Intuitionistic Modal Logic Made Explicit

Michel Marti[*]
Institute of Computer Science, University of Bern
mmarti@inf.unibe.ch

Thomas Studer
Institute of Computer Science, University of Bern
tstuder@inf.unibe.ch

Abstract

The logic of proofs of Heyting arithmetic includes explicit justifications for all admissible rules of intuitionistic logic in order to satisfy completeness with respect to provability semantics. We study the justification logic iJT4, which does not have these additional justification terms. We establish that iJT4 is complete with respect to modular models, which provide a Kripke-style semantics, and that there is a realization of intuitionistic S4 into iJT4. Hence iJT4 can be seen as an explicit version of intuitionistic S4.

1 Introduction

Justification logics are explicit modal logics in the sense that they unfold the $\Box$-modality in families of so-called justification terms. Instead of formulas $\Box A$, meaning that A is known, justification logics include formulas $t : A$, meaning that A is known for reason t.

The original semantics for the first justification logic, the Logic of Proofs LP, was Artemov's provability semantics that interpreted $t : A$ roughly as *t represents a proof of A* in the sense of a formal proof predicate in Peano Arithmetic [1, 2, 21].

Later Fitting [15] interpreted justifications as evidence in a more general sense and introduced epistemic, i.e., possible world, models for justification logics. These models have been further developed to modular models as we use them in this paper [6, 19]. This general reading of justification led to many applications in epistemic logic [4, 5, 8, 9, 10, 11, 12, 16, 18, 20].

We would like to thank the anonymous referees for many helpful comments.

[*]Supported by the SNSF grant 200020_153169 *Structural Proof Theory and the Logic of Proofs*

Given the interpretation of LP in Peano Arithmetic, it was a natural question to find an intuitionistic version iLP of LP that is the logic of proofs of Heyting Arithmetic. The work by Artemov and Iemhoff [7] and later by Dashkov [13] provides such an iLP. It turned out that iLP is not only LP with the underlying logic changed to intuitionistic propositional logic. In order to get a complete axiomatization with respect to provability semantics, one also has to include certain admissible rules of Heyting Arithmetic as axioms in iLP so that they are represented by novel proof terms.

The main question of this paper is *what is the justification counterpart of intuitionistic* S4. We find that the additional axioms of iLP are not needed if we are interested in completeness with respect to possible world models. We study the intuitionistic justification logic iJT4, which is simply LP over an intuitionistic base instead of a classical one but without any additional axioms. We introduce modular models for iJT4 that are inspired by the Kripke-style semantics for intuitionistic S4 and establish completeness of iJT4 with respect to these models.

Artemov [3] already considerend iJT4, under the name $\mathcal{ILP}$, to provide a provability interpretation of modal λ-terms. In order to achieve this, he established that there is a realization of iS4 into iJT4. We will restate that result as it shows that the justification logic iJT4 indeed is the explicit version of the intuitionistic modal logic iS4.

2 Intuitionistic Modal Logic

We present the intuitionistic modal logic iS4. We will start with introducing the language $\mathcal{L}_\mathsf{I}$ of iS4. For our purpose, we will only consider the $\Box$-modality but not the $\Diamond$-modality.

Definition 2.1 (Intuitionistic modal language)**.** We assume a countable set Prop of atomic propositions. The set of formulas $\mathcal{L}_\mathsf{I}$ is inductively defined by:

1. every atomic proposition is a formula;
2. the constant symbol $\bot$ is a formula;
3. If A and B are formulas, then $(A \wedge B)$, $(A \vee B)$ and $(A \to B)$ are formulas;
4. if A is a formula, then $\Box A$ is a formula.

There are various semantics available for intuitionistic modal logic. The intuitionistic Kripke models that we introduce in this section are the same as Ono's [22] I-models of type 0. Moreover, these models are equivalent to the models used by

Fischer Servi [14], Plotkin and Stirling