a finite set of logical variables. We note $Var_{\mathcal{N}}$ the set $S^{p_1}_{\mathcal{N}}\cup\ldots\cup S^{p_n}_{\mathcal{N}}$, $PL_{\mathcal{N}}$ the set $\{p_1,\ldots,p_n\}$ and $P^X_{\mathcal{N}}$ the set $\{p_i\mid X\in S^{p_i}_{\mathcal{N}}\}$.

**Definition 5.2** [Kripke tree] A *Kripke tree* is a pair $\mathcal{T}=(\mathcal{N}_{\mathcal{T}},[\mathcal{T}_1,\ldots,\mathcal{T}_p])$ where $\mathcal{N}_{\mathcal{T}}$ is a node And $[\mathcal{T}_1,\ldots,\mathcal{T}_p]$ is a finite list of Kripke trees. Moreover, for each $i$, $Var_{\mathcal{N}_{\mathcal{T}}}\subseteq Var_{\mathcal{N}_{\mathcal{T}_i}}$ and $\forall X\in Var_{\mathcal{N}_{\mathcal{T}}}$, $P^X_{\mathcal{N}_{\mathcal{T}}}\subseteq P^X_{\mathcal{N}_{\mathcal{T}_i}}$.

The concept of *subtree* is defined inductively by: $\mathcal{T}'$ is a subtree of $\mathcal{T}=(\mathcal{N}_{\mathcal{T}},[\mathcal{T}_1,\ldots,\mathcal{T}_p])$ iff $\mathcal{T}'=\mathcal{T}$ or there exists $i\in\{1,\ldots,p\}$ such that $\mathcal{T}'=\mathcal{T}_i$ or $\mathcal{T}'$ is a *subtree* of $\mathcal{T}_i$.

**Definition 5.3** Let $\mathcal{T}=(\mathcal{N}_{\mathcal{T}},[\mathcal{T}_1,\ldots,\mathcal{T}_p])$ be a Kripke tree, the *subtree model associated to* $\mathcal{T}$, denoted $\mathcal{K}_{\mathcal{T}}$, is the quadruple: $(\mathcal{T}^*,\leqslant,\{PL_{\mathcal{N}_{\mathcal{T}'}}\}_{\mathcal{T}'\in\mathcal{T}^*},\{I_{\mathcal{T}'}\}_{\mathcal{T}'\in\mathcal{T}^*})$ where
- $\mathcal{T}^*$ is the set of all subtrees of $\mathcal{T}$;
- $\leqslant$ is a partial order on $\mathcal{T}^*$ where $\mathcal{T}''\leqslant\mathcal{T}'$ iff $\mathcal{T}''$ is a subtree of $\mathcal{T}'$;

$$\frac{\Gamma, A^{p_A - p}; \Delta, A \text{ at } p \vdash^P G \text{ at } p'}{\Gamma, A^{p_A}; \Delta \vdash^P G \text{ at } p'} \; [COPY] \qquad \frac{(\Gamma[\Diamond A/A@q, P])^{+q}; \Delta, A \text{ at } q \vdash^{P+q} C \text{ at } p'}{\Gamma; \Delta, \Diamond A \text{ at } p \vdash^P C \text{ at } p'} \; [\Diamond_L]$$

$$\frac{\Gamma; \Delta, X \text{ at } p, B \text{ at } p \vdash^P G \text{ at } p'}{\Gamma; \Delta, X \text{ at } p, X \supset B \text{ at } p \vdash^P G \text{ at } p'} \; [\supset_L^!] \qquad \frac{\Gamma; \Delta, A \supset (B \supset C) \text{ at } p \vdash^P G \text{ at } p'}{\Gamma; \Delta, (A \wedge B) \supset C \text{ at } p \vdash^P G \text{ at } p'} \; [(\wedge)\supset_L]$$

$$\frac{\Gamma; \Delta, A \supset C \text{ at } p, B \supset C \text{ at } p \vdash^P G \text{ at } p'}{\Gamma; \Delta, (A \vee B) \supset C \text{ at } p \vdash^P G \text{ at } p'} \; [(\vee)\supset_L] \qquad \frac{\Gamma; \Delta, A \supset B@p' \text{ at } p \vdash^P G \text{ at } p''}{\Gamma; \Delta, A@p \supset B \text{ at } p' \vdash^P G \text{ at } p''} \; [@\supset]$$

$$\frac{\Gamma, (A \supset B@p)^P; \Delta \vdash^P G \text{ at } p'}{\Gamma; \Delta, \Diamond A \supset B \text{ at } p \vdash^P G \text{ at } p'} \; [\Diamond\supset_L] \qquad \frac{\Gamma; \Delta \vdash^P G \text{ at } p'}{\Gamma; \Delta, \bot \supset A \text{ at } p \vdash^P G \text{ at } p'} \; [\bot\supset_L]$$

$$\frac{\Gamma; \Delta, A \text{ at } p, B \supset C \text{ at } p \vdash^P B \text{ at } p \qquad \Gamma; \Delta, C \text{ at } p \vdash^P G \text{ at } p'}{\Gamma; \Delta, (A \supset B) \supset C \text{ at } p \vdash^P G \text{ at } p'} \; [(\supset)\supset_L]$$

Figure 4. The $SCT^@$ calculus

- $\forall \mathcal{T}' \in \mathcal{T}^*$, $I_{\mathcal{T}'} : \mathsf{Var} \to 2^{PL_{\mathcal{N}_{\mathcal{T}'}}}$ such that for all $X \in \mathsf{Var}$ we have $I_{\mathcal{T}'}(X) = P^X_{\mathcal{N}_{\mathcal{T}'}}$.

**Proposition 5.4** *For every Kripke tree $\mathcal{T} = (\mathcal{N}_\mathcal{T}, [\mathcal{T}_1, \ldots, \mathcal{T}_p])$, the subtree model $\mathcal{K}_\mathcal{T} = (\mathcal{T}^*, \leqslant, \{PL_{\mathcal{N}_{\mathcal{T}'}}\}_{\mathcal{T}' \in \mathcal{T}^*}, \{I_{\mathcal{T}'}\}_{\mathcal{T}' \in \mathcal{T}^*})$ is a Kripke model.*

**Proof** Let $\mathcal{T} = (\mathcal{N}_\mathcal{T}, [\mathcal{T}_1, \ldots, \mathcal{T}_p])$ be a Kripke tree. From Definition 2.1 and Definition 5.3, to show that $(\mathcal{T}^*, \leqslant, \{PL_{\mathcal{N}_{\mathcal{T}'}}\}_{\mathcal{T}' \in \mathcal{T}^*}, \{I_{\mathcal{T}'}\}_{\mathcal{T}' \in \mathcal{T}^*})$ is a Kripke model, we have only to show:
1. for all $\mathcal{T}', \mathcal{T}''$ in $\mathcal{T}^*$ such that $\mathcal{T}'' \leqslant \mathcal{T}'$, we have $PL_{\mathcal{N}_{\mathcal{T}''}} \subseteq PL_{\mathcal{N}_{\mathcal{T}'}}$;
2. for all $\mathcal{T}', \mathcal{T}''$ in $\mathcal{T}^*$ such that $\mathcal{T}'' \leqslant \mathcal{T}'$, we have for all $X \in \mathsf{Var}$, $P^X_{\mathcal{N}_{\mathcal{T}''}} \subseteq P^X_{\mathcal{N}_{\mathcal{T}'}}$.

These properties can be proved by structural induction on $\mathcal{T}$, namely with induction hypothesis for every subtree of $\mathcal{T}$. □

In order to define the $SCT^@$ calculus, we replace the rules $[COPY]$ and $[\supset_L]$ of the $SC_2^@$ calculus by the set of rules of Figure 4 in which every formula of the global contexts is indexed by a set of places $A^{ind}$. By such indexes we limit the use of $[COPY]$. Let us note that in the $[COPY]$ rule we have $p \in P_A$. Moreover the expression $\Gamma[\Diamond A/A@q, P]$ in the $[\Diamond_L]$ rule means that one substitutes $A@q$ to $\Diamond A$ in all formulae of $\Gamma$ and changes the index with $P$. In addition $(\Gamma)^{+q}$ means that one adds $q$ to the indexes of the $\Gamma$ formulae.

**Definition 5.5** [Irreducible sequent] An *irreducible sequent* is a sequent of the form $\Gamma; X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m, Y_1 \supset C_1 \text{ at } q_1, \ldots, Y_n \supset C_n \text{ at } q_n \vdash^P F \text{ at } p$ where $\Gamma$ is a multiset of pure formulae; for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$, if $X_i \equiv Y_j$ then $p_i \neq q_j$; and $F \in \mathsf{Var} \cup \{\bot\}$ and if $F \in \{X_1, \ldots, X_m\}$ then $p \notin \{p_1, \ldots, p_m\}$; for all $A^{ind}$ in $\Gamma$, $ind = \emptyset$.

**Definition 5.6** [Inv-irreducible sequent] An *inv-irreducible sequent* is a sequent of the form $\Gamma; X_1 \text{ at } p_1, \ldots, X_k \text{ at } p_k, Y_1 \supset D_1 \text{ at } q_1, \ldots, Y_l \supset D_l \text{ at } q_l, (A_1 \supset B_1) \supset C_1 \text{ at } r_1, \ldots, (A_m \supset B_m) \supset C_m \text{ at } r_m \vdash^P F \text{ at } p$ where $\Gamma$ is a multiset of pure formulae; for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$, if $X_i \equiv Y_j$ then $p_i \neq q_j$; $F \in \mathsf{Var} \cup \{\bot\}$, $F \equiv A \vee B$ or $F \equiv \Diamond A$; if $F \in \{X_1, \ldots, X_k\}$ then $p \notin \{p_1, \ldots, p_m\}$; for all $G^{ind}$ in $\Gamma$, $ind = \emptyset$.

**Proposition 5.7** *The number of applications of the COPY rule in any derivation in the $SCT^@$ calculus is finite.*

**Proof** Let $\mathcal{S} \equiv \Gamma; \Delta \vdash^P G \text{ at } p'$ be a sequent and $\mathcal{D}$ be a derivation of $\mathcal{S}$ in $SCT^@$. For every $A$ in $\Gamma$, the number of applications of the COPY rule is smaller than the size of $P$ and the

number of the new places introduced in $\mathcal{D}$. One can see that the number of the new places introduced in $\mathcal{D}$ is smaller than the number of the subformulae of the form $\Diamond F$ in $\mathcal{S}$. Since the size of $P$ and the set of subformulae of the form $\Diamond F$ in $\mathcal{S}$ are finite, we deduce that the number of applications of the COPY rule is finite. □

**Proposition 5.8** *The application of the SCT$^{@}$ rules to a given sequent terminates with axioms or irreducible sequents.*

**Proof** See Appendix B. □

**Theorem 5.9 (Soundness)** *The rules of the SCT$^{@}$ calculus are sound.*

**Proof** We consider the case for rule $[(\supset)\supset_L]$. We suppose that $\Gamma;\Delta,A \text{ at } p, B\supset C \text{ at } p \vdash^P B \text{ at } p$ and $\Gamma;\Delta,C \text{ at } p \vdash^P G \text{ at } p$ are valid. Let $\mathcal{K} = (K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a countermodel of $\Gamma;\Delta,(A\supset B)\supset C \text{ at } p \vdash^P G \text{ at } p'$. Then, $\exists k \in K$ such that $P \subseteq P_k$, $k \vDash \Gamma;\Delta$, $(k,p) \vDash ((A\supset B)\supset C)$ and $(k,p') \nvDash G$. From $(k,p) \vDash \Box((A\supset B)\supset C)$, we have $\forall l \geqslant k$, if $(l,p) \vDash A\supset B$ then $(l,p) \vDash C$. We suppose that there exists $l_0 \geqslant k$ such that $(l_0,p) \vDash A$ and $(l_0,p) \nvDash B$. From $l_0 \geqslant k$ and the Kripke monotonicity, we have $l_0 \vDash \Gamma;\Delta$. Moreover from $(l_0,p) \vDash A$ and $(l_0,p) \nvDash B$, we have $(l_0,p) \vDash B\supset C$, because for $l' > l_0$ if $(l',p) \vDash B$ then $(l',p) \vDash A\supset B$ and we deduce that $(l',p) \vDash C$. Therefore, $\mathcal{K}$ is countermodel of $\Gamma;\Delta,A \text{ at } p, B\supset C \text{ at } p \vdash^P B \text{ at } p$ and this is a contradiction. Thus, $\forall l \geqslant k$, we have $(l,p) \vDash A\supset B$ and thus $(l,p) \vDash C$. Since $(k,p') \nvDash G$, $\mathcal{K}$ is a countermodel of $\Gamma;\Delta,C \text{ at } p \vdash^P G \text{ at } p$. From this contradiction we deduce that $\Gamma;\Delta,(A\supset B)\supset C \text{ at } p \vdash^P G \text{ at } p'$ is valid. Proofs for other rules are similar. □

Let us remind that a proof rule is *invertible* if, for any instance of the rule, the non-validity of at least one of its premises entails the non-validity of its conclusion. It is *strongly invertible* if, for any instance of the rule and any Kripke model $\mathcal{K}$, if $\mathcal{K}$ is a countermodel of at least one of its premises then it is a countermodel of its conclusion. We can observe that strong invertibility implies invertibility.

**Theorem 5.10** *All the rules of the SCT$^{@}$ calculus, except the $[(\supset)_L\supset]$, $[\vee_R]$, $[\Diamond_R]$ rules, are strongly invertible.*

**Proof** We consider the case for rule $[\Diamond\supset_L]$. Let $\mathcal{K} = (K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a countermodel of $\Gamma,(A\supset B@p)^P;\Delta \vdash^P G \text{ at } p'$. Then, $\exists k \in K$ such that $P_k \subseteq P$, $k \vDash \Gamma;\Delta$, $(k,q) \vDash \Box(A\supset B@p)$ for $q \in P_k$ and $(k,p') \nvDash G$. Thus, from $(k,q) \vDash \Box(A\supset B@p)$, we have $\forall l \geqslant k$ and $\forall r \in P_l$, if $(l,r) \vDash A$ then $(l,p) \vDash B$. Therefore, $(k,p) \vDash \Diamond A\supset B$, because $\forall l \geqslant k$, if $(l,p) \vDash \Diamond A$ then $(l,p) \vDash B$. We deduce that $\mathcal{K}$ is a countermodel of $\Gamma;\Delta,\Diamond A\supset B \text{ at } p \vdash^P G \text{ at } p'$. Thus, the rule $[\Diamond\supset_L]$ is strongly invertible. Proofs for other rules are similar. □

A proof-refutation tree is a tree in which the nodes are indexed by sequents. Especially, the root node is indexed by a sequent in which the pure formulae of the global context are indexed by the set of all places belonging to this sequent. The rules of branch expansion are obtained from the rules of *SCT$^{@}$*: if the node is indexed by an inv-irreducible sequent then its children are indexed by the sequents which correspond to the premises of all rules that can be applied to its index. Else, the children correspond to premises of one of the strongly invertible rule which can be applied to its index.
From Proposition 5.8, we can deduce that a proof-refutation tree is finite and its leaf nodes are indexed by axioms and irreducible sequents. The formal definition is given below.

**Definition 5.11** [Proof-refutation tree] A *proof-refutation tree* is a tree where the nodes are indexed by sequents and verifying the following properties:
1) The root node is indexed by a sequent of the form $\Gamma;\Delta\vdash^P G$ at $p$ where the pure formulae of $\Gamma$ are indexed by the set $P$ of places.
2) For every internal node $n$ indexed by a sequent $\mathcal{S}$ which is not an inv-irreducible sequent, $n$ has a maximum of two children: if $n$ has two children (resp. a single child) indexed by $\mathcal{H}_1$ and $\mathcal{H}_2$ (resp. $\mathcal{H}$) then $\dfrac{\mathcal{H}_1 \quad \mathcal{H}_2}{\mathcal{S}}\ [R]$ (resp. $\dfrac{\mathcal{H}}{\mathcal{S}}\ [R]$ ) is an instance of a strongly invertible rule.
3) For every internal node $n$ indexed by an inv-irreducible sequent $\Gamma;X_1$ at $p_1,\ldots,X_m$ at $p_m$, $Y_1\supset D_1$ at $q_1,\ldots,Y_n\supset D_n$ at $q_n,(A_1\supset B_1)\supset C_1$ at $r_1,\ldots,(A_l\supset B_l)\supset C_l$ at $r_l\vdash^P K$ at $p$, the set of children of $n$ is obtained by: for every $i\in\{1,\ldots,l\}$, we have two children indexed respectively by $\Gamma;\Delta',\Delta_i'',C_i$ at $r_i\vdash^P K$ at $p$ and by $\Gamma;\Delta',\Delta_i'',A_i$ at $r_i,B_i\supset C_i$ at $r_i\vdash^P B_i$ at $r_i$ where $\Delta'=X_1$ at $p_1,\ldots,X_m$ at $p_m,Y_1\supset D_1$ at $q_1,\ldots,Y_n\supset D_n$ at $q_n$, $\Delta''=(A_1\supset B_1)\supset C_1$ at $r_1,\ldots,(A_l\supset B_l)\supset C_l$ at $r_l$ and $\Delta_i''$ is $\Delta''$ without $(A_i\supset B_i)\supset C_i$ at $r_i$. Moreover, if $K=A\vee B$ then we have two children indexed respectively by $\Gamma;\Delta',\Delta''\vdash^P A$ at $p$ and $\Gamma;\Delta',\Delta''\vdash^P B$ at $p$. And if $K=\Diamond A$ then for every $pl\in P$, we have a child indexed by $\Gamma;\Delta',\Delta''\vdash^P A$ at $pl$.
4) The leaf nodes are indexed by axioms and irreducible sequents.

**Proposition 5.12** *For a rule* $\dfrac{\Gamma;\Delta'\vdash^P G' \text{ at } p \qquad \Gamma;\Delta''\vdash^P G'' \text{ at } p}{\Gamma;\Delta\vdash^P G \text{ at } p}\ [R]$ *(resp.* $\dfrac{\Gamma';\Delta'\vdash^{P'} G' \text{ at } p'}{\Gamma;\Delta\vdash^P G \text{ at } p}\ [R]$ *) and* $\forall\mathcal{K}=(K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ *and* $\forall k\in K$ *such that* $P\subseteq P_k$ *(resp.* $P'\subseteq P_k$*), if (*$k\vDash\Delta'$ *or* $k\vDash\Delta''$*) (resp.* $k\vDash\Delta'$*) then* $k\vDash\Delta$.

**Proof** We consider the rules $[(\supset)\supset_L]$, $[\Diamond_L]$ and $[(\wedge)\supset_L]$. We start with the rule $[(\supset)\supset_L]$. Let $\mathcal{K}=(K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a Kripke model and $k\in K$ such that $P\subseteq P_k$. If $k\vDash\Delta,A$ at $p,B\supset C$ at $p$ then by monotonicity $\forall k'\geqslant k$ we have $k'\vDash\Delta,A$ at $p,B\supset C$ at $p$. Thus, $\forall k'\geqslant k$, if $(k',p)\vDash A\supset B$ then $(k',p)\vDash B$ and we have $(k',p)\vDash C$. Therefore, $k\vDash\Delta,(A\supset B)\supset C$ at $p$. Otherwise, if $k\vDash\Delta,C$ at $p$ then it is easy to see that $k\vDash\Delta,(A\supset B)\supset C$ at $p$.
We now consider the rule $[\Diamond_L]$. Let $\mathcal{K}=(K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a Kripke model and $k\in K$ such that $P+q\subseteq P_k$. If $k\vDash\Delta,A$ at $q$ then $k\vDash\Delta$ and there exists $pl\in P_k$ such that $(k,pl)\vDash A$. Thus, $k\vDash\Delta,\Diamond A$ at $p$. We now consider the rule $[(\wedge)\supset_L]$. Let $\mathcal{K}=(K,\leqslant,\{P_k\}_{k\in K},\{I_k\}_{k\in K})$ be a Kripke model and $k\in K$ such that $P\subseteq P_k$. If $k\vDash\Delta,A\supset(B\supset C)$ at $p$ then $\forall k'\geqslant k$, if $(k',p)\vDash A$ then $(k',p)\vDash B\supset C$. Thus, if $(k',p)\vDash A\wedge B$ then $(k',p)\vDash B\supset C$ and $(k',p)\vDash C$ because $(k',p)\vDash B$. Therefore $k\vDash\Delta,(A\wedge B)\supset C$ at $p$. Other cases are treated by similar arguments. □

**Theorem 5.13 (Completeness)** *Let* $\mathcal{S}=\Gamma;\Delta\vdash^P G$ at $p'$ *be a sequent where the formulae of* $\Gamma$ *are indexed by the set of places P. If* $\mathcal{S}$ *does not have a proof in SCT*$^@$ *then it has a countermodel.*

**Proof** Let $\mathcal{S}=\Gamma;\Delta\vdash^P G$ at $p'$ be a sequent where all the formulae of $\Gamma$ are indexed by the set of places $P$. Let $\mathcal{PR}$ be a proof-refutation tree in which the root node is indexed by $\mathcal{S}$. We suppose that $\mathcal{S}$ has not a proof in $SCT^@$ and we show how to extract a countermodel of $\mathcal{S}$ from $\mathcal{PR}$. See Appendix C. □

First we show how to generate a countermodel for the sequent $\vdash^{\{p\}}(\Diamond A)\supset A$ at $p$. For this, we need to build the proof-refutation tree associated to this sequent:

$$\dfrac{\dfrac{A \text{ at } q \vdash^{\{p,q\}} A \text{ at } p}{\Diamond A \text{ at } p \vdash^{\{p\}} A \text{ at } p}\,[\Diamond_L]}{\vdash^{\{p\}} \Diamond A \supset A \text{ at } p}\,[\supset_R]$$

| | $A$ |
|---|---|
| $p$ | $q$ |

As this logic can be seen as an hybridisation of *IS*5, we can provide, from the previous calculi, a new calculi for *IS*5. For example to prove the formula $\Box(A \supset B) \supset (\Diamond A \supset \Diamond B)$ we can prove $A \supset B; \vdash^{\{p\}} \Diamond A \supset \Diamond B \text{ at } p$ by using $SCT^{@}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \supset B; A \text{ at } q, B \text{ at } q \vdash^{\{p,q\}} B \text{ at } q}{A \supset B; A \text{ at } q, A \supset B \text{ at } q \vdash^{\{p,q\}} \Diamond B \text{ at } p}\,[\Diamond_R]}{A \supset B; A \text{ at } q \vdash^{\{p\}} \Diamond B \text{ at } p}\,[COPY]}{A \supset B; \Diamond A \text{ at } p \vdash^{\{p\}} \Diamond B \text{ at } p}\,[\Diamond_L]}{A \supset B; \vdash^{\{p\}} \Diamond A \supset \Diamond B \text{ at } p}\,[\supset_R]$$

## 6 Conclusion and Perspectives

In this paper we propose a sequent calculus for $IHML^p$ and its variants that absorb weakening and contraction rules. Moreover tableaux rules are naturally designed from a derived multi-conclusioned sequent calculus. Knowing that this logic can be seen as an hybridisation of the intuitionistic modal system *IS*5, namely it corresponds to *IS*5 extended with a satisfaction operator (@), we can provide, from our calculi, new calculi and decision procedures for *IS*5. Further investigations will be devoted to the comparison with existing calculi for such a logic [14]. Moreover we define a terminating calculus for the $\Box$-free fragment of $IHML^p$ that allows to build (finite) countermodels in case of non-validity. A consequence of this study, not developed here, is the proof of the finite model property w.r.t. the Kripke semantics for this $\Box$-free fragment and thus of the same result for *IS*5 without $\Box$. Next studies will be devoted to the definition of specific rules for the $\Box$ modality and to the characterization of the logical fragment of the logic, including $\Box$, for which the finite model property w.r.t. the Kripke semantics is verified. Moreover we will focus on semantics and on the design of new tree-based structures allowing to build finite countermodels w.r.t. birelational semantics. Finally we will consider our approach for the extension of the logic with nominals in order to deal with a full intuitionistic hybrid logic like in [3].

## References


[1] N. Biri and D. Galmiche. Models and separation logics for resource trees. *Journal of Logic and Computation*, 17(4):687–726, 2007.

[2] P. Blackburn. Representation, reasoning, and relational structures: a hybrid logic manifesto. *Logic Journal of the IGPL*, 8:339–365, 2000.

[3] T. Braüner and V. de Paiva. Towards constructive hybrid logic (extended abstract). *Elec. Proc. of Methods for Modalities*, 3, 2003.

[4] R. Chadha, D. Macedonio, and V. Sassone. A hybrid intuitionistic logic: Semantics and decidability. *Journal of Logic and Computation*, 16(1):27–59, 2006.

[5] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. In *ICALP*, volume 71 of *LNCS*, pages 188–202. Springer Verlag, 1979.

[6] R. Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *Journal of Symbolic Logic*, 57:795–807, 1992.

[7] D. Galmiche and D. Larchey-Wendling. Structural Sharing and Efficient Proof-search in Propositional Intuitionistic Logic. In *Asian Computing Science Conference, ASIAN'99, LNCS 1742*, pages 101–112, Phuket, Thailand, December 1999.

[8] L. Jia and D. Walker. Modal proofs as distributed programs. Technical Report TR-671-03, Princeton University, 2003.

[9] L. Jia and D. Walker. Modal proofs as distributed programs (extended abstract). In *ESOP*, volume 2986 of *LNCS*, pages 219–233. Springer Verlag, 2004.

[10] F. Pfenning. Structural cut elimination: I. intuitionistic and classical logic. *Journal of Information and Computation*, 157(1-2):84–141, 2000.

[11] D. Pym and C. Tofts. Systems modelling via resources and processes: Philosophy, calculus, semantics, and logic. *Electronic Notes in Theoretical Computer Science*, 172:545–587, 2007.

[12] D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.

[13] J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science*, pages 55–74, Copenhagen, Danemark, July 2002.

[14] A. Simpson. *The proof theory and semantics of intuitionistic modal logic*. PhD thesis, University of Edinburgh, 1994.

[15] A.S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*, volume 43 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1996.

# Appendix A: Proof of Theorem 3.3

**Theorem 3.3.** *Let $\mathcal{S}$ be a sequent. If $\mathcal{S}$ has a proof in $SC_1^@$ then $\mathcal{S}$ has a proof in $SC_1^@$ without using the cut rules.*

**Proof** We let $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^P G \text{ at } p'$ denote that $\Gamma;\Delta \vdash^P G \text{ at } p'$ has a derivation in $SC_1^@$ without using the cut rules. To make the proof we use the structural cut-elimination described in [10], by using a simple structural induction from the admissibility of the cut rules in the cut-free system.Thus, we have only to show:

(i) If $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^P A \text{ at } p$ and $\rhd_{SC_1^{@-}} \Gamma;\Delta, A \text{ at } p \vdash^P G \text{ at } p'$ then $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^P G \text{ at } p'$.

(ii) If $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^{P+q} A \text{ at } q$ and $\rhd_{SC_1^{@-}} \Gamma, A;\Delta \vdash^P G \text{ at } p'$ then $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^P G \text{ at } p'$.

The proof proceeds by mutual structural induction on the cut formula and the given derivations. For example, if we are in the case:

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_1}{\Gamma;\Delta, A \text{ at } p \vdash^P B \text{ at } p}}{\Gamma;\Delta \vdash^P A \supset B \text{ at } p}[\supset_R] \quad \dfrac{\dfrac{\mathcal{D}_2}{\Gamma;\Delta \vdash^P A \text{ at } p} \quad \dfrac{\mathcal{D}_3}{\Gamma;\Delta, B \text{ at } p \vdash^P G \text{ at } p'}}{\Gamma;\Delta, A \supset B \text{ at } p \vdash^P G \text{ at } p'}[\supset_L]}{\Gamma;\Delta \vdash^P G \text{ at } p'}[CUT_1]$$

It can be replaced by:

$$\dfrac{\dfrac{\mathcal{D}_2}{\Gamma;\Delta \vdash^P A \text{ at } p} \quad \dfrac{\mathcal{D}_1}{\Gamma;\Delta, A \text{ at } p \vdash^P B \text{ at } p}}{\Gamma;\Delta \vdash^P B \text{ at } p}[CUT_1] \quad \dfrac{\mathcal{D}_3}{\Gamma;\Delta, B \text{ at } p \vdash^P G \text{ at } p'}}{\Gamma;\Delta \vdash^P G \text{ at } p'}[CUT_1]$$

Since $A$ and $B$ are structurally lower than $A \supset B$, we deduce, by the induction hypothesis, that $\rhd_{SC_1^{@-}} \Gamma;\Delta \vdash^P G \text{ at } p'$. □

## Appendix B: Proof of Proposition 5.8

**Proposition 5.8.** *The application of the $SCT^{@}$ rules to a given sequent terminates with axioms or irreducible sequents.*

**Proof** From Proposition 5.7, the number of the applications of the COPY rule in every derivation of a given sequent in $SCT^{@}$ is finite. Thus, to prove termination, we have only to prove that the application of the $SCT^{@}$ rules without the COPY rule to a given sequent terminates. For this, we will use the technic proposed in [6], by showing that for every rule, its conclusion is more complex than its premises by using a measures of complexity over the pure formulae and the sentences. Here, we use the measure $\alpha$ defined by:
$\alpha(A) = 1 \ \ (A \in \mathsf{Var} \cup \{\top, \bot\})$, $\alpha(A \wedge B) = \alpha(A) + \alpha(B) + 1$, $\alpha(A \vee B) = \alpha(A) + \alpha(B) + 1$, $\alpha(A \supset B) = 2 * \alpha(A) + \alpha(B) + 1$, $\alpha(\Diamond A) = \alpha(A) + 1$, $\alpha(\Box A) = \alpha(A) + 1$, $\alpha(A@p) = \alpha(A) + 1$, $\alpha(A \text{ at } p) = \alpha(A) + 1$.
From this definition, the order relation $>$ on pure formulae and sentences, with $A > B$ iff $\alpha(A) > \alpha(b)$, is well-founded. Now, we define an order relation on multisets of pure formulae and sentences: let $M_1$ and $M_2$ two multisets of pure formulae and sentences, $M_1 >_m M_2$ iff $M_2$ is obtained form $M_1$ by replacing one or more pure formulae and sentences by a finite number of pure formulae and sentences, such that if $A$ is replaced by $B$ then $\alpha(A) > \alpha(B)$. Since the relation order on pure formulae and sentences is well-fonded, the order relation $>_m$ is well-founded [5]. It is the order relation which is used to show that in every rule, the conclusion is greater than the premises. For example for the rule $[(\wedge)\supset_L]$, we have $\Gamma \cup \Delta \cup \{(A \wedge B) \supset C \text{ at } p\} \cup \{G \text{ at } p'\} >_m \Gamma \cup \Delta \cup \{A \supset (B \supset C) \text{ at } p\} \cup \{G \text{ at } p'\}$, because $\alpha((A \wedge B) \supset C) = 2 * \alpha(A) + 2 * \alpha(B) + \alpha(C) + 3 > 2 * \alpha(A) + 2 * \alpha(B) + \alpha(C) + 2 = \alpha(A \supset (B \supset C))$.
Since there is always a rule for any sequent which is not an axiom or an irreducible sequent, we deduce that the application of the $SCT^{@}$ rules to a given sequent terminates with axioms or irreducible sequents. □

## Appendix C: Proof of Theorem 5.13

**Theorem 5.13.** *Let $\mathcal{S} = \Gamma; \Delta \vdash^{P} G \text{ at } p'$ be a sequent where all the formulae of $\Gamma$ are indexed by the set of places $P$. If $\mathcal{S}$ has not a proof in $SCT^{@}$ then it has a countermodel.*

**Proof** Let $\mathcal{S} = \Gamma; \Delta \vdash^{P} G \text{ at } p'$ be a sequent where all the formulae of $\Gamma$ are indexed by the set of places $P$. Let $\mathcal{PR}$ be a proof-refutation tree in which the root node is indexed by $\mathcal{S}$. We suppose that $\mathcal{S}$ has not a proof in $SCT^{@}$ and we show how to extract a countermodel of $\mathcal{S}$ from $\mathcal{PR}$.

We show how to decide if an index of a given node in $\mathcal{PR}$ is valid or not. We start by the leaf nodes. We know that the leaf nodes of $\mathcal{PR}$ are indexed by axioms and irreducible sequents. If a leaf node is indexed by an axiom then its index is valid. Now, we prove that the irreducible sequents are not valid. Let $\mathcal{L} = \Gamma; X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m, Y_1 \supset C_1 \text{ at } q_1, \ldots, Y_n \supset C_n \text{ at } q_n \vdash^{P} K \text{ at } p$ be an irreducible sequent. We denote by $VP$ the set $\{X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m\}$. Let $\mathcal{T} = (\mathcal{N}, \emptyset)$ be a Kripke tree with a single node such that $PL_{\mathcal{N}} = P$, $Var_{\mathcal{N}} = \{X_1, \ldots, X_m\}$, $\forall r \in P$ we have $S^{r}_{\mathcal{N}} = \{X_k \mid X_k \text{ at } r \in VP\}$. We have $\forall i \in 1 \ldots, m$, $(\mathcal{T}, p_i) \Vdash X_i$, and since $\forall i \in \{1, \ldots, m\}$ and $\forall j \in \{1, \ldots, n\}$ we have if $X_i \equiv Y_j$ then $p_i \neq q_j$, we obtain $\forall j \in 1 \ldots, n$, $(\mathcal{T}, q_j) \nVdash Y_j$, and thus, $\forall j \in 1 \ldots, n$, $(\mathcal{T}, q_j) \Vdash Y_j \supset C_j \text{ at } q_j$. We can see that for every $A^{\emptyset} \in \Gamma$ and $p \in P$, there exists a derivation with a root sequent of the form $\Gamma'; \Delta', A \text{ at } p \vdash^{P'} G' \text{ at } q$ where $\mathcal{L}$ is one of its leaf sequents. Thus, by using

Proposition 5.12, we have $\mathcal{T} \vDash \Gamma$. It is easy to see that $(\mathcal{T}, p) \nvDash K$. From Proposition 5.4, we deduce that $\mathcal{K}_{\mathcal{T}}$ is a countermodel of $\mathcal{L}$.

Now, we see how, from the children of a given internal node, we can propagate the validity or build a countermodel. Let $I$ be an index of an internal node. If $I$ is not an inv-irreducible sequent then, from Definition 5.11, this node has a maximum of two children where if these children are indexed by $\mathcal{H}_1$ and $\mathcal{H}_2$ (resp. $\mathcal{H}$) then $\dfrac{\mathcal{H}_1 \quad \mathcal{H}_2}{\mathcal{S}}\ [R]$ (resp. $\dfrac{\mathcal{H}}{\mathcal{S}}\ [R]$ ) is an instance of a strongly invertible rule. Thus, if $\mathcal{H}_1$ and $\mathcal{H}_2$ (resp. $\mathcal{H}$) are valid then $I$ is valid because $[R]$ is a sound rule. Else, from the strong invertibility of $[R]$, $I$ has the same countermodels of the non-valid premises of $[R]$.

Let us consider the case of the internal nodes indexed by inv-irreducible sequents. Let $I = \Gamma; X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m, Y_1 \supset D_1 \text{ at } q_1, \ldots, Y_n \supset D_n \text{ at } q_n, (A_1 \supset B_1) \supset C_1 \text{ at } r_1, \ldots, (A_l \supset B_l) \supset C_l \text{ at } r_l \vdash^P K \text{ at } p$ be an inv-irreducible sequent and the index of an internal node. We define $\Delta' \triangleq X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m, Y_1 \supset D_1 \text{ at } q_1, \ldots, Y_n \supset D_n \text{ at } q_n$ and $\Delta'' \triangleq (A_1 \supset B_1) \supset C_1 \text{ at } r_1, \ldots, (A_l \supset B_l) \supset C_l \text{ at } r_l \vdash^P K \text{ at } p$. Then, we define $\Delta''_i$ for $i \in \{1, \ldots, l\}$ by $\Delta''$ without $(A_i \supset B_i) \supset C_i \text{ at } r_i$ and $VP \triangleq \{X_1 \text{ at } p_1, \ldots, X_m \text{ at } p_m\}$. Here, we start by studying the case where $k \equiv \Diamond F$. From Definition 5.11, the children of our internal node are indexed by the premises of the following rules:

$$\frac{\Gamma; \Delta', \Delta''_i, A_i \text{ at } r_i, B_i \supset C_i \text{ at } r_i \vdash^P B_i \text{ at } r_i \qquad \Gamma; \Delta', \Delta''_i, C_i \text{ at } r_i \vdash^P \Diamond F \text{ at } p}{\Gamma; \Delta', \Delta''_i, (A_i \supset B_i) \supset C_i \text{ at } r_i \vdash^P \Diamond F \text{ at } p}\ [(\supset)\supset_L]$$

and

$$\frac{\Gamma; \Delta', \Delta'' \vdash^P F \text{ at } pl}{\Gamma; \Delta', \Delta'' \vdash^P \Diamond F \text{ at } p}\ [\Diamond_L]$$

where $i \in \{1, \ldots, l\}$ and $pl \in P$. If there exists $i \in \{1, \ldots, l\}$ such that $\Gamma; \Delta', \Delta''_i, C_i \text{ at } r_i \vdash^P \Diamond F \text{ at } p$ is not valid, then, it has a countermodel $\mathcal{T}_{C_i}$. Therefore, $\mathcal{T}_{C_i}$ is a countermodel of $I$ because the premiss $\Gamma; \Delta', \Delta''_i, C_i \text{ at } r_i \vdash^P \Diamond F \text{ at } p$ in $[(\supset)\supset_L]$ is strongly invertible. Else, if there exists $i \in \{1, \ldots, l\}$ such that $\Gamma; \Delta', \Delta''_i, A_i \text{ at } r_i, B_i \supset C_i \text{ at } r_i \vdash^P B_i \text{ at } r_i$ is valid or there exists $pl \in P$ such that $\Gamma; \Delta', \Delta'' \vdash^P F \text{ at } pl$ is valid, then $I$ is valid because the rules $[(\supset)\supset_L]$ and $[\Diamond_L]$ are sound. Now we deal with the last case, $\forall i \in \{1, \ldots, l\}$, $\Gamma; \Delta', \Delta''_i, A_i \text{ at } r_i, B_i \supset C_i \text{ at } r_i \vdash^P B_i \text{ at } r_i$ has a countermodel $\mathcal{K}_{\mathcal{T}_i}$; and for all $pl \in P$ we have $\Gamma; \Delta', \Delta'' \vdash^P F \text{ at } pl$ has a countermodel $\mathcal{K}_{\mathcal{T}_{pl}}$. We define $\mathcal{T} \triangleq (\mathcal{N}, \{\mathcal{T}_1, \ldots, \mathcal{T}_l, \mathcal{T}_{pl_1}, \ldots, \mathcal{T}_{pl_k}\})$ where $P = \{pl_1, \ldots, pl_k\}$, $PL_{\mathcal{N}} = P$, $Var_{\mathcal{N}} = \{X_1, \ldots, X_m\}$, $\forall r \in P$ we have $S^r_{\mathcal{N}} = \{X_k \mid X_k \text{ at } r \in VP\}$. It is easy to see that $\mathcal{T}$ is a Kripke tree.

Now we prove that $\mathcal{T} \vDash \Gamma; \Delta', \Delta''$ and $(\mathcal{T}, p) \nvDash \Diamond F$ in $\mathcal{K}_{\mathcal{T}}$. By using Proposition 5.12, we have for all $i \in \{1, \ldots, l\}$ and for all $j \in \{1, \ldots, k\}$, $\mathcal{T}_i \vDash \Gamma; \Delta', \Delta''$ and $\mathcal{T}_{pl_j} \vDash \Gamma; \Delta', \Delta''$. We have for all $i \in \{1, \ldots, l\}$, $\mathcal{T}_i \vDash A$ and $\mathcal{T}_i \nvDash B$. Thus, $\mathcal{T}_i \nvDash A \supset B$ and by Kripke monotonicity we obtain $\mathcal{T} \nvDash A \supset B$. Therefore, $\mathcal{T} \vDash \Gamma; \Delta', \Delta''$ holds. As $\forall j \in \{1, \ldots, k\}$ we have $(\mathcal{T}_{pl_j}, pl_j) \nvDash F \text{ at } pl$, and we obtain by monotonicity $(\mathcal{T}, p) \nvDash \Diamond F$ because in $\mathcal{K}_{\mathcal{T}}$ we have $P_{\mathcal{T}} = P$. Thus, $\mathcal{K}_{\mathcal{T}}$ is a countermodel of $\Gamma; \Delta', \Delta'' \vdash^P \Diamond F \text{ at } p$. For the case $K \equiv A \vee B$, the Kripke model is $\mathcal{T} \triangleq (\mathcal{N}, \{\mathcal{T}_1, \ldots, \mathcal{T}_l, \mathcal{T}_A, \mathcal{T}_B\})$ where $\mathcal{T}_A$ (resp. $\mathcal{T}_B$) is a countermodel of $\Gamma; \Delta', \Delta'' \vdash^P A \text{ at } p$ (resp. $\Gamma; \Delta', \Delta'' \vdash^P B \text{ at } p$). For the case $K \in \mathsf{Var} \cup \bot$, we use the Kripke model $\mathcal{T} \triangleq (\mathcal{N}, \{\mathcal{T}_1, \ldots, \mathcal{T}_l\})$. The proofs of these two cases are similar to the previous proof. We can see that if $\mathcal{S}$ is valid then it has a proof in $SCT^{@}$ and we get a contradiction. Therefore, $\mathcal{S}$ has a countermodel built by the previous method. □

# Two-sequent K and simple fibrations (preliminary report)

Kurt Ranalter[1]

kurt@dcs.qmul.ac.uk

**Abstract**

We report on work in progress concerning the investigation of a semantics of proofs for the positive fragment of intuitionistic two-sequent **K**. We propose a semantics that is given in terms of simple fibrations and argue that the syntactic model construction yields an instance of it. The semantics provides means to characterize the $\Box$-modality as the right adjoint of the substitution functor induced by a projection in the base category.

*Keywords:* modal logic, proof theory, fibred category theory

## 1 Introduction

Finding a good proof theory for intuitionistic modal logics has a long history and various proposals are suggested in the literature. Particular attention deserves Martini and Masini's proposal given in [4]. It provides a two-dimensional natural deduction system that allows one to express the modal rules as introduction and elimination rules. An analogous proposal for intuitionistic **K** can be found in the Fitch-style natural deduction system outlined in [1]. It corresponds to a one-dimensional representation of two-sequent **K** that employs stacks of context instead of the indexing used by Martini and Masini.

We propose a categorical semantics for the positive fragment of intuitionistic two-sequent **K**. It is given in terms of fibred category theory and is closely related to models of simple type theory or, equivalently, intuitionistic propositional logic. The investigation of a semantics of proofs for two-sequent **K** is motivated by the observation that two-sequent modal logic seems fine-grained enough to express other approaches to intuitionistic modal logic in terms of it, thus providing a sort of unifying framework. Furthermore, the proposed semantics allows one to characterize the modal rules as arising from an adjoint situation, thus satisfying the well-known

[1] I would like to thank Gianluigi Bellin for his suggestion to look for a categorical semantics of Martini and Masini's two-sequent approach to intuitionistic modal logic and for providing me with the opportunity to present the ideas developed in this note at a seminar at the University of Verona.

criteria according to which logical connectives should be expressed in terms of adjunctions. This note is organized as follows: section 2 provides a concise overview of intuitionistic two-sequent **K**; section 3 deals with the categorical structure induced by the so-called syntactic model construction.

## 2 Two-sequent K

We work with the positive fragment of intuitionistic two-sequent **K**, i.e formulae or types $A$ are defined by the grammar $A ::= p \mid \top \mid A \wedge A \mid A \to A \mid \Box A$. The rules of the system are provided in table 1 where types have been annotated with terms $t$ defined by the grammar $t ::= x \mid * \mid \lambda x.t \mid tt \mid \langle t, t\rangle \mid \pi_i(t) \mid \mathtt{box}(t) \mid \mathtt{unbox}(t)$. As usual in such presentations $\Gamma$ stands for a context, i.e. a multiset $x_1 \colon A_1, \ldots, x_n \colon A_n$ of typed variables. The main feature of the system is that sequents $\mathfrak{S} \mid \Gamma \vdash t \colon A$ also depend on a stack $\mathfrak{S}$ of contexts.

Stacks of contexts are defined by the grammar $\mathfrak{S} ::= () \mid \mathfrak{S} \lhd \Gamma$ where $()$ stands for the empty stack and $\lhd$ for the separator between the elements of the stack. For a nonempty stack we shall omit the leading empty stack when writing out the stack in full. Hence $\Gamma$ may stand both for a multiset of typed variables and for a stack of length 1. $|\mathfrak{S}|$, the number of elements in a stack $\mathfrak{S}$, is defined inductively as follows: $|()| = 0$ and $|\mathfrak{S} \lhd \Gamma| = |\mathfrak{S}| + 1$.

Our presentation of the rules is inspired by the Fitch-style natural deduction system outlined in [1], the main difference being that we use stacks to emulate the arbitrary number of so-called stoups in the lefthand side of the sequent, and it differs slightly from the one given in [4]. Indeed, since it would be to cumbersome to write out two-sequents such as

$$\begin{array}{ccc} \Gamma_1 & & \epsilon \\ \Gamma_2 & & \epsilon \\ \vdots & \vdash & \vdots \\ \Gamma_n & & \epsilon \\ \Gamma & & t \colon A \end{array}$$

in full all the time one uses a one-dimensional representation of it instead. Whereas Martini and Masini use indexed types and terms to distinguish the different levels of the two-sequent under consideration we do so by using a stack. Our Fitch-style representation $\Gamma_1 \lhd \cdots \lhd \Gamma_n \mid \Gamma \vdash t \colon A$ of the above two-sequent can simply be regarded as the sequent $(\Gamma_1)^1, \ldots, (\Gamma_n)^n, (\Gamma)^{n+1} \vdash t^{n+1} \colon A^{n+1}$ in their one-dimensional representation where the function $(-)^i$ maps a multiset $x_1 \colon A_1, \ldots, x_n \colon A_n$ into the multiset $x_1^i \colon A_1^i, \ldots, x_n^i \colon A_n^i$.

It is worth mentioning that the position of a context in the stack plays a crucial role, since there is a close connection with the nesting of $\Box$-modalities. This can be best explained by considering the informal interpretation of a two-sequent as a modal formula: for instance, the above two-sequent is interpreted as the modal formula $\bigwedge \Gamma_1 \to \Box(\bigwedge \Gamma_2 \to \cdots \Box(\bigwedge \Gamma_n \to \Box(\bigwedge \Gamma \to A)) \cdots)$. Therefore, the position of a context in the stack is in one-to-one correspondence with the number of

$$\frac{}{\mathfrak{S} \,|\, \Gamma, x\colon A \vdash x\colon A}\,\mathtt{ax} \qquad \frac{}{\mathfrak{S} \,|\, \Gamma \vdash *\colon \top}\,\top\,\mathtt{ax}$$

$$\frac{\mathfrak{S} \,|\, \Gamma \vdash t_1\colon A_1 \quad \mathfrak{S} \,|\, \Gamma \vdash t_2\colon A_2}{\mathfrak{S} \,|\, \Gamma \vdash \langle t_1, t_2\rangle\colon A_1 \wedge A_2}\,\wedge\mathcal{I} \qquad \frac{\mathfrak{S} \,|\, \Gamma \vdash t\colon A_1 \wedge A_2}{\mathfrak{S} \,|\, \Gamma \vdash \pi_i(t)\colon A_i}\,\wedge\mathcal{E}_i$$

$$\frac{\mathfrak{S} \,|\, \Gamma, x\colon A_1 \vdash t\colon A_2}{\mathfrak{S} \,|\, \Gamma \vdash \lambda x.t\colon A_1 \to A_2}\,\to\mathcal{I} \qquad \frac{\mathfrak{S} \,|\, \Gamma \vdash t\colon A_1 \to A_2 \quad \mathfrak{S} \,|\, \Gamma \vdash s\colon A_1}{\mathfrak{S} \,|\, \Gamma \vdash ts\colon A_2}\,\to\mathcal{E}$$

$$\frac{\mathfrak{S} \lhd \Gamma \,|\, \varnothing \vdash t\colon A}{\mathfrak{S} \,|\, \Gamma \vdash \mathtt{box}(t)\colon \Box A}\,\Box\mathcal{I} \qquad \frac{\mathfrak{S} \,|\, \Gamma \vdash t\colon \Box A}{\mathfrak{S} \lhd \Gamma \,|\, \Gamma' \vdash \mathtt{unbox}(t)\colon A}\,\Box\mathcal{E}$$

Table 1
Natural deduction rules

modalities that prefix its interpretation as a conjunction of formulae. It is for this reason that the substitution rules have following form.

**Lemma 2.1** *The substitution rules*

$$\frac{\mathfrak{S} \,|\, \Gamma \vdash s\colon A' \quad \mathfrak{S} \,|\, \Gamma, x\colon A' \vdash t\colon A}{\mathfrak{S} \,|\, \Gamma \vdash t[s/x]\colon A}\,\mathtt{sub}$$

*and*

$$\frac{\mathfrak{S} \,|\, \Gamma' \vdash s\colon A' \quad \mathfrak{S}'[\Gamma', x\colon A'] \,|\, \Gamma \vdash t\colon A}{\mathfrak{S}'[\Gamma'] \,|\, \Gamma \vdash t[s/x]\colon A}\,\mathtt{sub}$$

*where in the latter case* $\mathfrak{S}'[\Gamma]$ *is shorthand for* $\mathfrak{S} \lhd \Gamma \lhd \Gamma_1 \lhd \cdots \lhd \Gamma_n$*, are admissible in natural deduction.*

**Proof.** By simultaneous induction on the length of the derivation of the right premise. The following cases are the most interesting ones. If the derivation ends with an instance

$$\frac{\begin{array}{c}\pi\\ \mathfrak{S}' \,|\, \Gamma' \vdash t\colon \Box A\end{array}}{\mathfrak{S}' \lhd \Gamma' \,|\, \Gamma, x\colon A' \vdash \mathtt{unbox}(t)\colon A}$$

of $\Box\,\mathcal{E}$ then we can simply eliminate the substitution. Further, if the derivation ends with an instance

$$\frac{\begin{array}{c}\pi\\ \mathfrak{S} \lhd (\Gamma, x\colon A') \,|\, \varnothing \vdash t\colon A\end{array}}{\mathfrak{S} \,|\, \Gamma, x\colon A' \vdash \mathtt{box}(t)\colon \Box A}$$

of $\Box\,\mathcal{I}$ then we switch from the former variant of substitution to the latter. □

That we have two instances of the substitution rule follows from the fact that

| $\beta$-reductions: | $\eta$-expansions: |
|---|---|
| $\pi_i(\langle t_1, t_2\rangle) \rightsquigarrow t_i$ | $t \rightsquigarrow \langle \pi_1(t), \pi_2(t)\rangle$ |
| $(\lambda x.t)s \rightsquigarrow t[s/x]$ | $t \rightsquigarrow \lambda x.(tx)$ [where $x \notin FV(t)$] |
| $\mathtt{unbox}(\mathtt{box}(t)) \rightsquigarrow t$ | $t \rightsquigarrow \mathtt{box}(\mathtt{unbox}(t))$ |

Table 2
Reductions and expansions

we distinguish between the stack $\mathfrak{S}$ and and the current context $\Gamma$ in a sequent; we could avoid this by writing sequents as $\mathfrak{S} \lhd \Gamma \vdash t\colon A$ but refrain from doing so in order to get a tighter correspondence with the categorical semantics. Since a substitution applies only when the stack of the sequent in the left premise matches with the one of the sequent in the right premise as shown in the statement of the previous lemma, we have to prove that weakening is admissible. We have to consider the following two cases: weakening of contexts is tackled in lemma 2.2 below; weakening of stacks in lemma 2.3 below. It is worth mentioning that weakening of stacks corresponds to the lifting of indexes used in the proof of lemma 3.2 of [4]. For a concise statement of the latter result we shall use the following notational convention: given a stack $\mathfrak{S} = \Gamma_1 \lhd \cdots \lhd \Gamma_n$, we say that $\mathfrak{S}' \subseteq \mathfrak{S}$ if and only if there exists $m \geq 0$ such that $\mathfrak{S}' = \Gamma'_1 \lhd \cdots \lhd \Gamma'_m \lhd \Gamma_1 \lhd \cdots \lhd \Gamma_n$.

**Lemma 2.2** *Given $\Gamma \subseteq \Gamma'$,*

(i) *if $\mathfrak{S} \,|\, \Gamma \vdash t\colon A$ is derivable then so is $\mathfrak{S} \,|\, \Gamma' \vdash t\colon A$;*

(ii) *if $\mathfrak{S}[\Gamma] \,|\, \Gamma'' \vdash t\colon A$ is derivable then so is $\mathfrak{S}[\Gamma'] \,|\, \Gamma'' \vdash t\colon A$.*

**Proof.** By induction on the length of the derivation. □

**Lemma 2.3** *Given $\mathfrak{S}' \subseteq \mathfrak{S}$, if $\mathfrak{S} \,|\, \Gamma \vdash t\colon A$ is derivable then so is $\mathfrak{S}' \,|\, \Gamma \vdash t\colon A$.*

**Proof.** By induction on the length of the derivation. □

We conclude this section with a brief remark about the computational interpretation of the system. As usual, one is interested in relating certain derivations to each other via so-called reductions and expansions: the $\beta$-reductions and $\eta$-expansions for the positive fragment of two-sequent **K** are summarized in table 2. Note that the $\beta$-reductions are simply the ones provided in [4]. With respect to the $\eta$-expansions it is worth mentioning that each of them applies only if the term $t$ is of the appropriate type: for instance, the expansion $t \rightsquigarrow \mathtt{box}(\mathtt{unbox}(t))$ applies only if the type of $t$ is of the form $\Box A$.

## 3 Simple fibrations

The semantics we propose is based on the concept of simple fibration provided in section 1.3 of [2]. Given a category $\mathbb{B}$ with finite products $\times$, let $s(\mathbb{B})$ denote the category having:

**objects** pairs $(I, X)$ of objects of $\mathbb{B}$;

**morphisms** $(I_1, X_1) \longrightarrow (I_2, X_2)$ are pairs $(u\colon I_1 \longrightarrow I_2, f\colon I_1 \times X_1 \longrightarrow X_2)$ of morphisms in $\mathbb{B}$.

The functor $s_{\mathbb{B}}\colon s(\mathbb{B}) \longrightarrow \mathbb{B}$ given by $(I, X) \mapsto I$ and $(u, f) \mapsto u$ is then called the simple fibration on $\mathbb{B}$. We argue that a categorical semantics for the positive fragment of intuitionistic two-sequent **K** consists of a simple fibration that satisfies the following properties:

(i) the fibres $s(\mathbb{B})_I$ over $I$ are cartesian closed categories;

(ii) the substitution functor induced by the left projection $\pi_1$ has a right adjoint.

The aim of this section is to show that the syntactic model construction yields such a simple fibration. Making the assumption that we have a category $\mathbb{C}$ with objects given by formulae $A$, we show that stacks of objects of $\mathbb{C}$ yield a category **Stacks**$(\mathbb{C})$ with finite products $\odot$. Since objects of $\mathbb{C}$ can be seen as stacks that contain exactly one element, we have that sequents $\Gamma_1 \lhd \cdots \lhd \Gamma_n \,|\, \Gamma \vdash t\colon A$ can be seen as morphisms $t\colon (\bigwedge \Gamma_1 \lhd \cdots \lhd \bigwedge \Gamma_n) \odot \bigwedge \Gamma \longrightarrow A$ of **Stacks**$(\mathbb{C})$, thus giving rise to the second morphism in the pair $(u, f)$ of morphisms from the definition of $s(\mathbb{B})$ provided above.

**Definition 3.1** Given a category $\mathbb{C}$, **Stacks**$(\mathbb{C})$ denotes the category having:

**objects** stacks of objects $A$ of $\mathbb{C}$, i.e. $\mathfrak{S} ::= () \,|\, \mathfrak{S} \lhd A$;

**morphisms** $\mathfrak{S}_1 \longrightarrow \mathfrak{S}_2$ are compositions of the three basic morphisms

$1_{\mathfrak{S}}\colon \mathfrak{S} \longrightarrow \mathfrak{S} \quad \mathtt{push}^A_{\mathfrak{S}}\colon \mathfrak{S} \longrightarrow (\mathfrak{S} \lhd A) \quad \mathtt{pop}^A_{\mathfrak{S}}\colon (\mathfrak{S} \lhd A) \longrightarrow \mathfrak{S}$

satisfying the two kinds of structural properties listed below.

| inverse | identity |
|---|---|
| $\mathtt{push}^A_{\mathfrak{S}}; \mathtt{pop}^X_{\mathfrak{S}} = 1_{\mathfrak{S}}$ | $1_{\mathfrak{S} \lhd A}; \mathtt{pop}^A_{\mathfrak{S}} = \mathtt{pop}^A_{\mathfrak{S}} = \mathtt{pop}^A_{\mathfrak{S}}; 1_{\mathfrak{S}}$ |
| $\mathtt{pop}^A_{\mathfrak{S}}; \mathtt{push}^A_{\mathfrak{S}} = 1_{\mathfrak{S} \lhd A}$ | $1_{\mathfrak{S}}; \mathtt{push}^A_{\mathfrak{S}} = \mathtt{push}^A_{\mathfrak{S}} = \mathtt{push}^A_{\mathfrak{S}}; 1_{\mathfrak{S} \lhd A}$ |

Note that, since associativity of composition is trivial, the equations on the righthand side of the above table guarantee that **Stacks**$(\mathbb{C})$ is indeed a category. The equations on the lefthand side state that `push` and `pop` are inverse to each other and, furthermore, they guarantee that each composition of basic morphisms is equivalent to one that uses a minimum number of `push` and `pop` operations, thus making **Stacks**$(\mathbb{C})$ become a discrete category. As a consequence thereof we can easily prove the following result.

**Lemma 3.2** *The category* **Stacks**$(\mathbb{C})$ *has finite products.*

**Proof.** First we note that **Stacks**$(\mathbb{C})$ has a terminal object, namely the empty stack $()$. The unique morphism from $\mathfrak{S}$ to $()$ consists of $|\mathfrak{S}|$ consecutive `pop` operations. Given stacks $\mathfrak{S}_i = A_{i1} \lhd \cdots \lhd A_{ik_i}$ $(i \in \{1, 2\})$, we define their concatenation $\odot$ as follows:

$$\mathfrak{S}_1 \odot \mathfrak{S}_2 =_{def} A_{11} \lhd \cdots \lhd A_{1k_1} \lhd A_{21} \lhd \cdots \lhd A_{2k_2}$$

Binary products are given by concatenation of two stacks; left and right projections ($\pi_1 \colon \mathfrak{S}_1 \odot \mathfrak{S}_2 \longrightarrow \mathfrak{S}_1$ and $\pi_2 \colon \mathfrak{S}_1 \odot \mathfrak{S}_2 \longrightarrow \mathfrak{S}_2$) can be defined as compositions of `pop` and/or `push` operations in a straightforward way. □

**Definition 3.3** Given a category $\mathbb{C}$, $st(\mathbb{C})$ denotes the category having:

| | |
|---|---|
| **objects** | pairs $(\mathfrak{S}, A)$ of objects of **Stacks**$(\mathbb{C})$; |
| **morphisms** | $(\mathfrak{S}_1, A_1) \longrightarrow (\mathfrak{S}_2, A_2)$ are pairs $(u \colon \mathfrak{S}_1 \longrightarrow \mathfrak{S}_2, f \colon \mathfrak{S}_1 \odot A_1 \longrightarrow A_2)$ of morphisms in **Stacks**$(\mathbb{C})$. |

Note that $st(\mathbb{C})$ is equivalent to $s(\mathbf{Stacks}(\mathbb{C}))$. Hence, we have shown that the syntactic model construction yields the simple fibration given by the projection functor $s(\mathbf{Stacks}(\mathbb{C})) \longrightarrow \mathbf{Stacks}(\mathbb{C})$. However, it remains to show that this fibration also satisfies the properties mentioned at the beginning of the section. With respect to the first property we have that a close examination of the rules provided in table 1 and of the reductions and expansions provided in table 2 immediately reveals that the fibres $st(\mathbb{C})_{\mathfrak{S}}$ over $\mathfrak{S}$ are cartesian closed. The argument for the second property is more involved.

In contrast to the rules of the □-free fragment the □-rules do not induce specific structure in the fibres, but provide means to relate the fibres to each other. Indeed, we have that

$$\frac{\Gamma_1 \lhd \cdots \lhd \Gamma_n \lhd \Gamma \,|\, \varnothing \vdash t \colon A}{\Gamma_1 \lhd \cdots \lhd \Gamma_n \,|\, \Gamma \vdash t' \colon \Box A}$$

i.e. that the sequent in the premise is derivable if and only the sequent in the conclusion is. That $t \mapsto \mathtt{box}(t)$ and $t' \mapsto \mathtt{unbox}(t')$ are inverses of each other follows immediately from the lowermost $\beta$-reduction and $\eta$-expansion provided in table 2. Therefore, the introduction of the □-modality is in bijective correspondence with the application of a `pop` operation. If we use $\mathfrak{S}$ as shorthand for $\bigwedge \Gamma_1 \lhd \cdots \lhd \bigwedge \Gamma_n$ and $A'$ as shorthand for $\bigwedge \Gamma$ then we can define the two functors $\pi_1^*$ and $\Pi_{(\mathfrak{S},A')}$ as follows:

| $\pi_1^* \colon st(\mathbb{C})_{\mathfrak{S}} \longrightarrow st(\mathbb{C})_{\mathfrak{S} \odot A'}$ | $\Pi_{(\mathfrak{S},A')} \colon st(\mathbb{C})_{\mathfrak{S} \odot A'} \longrightarrow st(\mathbb{C})_{\mathfrak{S}}$ |
|---|---|
| $(\mathfrak{S}, A) \mapsto (\mathfrak{S} \odot A', \top)$ | $(\mathfrak{S} \odot A', A) \mapsto (\mathfrak{S}, \Box A)$ |
| $(\mathfrak{S}, A_1) \quad (\mathfrak{S} \odot A', \top)$ | $(\mathfrak{S} \odot A', A_1) \quad (\mathfrak{S}, \Box A_1)$ |
| $\downarrow \mapsto \downarrow$ | $\downarrow \mapsto \downarrow$ |
| $(\mathfrak{S}, A_2) \quad (\mathfrak{S} \odot A', \top)$ | $(\mathfrak{S} \odot A', A_2) \quad (\mathfrak{S}, \Box A_2)$ |

From a fibred category theory perspective we have that the substitution functor $\pi_1^* \colon st(\mathbb{C})_{\mathfrak{S}} \longrightarrow st(\mathbb{C})_{\mathfrak{S} \odot A'}$ induced by the left projection $\pi_1 \colon \mathfrak{S} \odot A' \longrightarrow \mathfrak{S}$ has a right adjoint $\Pi_{(\mathfrak{S},A')} \colon st(\mathbb{C})_{\mathfrak{S} \odot A'} \longrightarrow st(\mathbb{C})_{\mathfrak{S}}$, i.e. we obtain the following bijective correspondence:

$$\frac{[\,\pi_1^*(\mathfrak{S}, A') = ]\ (\mathfrak{S} \odot A', \top) \longrightarrow (\mathfrak{S} \odot A', A)}{(\mathfrak{S}, A') \longrightarrow (\mathfrak{S}, \Box A))\ [= \Pi_{(\mathfrak{S},A')}(\mathfrak{S} \odot A', A)\,]}$$

## 4 Conclusion

Starting from a Fitch-style presentation of two-sequent **K** we have worked out the categorical structure induced by the so-called syntactic model construction, thus providing part of the proof of a completeness theorem. We have not investigated soundness but plan to do so in future research. One of the reasons for this omission is that a more direct semantics might be obtained by switching to indexed categories and developing a categorical semantics along the lines of [3] where an **S4**-like modality has been taken into consideration as well. This line of attack would not only provide means to tackle other modal logics but it would also pave the ground for a comparison with [5] where we have proposed a semantics for a parameterized variant of relevant **K** with a flat modality, i.e. without iterations of $\Box$, in terms of indexed categories.

Besides these issue we would also like to compare our semantics with the one provided in [1]. Our one-dimensional representation of two-sequents is inspired by their Fitch-style natural deduction system and thus our semantics can be regarded as a direct semantics for it. However, this does not explain how the semantics proposed in this note relates to the one given in terms of a monoidal functor on a cartesian closed category. We believe that a good starting point for the investigation of this issue is provided by the observation that the modal rule investigated in [1] can be regarded as a derived rule of two-sequent **K**. Indeed, the following simple instance of the rule

$$\frac{\Gamma \vdash s\colon \Box A' \quad x\colon A' \vdash t\colon A}{\Gamma \vdash \mathtt{box}\ t\ \mathtt{with}\ s\ \mathtt{for}\ x\colon \Box A}$$

can be expressed as:

$$\dfrac{\dfrac{\dfrac{() \mid \Gamma \vdash s\colon \Box A'}{\Gamma \mid \varnothing \vdash \mathtt{unbox}(s)\colon A'}\,\Box\mathcal{E} \qquad \dfrac{() \mid x\colon A' \vdash t\colon A}{\Gamma \mid x\colon A' \vdash t\colon A}\,(2.3)}{\Gamma \mid \varnothing \vdash t[\mathtt{unbox}(s)/x]\colon A}\,\mathtt{sub}}{() \mid \Gamma \vdash \mathtt{box}(t[\mathtt{unbox}(s)/x])\colon \Box A}\,\Box\mathcal{I}$$

Note that if $\Gamma = x'\colon \Box A'$ and $s = x'$ then the above derived rule yields a derivation of $() \mid x'\colon \Box A' \vdash \mathtt{box}(t[\mathtt{unbox}(x')/x])\colon \Box A$ from a derivation of $() \mid x'\colon A' \vdash t\colon A$. Furthermore, there exists a term $t$ such that $() \mid x\colon \Box(A_1 \to A_2) \vdash t\colon \Box A_1 \to \Box A_2$ is derivable in two-sequent **K** (see for instance [4]). Thus we get a monoidal endofunctor on the fibre over the empty stack $()$.

## References


[1] Bellin, G., V. C. V. de Paiva and E. Ritter, *Extended Curry-Howard correspondence for a basic constructive modal logic* (2001), http://profs.sci.univr.it/~bellin/papers.html.

[2] Jacobs, B., "Categorical Logic and Type Theory," North Holland, 1999.

[3] Maietti, M. E., V. C. V. de Paiva and E. Ritter, *Categorical models for intuitionistic and linear type theory*, in: J. Tiuryn, editor, "Foundations of Software Science and Computation Structures", LNCS **1784**, 2000, pp. 223–237.

[4] Martini, S. and A. Masini, *A computational interpretation of modal proofs*, in: H. Wansing, editor, "Proof Theory of Modal Logics", Kluwer, 1996 pp. 213–241.

[5] Ranalter, K., *A semantic analysis of a logic for pragmatics with assertions, obligations and causal implication*, Fundamenta Informaticae **84** (2008), pp. 443–470.

# Principal-Centric Reasoning in Constructive Authorization Logic

## (Extended Abstract)

Deepak Garg
dg@cs.cmu.edu
Carnegie Mellon University

**Abstract**

We present an authorization logic that is quite similar to constructive modal S4. The logic assumes that principals are conceited in their beliefs. We describe the sequent calculus, Hilbert-style axiomatization, and Kripke semantics of the logic. A distinguishing characteristic of the sequent calculus is that hypothetical reasoning is relativized to beliefs of principals. We prove several meta-theoretic results including cut-elimination, and soundness and completeness for the Kripke semantics.

## 1 Introduction

Authorization refers to the act of deciding whether or not an agent making a request to perform an operation on a resource should be allowed to do so. For example, the agent may be a browser trying to read pages from a website. In that case, the site's web server may consult the browser's credentials and a `.htaccess` file to determine whether to send the pages or not. Such access control is pervasive in computer systems. As systems and their user environments evolve, policies used for access control may become complex and error prone. This suggests the need for formal mechanisms to represent, enforce, and analyze policies. Logic appears to be a useful mechanism for these purposes. Policies may be expressed as formulas in a suitably chosen logic. This has several merits. First, the logic's rigorous inference eliminates any ambiguity in meaning that may be inherent in a textual description of policies. Second, policies may be enforced end-to-end using generic logic-based mechanisms like proof-carrying authorization [8–10, 29]. Third, by writing policies in a logic, there is hope that the policies themselves can be checked for correctness against some given criteria.

Whereas first-order logic and sometimes propositional logic suffice to express many authorization policies, distributed systems pose a peculiar challenge: how do we express and combine policies of *different* agents and systems? This is often necessary since policies and the authorizations derived from them may vary from system to system.

Policies on different systems may also interact to allow or deny access. To model such distributed policies, Abadi and others proposed logics with formulas of the form $K$ says $A$, where $K$ is an agent or a system (abstractly called a principal) and $A$ is a formula representing a policy [6, 28]. The intended meaning of the formula is that principal $K$ states, or believes that policy $A$ holds. From a logical perspective $K$ says $\cdot$ is a modality and the logic is an indexed modal logic with one modality for each principal. We call such a modal logic an *authorization logic*. In the past fifteen years there have been numerous proposals describing authorization logics that differ widely in the specific axioms (or inference rules) used for $K$ says $\cdot$ [2, 3, 8–10, 15, 17, 19, 24–26, 29, 30]. One emerging trend is the increased use of intuitionistic logics for authorization (e.g., [3, 19, 22, 24–26, 29, 37]) as opposed to classical logics.

This paper presents a new intuitionistic authorization logic called $\mathrm{DTL}_0$. This logic is peculiar in a certain respect: it abandons the usual objectivity in reasoning from hypothesis, relativizing hypothetical reasoning to principals. The hypothetical judgment of the logic has the form $\Gamma \xrightarrow{K} A$, which means, up to a first approximation, that under the assumption that all beliefs of $K$ are true, the hypotheses $\Gamma$ imply $A$. Although this choice of binding hypothetical reasoning to principals may be unintuitive from a philosophical point of view, it seems attractive from the perspective of access control.

Our primary interest in developing $\mathrm{DTL}_0$ is deployment in proof-carrying authorization [8–10, 29, 37]. Hence our main focus is $\mathrm{DTL}_0$'s proof-theory, especially the sequent calculus, which we describe in detail (Section 3). We prove several meta-theoretic properties of the sequent calculus, including cut-elimination (Section 3.1). We also present a Hilbert-style system for $\mathrm{DTL}_0$ (Section 2), and sound and complete Kripke semantics (Section 4). The principal-centric reasoning of $\mathrm{DTL}_0$ reflects in the Kripke semantics: worlds are explicitly associated with principals who may view them. This suggests that principals in $\mathrm{DTL}_0$ may be related to nominals from hybrid logic [13, 14, 16]. We also show that $\mathrm{DTL}_0$ is a generalization of constructive modal S4 [7, 33].

$\mathrm{DTL}_0$ is a fragment of a larger authorization logic, DTL, which we are currently developing. The latter is quite broad, incorporating first-order quantifiers, explicit time for modeling time-bounded policies [19], and linearity for modeling consumable credentials [25]. Besides developing the logic's theory, a secondary goal of ongoing work is to understand how $\mathrm{DTL}_0$ relates to existing authorization logics, through translations between them. The eventual objective of this line of work is more ambitious; we want to establish a common framework in which policies written in different logics may be combined. Initial efforts in this direction using (classical) modal S4 as foundation appeared in earlier work [24].

By itself, this paper makes two contributions. First, it presents a new authorization logic that explicitly relativizes hypothetical reasoning to principals, and describes the logic's proof theory. To the best of our understanding, such relativization is unique to our logic, at least in the context of authorization. A second, albeit minor contribution of the paper is sound and complete Kripke semantics, which are relatively rare for authorization logics (as opposed to their prevalence in modal logics). The only other examples we know of are Kripke semantics for authorization logics based on lax-like

modalities [24], and those for an earlier authorization logic based on the modal logic K [6].

To save space, proofs of theorems and many other results related to $\mathrm{DTL}_0$ have been omitted from this extended abstract. These may be found in the full version of the paper that is available on the author's web page [23]. In addition to proofs and a description of some of the design choices, the full version contains a natural deduction system, a construction of canonical Kripke models, and sound and complete translations between $\mathrm{DTL}_0$ and other modal logics, including several authorization logics and constructive multi-modal S4.

## 2 The logic $\mathrm{DTL}_0$

$\mathrm{DTL}_0$ extends propositional intuitionistic logic with a principal-indexed modality, $K$ says $A$. Principals, denoted $K$, are abstractions for users, programs, machines, and systems, that either create policies or request access to resources. We stipulate a fixed set of principals `Prin`, pre-ordered by a relation written $\succeq$. $K_1 \succeq K_2$ is read "principal $K_1$ is stronger than principal $K_2$", and entails that $K_1$ says $A$ implies $K_2$ says $A$ for every formula $A$. We assume that `Prin` has at least one maximum element, called the *local authority* (denoted $\ell$).[1] The syntax of formulas in $\mathrm{DTL}_0$ is shown below. $P$ denotes atomic formulas.

$$A, B, C \ ::= \ P \mid A \wedge B \mid A \vee B \mid \top \mid \bot \mid A \supset B \mid K \text{ says } A$$

**Axiomatic Proof-System.** A Hilbert-style proof-system for $\mathrm{DTL}_0$ consists of any axiomatization of propositional intuitionistic logic (elided here), and the following axioms and rules for $K$ says $A$. We write $\vdash A$ to mean that $A$ is valid.

$$\frac{\vdash A}{\vdash K \text{ says } A} \quad \text{(nec)}$$

$$\vdash (K \text{ says } (A \supset B)) \supset ((K \text{ says } A) \supset (K \text{ says } B)) \quad \text{(K)}$$

$$\vdash (K \text{ says } A) \supset K \text{ says } K \text{ says } A \quad (4)$$

$$\vdash K \text{ says } ((K \text{ says } A) \supset A) \quad \text{(C)}$$

$$\vdash (K_1 \text{ says } A) \supset (K_2 \text{ says } A) \text{ if } K_1 \succeq K_2. \quad \text{(S)}$$

(nec) and (K) are the usual necessitation rule and closure under consequence axiom for normal modal logics (see e.g., [12]). (4) is also standard from modal logics such as S4. (C) is the characterizing axiom of $\mathrm{DTL}_0$. It is characteristic of the doxastic logic of conceited reasoners (hence the name C) [35]. Intuitively, the axiom means that every principal says that all its statements are true. Although the propriety of this axiom in the context of doxastic reasoning has been questioned, it seems quite useful for authorization. The axiom (S) means that whenever principal $K_1$ believes a formula $A$, every weaker principal $K_2$ believes it as well.

[1] To the best of our understanding, the term *local authority* as used here was first introduced in the preview implementation of the language SecPAL [1].

The following properties may be established in $\mathrm{DTL}_0$. $\not\vdash A$ means that $A$ is not valid in the stated generality (although specific instances of $A$ may be valid). $A \equiv B$ denotes $(A \supset B) \wedge (B \supset A)$.

$\vdash (\ell \text{ says } A) \supset (K \text{ says } A)$

$\vdash (K \text{ says } K \text{ says } A) \equiv (K \text{ says } A)$

$\not\vdash A \supset K \text{ says } A$

$\not\vdash (K \text{ says } A) \supset A$

$\vdash (K \text{ says } (A \wedge B)) \equiv ((K \text{ says } A) \wedge (K \text{ says } B))$

$\not\vdash (K \text{ says } (A \vee B)) \supset ((K \text{ says } A) \vee (K \text{ says } B))$

$\not\vdash \bot$

$\not\vdash (K \text{ says } A) \supset (K' \text{ says } (K \text{ says } A))$

The last property means that if a principal $K$ states policy $A$, not every principal may believe this. In some cases, this may not be desirable, since some policies may be stated and *published* by $K$. If $K$ publishes policy $A$, we may expect that $K' \text{ says } K \text{ says } A$. In $\mathrm{DTL}_0$, published policies may be expressed using the defined connective $K \text{ publ } A = \ell \text{ says } K \text{ says } A$ (read "$K$ publishes $A$"), which satisfies the following properties:

$\vdash (K \text{ publ } A) \supset K \text{ says } A.$

$\not\vdash (K \text{ says } A) \supset K \text{ publ } A.$

$\vdash (K \text{ publ } A) \supset K' \text{ says } (K \text{ publ } A).$

$\vdash (K \text{ publ } A) \supset K' \text{ says } (K \text{ says } A).$

**Example 2.1** ($\mathrm{DTL}_0$)**.** We illustrate the use of $\mathrm{DTL}_0$ for expressing authorization policies through a simple example. Suppose that the principal OAL (Online Academic Library) represents an online repository of scientific articles. Academics institutions (such as CMU) may buy corporate subscriptions that allow all their members to download articles from OAL. It is up to the subscribing institutions to tell OAL who their members are. Alice is an individual who wishes to download an article from OAL. Let the formula `downloadAlice` mean that Alice may download articles from OAL, and let `memberAliceCMU` mean that Alice is a member of CMU. Further, let us assume that CMU has a subscription at OAL. The following represent possible policies of the principals.

1. OAL says ((CMU says `memberAliceCMU`) $\supset$ `memberAliceCMU`)
2. OAL says (`memberAliceCMU` $\supset$ `downloadAlice`)

3. CMU publ `memberAliceCMU`

The first policy, stated by OAL, means that if CMU says that Alice is its member, then this is the case. The second policy, also stated by OAL, means that if Alice is a member of CMU, then she may download articles. The third policy, stated and published by CMU, means that Alice is a member of CMU. It is easy to check that these three policies entail the formula OAL says `downloadAlice` in $\mathrm{DTL}_0$, and that this would not be the case if we changed publ to says in the last policy.

# 3 Sequent Calculus

Now we describe a sequent calculus for $\mathrm{DTL}_0$. Our presentation is inspired by earlier work on proof-theory for modal logics [25, 33]. Broadly, we follow Martin-Löf's judgmental method [31], and make a strong distinction between formulas and judgments. Judgments are the objects of knowledge, and are established through proofs. Formulas are subjects of judgments. For $\mathrm{DTL}_0$, we use two basic (categorical) judgments: $A$ true, meaning that formula $A$ is true, and $K$ claims $A$, meaning that principal $K$ believes or claims that formula $A$ is true. The two categorical judgments do not entail each other in general. $K$ says $A$ *internalizes* the judgment $K$ claims $A$ as a formula, allowing it to be combined with other connectives. In other words the judgments ($K$ says $A$) true and $K$ claims $A$ are equivalent.

To reason from hypothesis, we introduce hypothetical judgments (sequents) $\Gamma \xrightarrow{K} A$ true, informally meaning that principal $K$ may reason from the hypothesis in $\Gamma$ that $A$ is true. Formally, the symbol $\Gamma$ denotes a (possibly empty) multiset of categorical judgments, called the hypothesis or assumptions:

$$\Gamma \ ::= \ \cdot \mid \Gamma, A \text{ true} \mid \Gamma, K' \text{ claims } A$$

The principal $K$ is called the *context* of the judgment. In context $K$, $K'$ claims $C$ entails $C$ true if $K' \succeq K$. This is the only principle that distinguishes reasoning in one context from that in another. The formula $A$ on the right of $\xrightarrow{K}$ is called the conclusion of the sequent.

The inference rules of the sequent calculus are shown in Figure 1. For brevity, we often elide the judgment name true, abbreviating $A$ true to $A$. The notation $\Gamma|_K$ used in the rule (saysR) stands for the multiset $\{(K' \text{ claims } C) \in \Gamma \mid K' \succeq K\}$. If we assume that formula $A$ is true, we should certainly be able to conclude that $A$ is true. For atomic formulas, this may be established by the rule (init); for others we prove it as a theorem (see Theorem 3.2).

The rules (claims), (saysR), and (saysL) characterize $\mathrm{DTL}_0$. Read from the conclusion to the premises, the rule (claims) states that whenever we assume $K$ claims $A$, we are also justified in assuming that $A$ is true, if we are reasoning in a context $K'$ such that $K \succeq K'$. The rule (saysR) means that $K$ says $A$ may be established in any context if we can prove in context $K$ that $A$ is true using only assumptions $K''$ claims $C$ for $K'' \succeq K$. Observe that this is the only rule that changes the context of the sequent.

$$\frac{P \text{ atomic}}{\Gamma, P \xrightarrow{K} P}\text{init} \qquad \frac{\Gamma, K \text{ claims } A, A \xrightarrow{K'} C \qquad K \succeq K'}{\Gamma, K \text{ claims } A \xrightarrow{K'} C}\text{claims}$$

$$\frac{\Gamma|_K \xrightarrow{K} A}{\Gamma \xrightarrow{K'} K \text{ says } A}\text{saysR} \qquad \frac{\Gamma, K \text{ says } A, K \text{ claims } A \xrightarrow{K'} C}{\Gamma, K \text{ says } A \xrightarrow{K'} C}\text{saysL}$$

$$\frac{\Gamma \xrightarrow{K} A \qquad \Gamma \xrightarrow{K} B}{\Gamma \xrightarrow{K} A \wedge B}\wedge\text{R} \qquad \frac{\Gamma, A \wedge B, A, B \xrightarrow{K} C}{\Gamma, A \wedge B \xrightarrow{K} C}\wedge\text{L}$$

$$\frac{\Gamma \xrightarrow{K} A}{\Gamma \xrightarrow{K} A \vee B}\vee\text{R}_1 \qquad \frac{\Gamma \xrightarrow{K} B}{\Gamma \xrightarrow{K} A \vee B}\vee\text{R}_2 \qquad \frac{\Gamma, A \vee B, A \xrightarrow{K} C \qquad \Gamma, A \vee B, B \xrightarrow{K} C}{\Gamma, A \vee B \xrightarrow{K} C}\vee\text{L}$$

$$\frac{}{\Gamma \xrightarrow{K} \top}\top\text{R} \qquad \frac{}{\Gamma, \bot \xrightarrow{K} C}\bot\text{L}$$

$$\frac{\Gamma, A \xrightarrow{K} B}{\Gamma \xrightarrow{K} A \supset B}\supset\text{R} \qquad \frac{\Gamma, A \supset B \xrightarrow{K} A \qquad \Gamma, A \supset B, B \xrightarrow{K} C}{\Gamma, A \supset B \xrightarrow{K} C}\supset\text{L}$$

Figure 1: Sequent calculus for $\text{DTL}_0$

The rule (saysL) captures the idea that $K$ says $A$ internalizes $K$ claims $A$: if we assume that $K$ says $A$ is true, then we may also assume $K$ claims $A$.

The rules for the connectives $\wedge$, $\vee$, $\top$, $\bot$, and $\supset$ are standard, except for a context which is associated with each sequent. We elide a description of these standard rules, and turn to the meta-theoretic properties of the sequent calculus.

### 3.1 Meta-Theory

Meta-theoretic properties, such as cut-elimination, are important from our perspective because proof-carrying authorization (our intended application) is heavily based in proof-checking, and proof-construction. Besides, meta-theoretic properties also imply that the inference rules of the logic fit well with each other, increasing faith in the logic's good foundation. Cut-elimination also means that all proofs can be normalized. Normalization is sometimes useful for auditing proofs of authorization.

Formally, the cut-elimination theorem states that adding a cut rule to a sequent calculus does not make more judgments provable. This is an easy consequence of the following theorem.

**Theorem 3.1** (Admissibility of Cut)**.** *The following hold for the sequent calculus of Figure 1.*

1. $\Gamma \xrightarrow{K} A$ *and* $\Gamma, A \xrightarrow{K} C$ *imply that* $\Gamma \xrightarrow{K} C$.

2. $\Gamma|_K \xrightarrow{K} A$ *and* $\Gamma, K \;\mathsf{claims}\; A \xrightarrow{K'} C$ *imply that* $\Gamma \xrightarrow{K'} C$.

*Proof (Outline).* Both statements can be proved simultaneously by lexicographic induction, first on the size of the cut formula $A$, and then on the size of the two given derivations, as in earlier work [32]. □

The logical dual of the cut-elimination theorem is identity, which states that whenever $A$ $\mathsf{true}$ is assumed as a hypothesis, we may conclude it. The following theorem captures this generalization of the (init) rule.

**Theorem 3.2** (Identity)**.** *For each formula* $A$, $\Gamma, A \xrightarrow{K} A$.

*Proof (Outline).* By induction on $A$. □

Another theorem of interest for $\mathrm{DTL}_0$ is subsumption, which states that contexts lower in the order $\succeq$ allow more provable formulas.

**Theorem 3.3** (Subsumption)**.** *If* $\Gamma \xrightarrow{K} A$ *and* $K \succeq K'$, *then* $\Gamma \xrightarrow{K'} A$.

*Proof (Outline).* By induction on the given derivation of $\Gamma \xrightarrow{K} A$. □

Finally, we prove equivalence of the sequent calculus and the Hilbert-style system.

**Theorem 3.4** (Equivalence)**.** $\Gamma \xrightarrow{K} A$ *if and only if* $\vdash K \;\mathsf{says}\; (\Gamma \supset A)$.

*Proof (Outline).* In each direction by induction on the given derivations. For proving the "only-if" clause, we have to generalize the Hilbert-style system to allow hypothesis and prove the deduction theorem. This is done in the usual way. □

Observe that there is no equivalent of $\vdash B$ in the sequent calculus unless $B$ has the form $K \;\mathsf{says}\; A$. In this sense, the above theorem actually *embeds* the sequent calculus into the Hilbert-style system. While it is possible to recover the entire Hilbert-style system in the sequent calculus by adding non-indexed hypothetical judgments $\Gamma \longrightarrow A$, this extension seems uninteresting for authorization policies, and we omit it here.

## 4 Kripke Semantics for $\mathrm{DTL}_0$

Next we describe sound and complete Kripke semantics for $\mathrm{DTL}_0$. Although not directly applicable to policies, Kripke semantics are an invaluable tool for proving properties of the logic (e.g., [4, 24]). There is also hope that Kripke countermodels can be used as proofs of *failure*, in case an authorization does not succeed. Our presentation of Kripke

semantics is inspired by work on the modal logic constructive S4 [7], and also uses some ideas from work on Kripke semantics of lax logic [21, 24].

The distinguishing characteristic of our Kripke semantics are *views* [24]. With each world $w$, we associate a set of principals $\theta(w)$ to whom the world is said to be visible. Our correctness property is that $\cdot \xrightarrow{K} A$ if and only if *each world visible to* $K$ *satisfies* $A$.[2] In this manner, views allow us to distinguish reasoning in one context from that in another. If $K \succeq K'$ then we require that any world visible to $K'$ also be visible to $K$. This ensures that context $K$ validates fewer formulas than context $K'$, and captures the subsumption principle (Theorem 3.3).

We model falsehood by explicitly specifying in each frame a set $F$ of worlds where $\bot$ holds. These worlds are called fallible worlds [20, 21, 36]. We say that $w \models \bot$ iff $w \in F$. To model intuitionistic implication, we use a pre-order $\leq$ between worlds (as usual) and say that $w \models A \supset B$ iff for all $w'$, $w \leq w'$ and $w' \models A$ imply $w' \models B$. Finally, to model the modality $\mathsf{says}$, we use a principal-indexed binary relation $\sqsubseteq_K$ between worlds and define:

$$w \models K \ \mathsf{says}\ A \text{ iff either } w \in F \text{ or for all } w', w'',\ w \leq w' \sqsubseteq_K w'' \text{ implies } w'' \models A.$$

The clause $w \in F$ in the above definition is required to validate $\bot \supset K \ \mathsf{says}\ A$. The remaining definition is a generalization of satisfaction for $\Box A$ from Kripke semantics of constructive S4 [7]. To validate axiom (4), we stipulate that $\sqsubseteq_K ; \leq$ be a subset of $\sqsubseteq_K$.[3]

Both the use of a pre-order to model intuitionistic implication, and the use of different binary relations to model each modality are standard in modal logic. The novelty here is the interaction of these relations with views. We require that $\leq$ preserve views, i.e., if $w \leq w'$ and $w$ be visible to $K$, then $w'$ also be visible to $K$. We also require that whenever $w \sqsubseteq_K w'$, $w'$ be visible to $K$. For example, in the definition of $w \models K \ \mathsf{says}\ A$ above, $w''$ would be visible to $K$. By forcing these restrictions, we ensure that the semantics of all connectives except $K \ \mathsf{says}\ \cdot$ can be defined without changing views. On the other hand, the semantics of $K \ \mathsf{says}\ \cdot$ shift the reasoning to worlds that are visible to $K$. This subtle interaction between views and binary relations captures the exact meaning of formulas in $\mathrm{DTL}_0$.

**Definition 4.1** (Kripke Models)**.** A Kripke model $M$ for $\mathrm{DTL}_0$ is a tuple $(W, \theta, \leq, (\sqsubseteq_K)^{K \in \mathtt{Prin}}, \rho, F)$, where

- $W$ is a non-empty set of worlds (worlds are denoted $w$).
- $\theta : W \mapsto 2^{\mathtt{Prin}}$ is a *view function* that maps each world $w$ to a set of principals. If $K \in \theta(w)$, we say that $w$ is visible to $K$, else $w$ is said to be invisible to $K$. We often write $W^K$ for the set $\{w \in W \mid K \in \theta(w)\}$. We require that:

[2] Throughout this section we use the sequent calculus of $\mathrm{DTL}_0$ to state correctness properties. Use of the sequent calculus as opposed to the axiomatic system is partly a matter of personal taste and partly a matter of technical convenience.

[3] We believe that this condition can be weakened to $(\sqsubseteq_K ; \leq) \subseteq (\leq ; \sqsubseteq_K)$ without affecting the correctness of the Kripke semantics, but have not verified that this is the case.

(View-closure) $K \in \theta(w)$ and $K' \succeq K$ imply $K' \in \theta(w)$.

- $\leq$ is a pre-order on $W$ called the *implication relation*. We require that:

  (Imp-mon) $w \leq w'$ imply $\theta(w) \subseteq \theta(w')$.

- For each $K$, $\sqsubseteq_K$ is a subset of $W \times W^K$ called the *modality relation*. We require that:

  (Mod-refl) If $w \in W^K$, then $w \sqsubseteq_K w$.

  (Mod-trans) $\sqsubseteq_K$ be transitive.

  (Mod-closure) $w \sqsubseteq_K w'$ and $K' \succeq K$ imply $w \sqsubseteq_{K'} w'$

  (Commutativity) If $w \sqsubseteq_K w' \leq w''$, then $w \sqsubseteq_K w''$.

- $\rho : W \mapsto 2^{\texttt{AtomicFormulas}}$ is a *valuation function* that maps each world to the set of atomic formulas that hold in it. We require that:

  (Rho-her) $P \in \rho(w)$ and $w \leq w'$ imply $P \in \rho(w')$.

- $F \subseteq W$ is the set of *fallible worlds*. We require that:

  (F-her) $w \in F$ and $w \leq w'$ imply $w' \in F$.

  (F-univ) $w \in F$ imply $P \in \rho(w)$

**Definition 4.2** (Satisfaction)**.** Given a model $M = (W, \theta, \leq, (\sqsubseteq_K)^{K \in \texttt{Prin}}, \rho, F)$, and a world $w \in W$, the satisfaction relation $w \models A$ (world $w$ satisfies formula $A$) is defined by induction on $A$ as follows.

$w \models P$ iff $P \in \rho(w)$.

$w \models A \wedge B$ iff $w \models A$ and $w \models B$.

$w \models A \vee B$ iff $w \models A$ or $w \models B$.

$w \models \top$.

$w \models \bot$ iff $w \in F$.

$w \models A \supset B$ iff for all $w'$, $w \leq w'$ and $w' \models A$ imply $w' \models B$.

$w \models K \ \mathsf{says}\ A$ iff either $w \in F$ or for all $w', w''$, $w \leq w' \sqsubseteq_K w''$ implies $w'' \models A$.

We say that a principal $K$ validates $A$ in model $M$ (written $M \models^K A$) if for each world $w \in W^K$ in $M$, it is the case that $w \models A$. The Kripke semantics defined above are sound and complete in the following sense.

**Theorem 4.3** (Soundness and Completeness)**.** $\cdot \xrightarrow{K} A$ *in the sequent calculus if and only if for each Kripke model* $M$*,* $M \models^K A$*.*

Soundness ("only if" direction) follows by an induction on the given sequent calculus proof. We must generalize the statement to allow non-empty hypotheses. The proof of completeness ("if" direction) uses a canonical model construction, which we omit here. The construction generalizes Alechina et al's construction of canonical models for constructive S4 [7].

### $\text{DTL}_0$ as a Generalization of Constructive S4

In the special case where there is only one principal (say $\ell$), $\text{DTL}_0$ reduces to the modal logic constructive S4. The sole modality $\ell$ says $A$ behaves exactly like the necessitation modality $\Box A$. The sequent calculus of Figure 1 reduces to a judgmental sequent calculus for constructive S4 (e.g., [25]). Similarly, the Kripke semantics reduce to those of constructive S4 described by Alechina et al [7], with the exception that our treatment of falsehood uses fallible worlds explicitly, and that $\text{DTL}_0$ does not have a modality corresponding to $\Diamond$. The following theorem is straightforward.

**Theorem 4.4.** *In the special case where there is only one principal $\ell$, the following are equivalent:*

1. $\vdash A$ *treating* $\ell$ says $\cdot$ *as the* $\Box$ *modality from constructive S4.*
2. $\xrightarrow{\ell} A$ *in the sequent calculus of Figure 1.*
3. $\vdash \ell$ says $A$ *in the axiomatic system of Section 2.*

Even though $\text{DTL}_0$ reduces to constructive S4 when there is only one principal, it is very different from the multi-modal constructive S4 obtained by taking independent S4 $\Box$ modalities (i.e., the logic $\text{S4} \otimes \text{S4} \ldots \otimes \text{S4}$). For example, the latter logic validates $(K \text{ says } K' \text{ says } A) \supset K' \text{ says } A$, which $\text{DTL}_0$ does not. In earlier work, we described the use of this logic for modeling *knowledge* in authorization policies [25].

## 5 Related Work

Many authorization logics have been proposed in the past, all of which contain the modality $K$ says $A$ [2, 3, 8–10, 15, 17, 19, 24–26, 29, 30]. The axioms and rules used in these logics differ widely. The particular combination of rules used in $\text{DTL}_0$ appears to be novel. Perhaps most closely related to $\text{DTL}_0$ is a proposal by Abadi in a survey paper [2], where the axiom $(K \text{ says } A) \supset (K' \text{ says } K \text{ says } A)$ is suggested. says with this axiom behaves very much like the defined connective publ in $\text{DTL}_0$. In a recent paper, Abadi studies connections between many possible axiomatizations of says, as well as higher level policy constructs such as delegation and control [4].

Also related to $\text{DTL}_0$ is work on languages for authorization (e.g., [11, 18, 27, 34]), most notably the languages Soutei and Binder [18, 34]. Our use of the term "context" is borrowed from the latter. Binder was also one of the earliest languages to explicitly define a notion of exporting policies from one context to another, which is very similar to publication of policies illustrated in Section 2. The pre-order $\succeq$ on principals draws on

ideas from the Dependency Core Calculus [3, 5], where the modal indices are elements of a lattice.

Our Kripke semantics, as well as the completeness proof, are based on those of Alechina et al's work [7] for constructive S4. View functions were used earlier by the author and Abadi to describe semantics of authorization logics with lax-like modalities [24]. Fallible worlds have been used in the past to explain intuitionistic logic [20, 36], and also in semantics of lax logic [21]. It also appears to us that $\mathrm{DTL}_0$ may be closely related to intuitionistic hybrid logics, and especially to the work of Chadha and others [16], but further investigation is needed to make an explicit connection. The presentation of the sequent calculus for $\mathrm{DTL}_0$ is inspired by Pfenning and Davies' work on constructive S4 [33], and more directly by earlier work of the author and others [25].

## 6 Conclusion

We have presented a new constructive authorization logic, which explicitly relativizes hypothetical reasoning to the policies of individual principals. We have described the proof-theory and Kripke semantics of the logic. In ongoing work, we are considering extensions of the logic with first-order connectives, explicit time, and linearity to model other policy motifs. We are also translating existing authorization logics and languages for writing authorization policies to $\mathrm{DTL}_0$, with the goal of understanding relations between the different formalisms.

There are several other avenues for future work. For instance, there seem to be strong connections between $\mathrm{DTL}_0$ and hybrid logics. A useful generalization of $\mathrm{DTL}_0$ would be to internalize the pre-order $\succeq$ as a formula. Such an extension would allow us to model delegation, along lines of the "speaks for" connective present in some authorization logics [3, 6, 24, 28]. Although the proof-theory of such an extension is relatively straightforward, it would be interesting to see its effects on Kripke semantics.

**Acknowledgment.** This work was partly supported by the Air Force Research Laboratory under grant no. FA87500720028. The author wishes to acknowledge Frank Pfenning for discussions and feedback on the logic and the paper, and Martín Abadi for feedback on the logic.

## References

[1] SecPAL Preview release for .NET, 2006. http://research.microsoft.com/projects/SecPAL/.

[2] Martín Abadi. Logic in access control. In *Proceedings of the 18th Annual Symposium on Logic in Computer Science (LICS'03)*, pages 228–233, June 2003.

[3] Martín Abadi. Access control in a core calculus of dependency. *Electronic Notes in Theoretical Computer Science*, 172:5–31, April 2007. *Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin.*

[4] Martín Abadi. Variations in access control logic, 2008. Personal communication.

[5] Martín Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. A core calculus of dependency. In *Conference Record of the 26th Sympoisum on Principles Of Programming Languages (POPL'99)*, pages 147–160, San Antonio, Texas, January 1999. ACM Press.

[6] Martín Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, 1993.

[7] Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and Kripke semantics for constructive S4 modal logic. In *CSL '01: Proceedings of the 15th International Workshop on Computer Science Logic*, pages 292–307, London, UK, 2001. Springer-Verlag.

[8] Andrew W. Appel and Edward W. Felten. Proof-carrying authentication. In G. Tsudik, editor, *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 52–62, Singapore, November 1999. ACM Press.

[9] Lujo Bauer. *Access Control for the Web via Proof-Carrying Authorization*. PhD thesis, Princeton University, November 2003.

[10] Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-enabled authorization in the Grey system. In *Information Security: 8th International Conference (ISC '05)*, Lecture Notes in Computer Science, pages 431–445, September 2005.

[11] Moritz Y. Becker, Cédric Fournet, and Andrew D. Gordon. Design and semantics of a decentralized authorization language. In *20th IEEE Computer Security Foundations Symposium*, pages 3–15, 2007.

[12] P. Blackburn, J. van Benthem, and F. Wolter. *Handbook of Modal Logic*. Elsevier B. V., 2007.

[13] Patrick Blackburn. Representation, reasoning, and relational structures: A hybrid logic manifesto. *Logic Journal of IGPL*, 8(3):339–365, 2000.

[14] Torben Braüner and Valeria de Paiva. Towards constructive hybrid logic. In *Electronic Proceedings of Methods for Modalities 3 (M4M3)*, 2003.

[15] J. G. Cederquist, R. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *International Journal of Information Security*, 6(2):133–151, 2007.

[16] Rohit Chadha, Damiano Macedonio, and Vladimiro Sassone. A hybrid intuitionistic logic: Semantics and decidability. *Journal of Logic and Computation*, 16:27–59(33), February 2006.

[17] Jason Crampton, George Loizou, and Greg O' Shea. A logic of access control. *The Computer Journal*, 44(1):137–149, 2001.

[18] John DeTreville. Binder, a logic-based security language. In M. Abadi and S. Bellovin, editors, *Proceedings of the 2002 Symposium on Security and Privacy (S&P'02)*, pages 105–113, Berkeley, California, May 2002. IEEE Computer Society Press.

[19] Henry DeYoung, Deepak Garg, and Frank Pfenning. An authorization logic with explicit time. In *Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSF-21)*, Pittsburgh, Pennsylvania, June 2008. IEEE Computer Society Press. To appear. Extended version available as Technical Report CMU-CS-07-166.

[20] M. Dummett. *Elements of Intuitionism*. Oxford University Press, 1977.

[21] M. Fairtlough and M.V. Mendler. Propositional lax logic. *Information and Computation*, 137(1):1–33, August 1997.

[22] Cédric Fournet, Andrew Gordon, and Sergio Maffeis. A type discipline for authorization in distributed systems. In *CSF '07: Proceedings of the 20th IEEE Computer Security Foundations Symposium*, pages 31–48. IEEE Computer Society, 2007.

[23] Deepak Garg. Principal-centric reasoning in constructive authorization logic (full version), 2008. Available electronically from http://www.cs.cmu.edu/~dg.

[24] Deepak Garg and Martín Abadi. A modal deconstruction of access control logics. In *Proceedings of the 11th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2008)*, pages 216–230, Budapest, Hungary, April 2008.

[25] Deepak Garg, Lujo Bauer, Kevin Bowers, Frank Pfenning, and Michael Reiter. A linear logic of affirmation and knowledge. In D. Gollman, J. Meier, and A. Sabelfeld, editors, *Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS '06)*, pages 297–312, Hamburg, Germany, September 2006. Springer LNCS 4189.

[26] Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In J. Guttman, editor, *Proceedings of the 19th Computer Security Foundations Workshop (CSFW '06)*, pages 283–293, Venice, Italy, July 2006. IEEE Computer Society Press.

[27] Yuri Gurevich and Itay Neeman. DKAL: Distributed-knowledge authorization language. In *Proceedings of the 21st IEEE Symposium on Computer Security Foundations (CSF-21)*, 2008. To appear.

[28] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, November 1992.

[29] Chris Lesniewski-Laas, Bryan Ford, Jacob Strauss, Robert Morris, and M. Frans Kaashoek. Alpaca: Extensible authorization for distributed services. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS-2007)*, Alexandria, VA, October 2007.

[30] Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. *ACM Transactions on Information and Systems Security*, 6(1):128–171, 2003.

[31] Per Martin-Löf. On the meanings of the logical constants and the justifications of the logical laws. *Nordic Journal of Philosophical Logic*, 1(1):11–60, 1996.

[32] Frank Pfenning. Structural cut elimination I. Intuitionistic and classical logic. *Information and Computation*, 157(1/2):84–141, March 2000.

[33] Frank Pfenning and Rowan Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 11:511–540, 2001.

[34] Andrew Pimlott and Oleg Kiselyov. Soutei, a logic-based trust-management system. In *Proceedings of the Eighth International Symposium on Functional and Logic Programming (FLOPS 2006)*, pages 130–145, 2006.

[35] Raymond M. Smullyan. *Forever Undecided*. Oxford University Press, 1988.

[36] A. S. Troelstra and D. Van Dalen. *Constructivism in Mathematics: Volume 2*. Elsevier Science Publishing Company, 1988.

[37] Jeffrey A. Vaughan, Limin Jia, Karl Mazurak, and Steve Zdancewic. Evidence-based audit. In *Proceedings of the 21st IEEE Symposium on Computer Security Foundations (CSF-21)*, 2008. To appear.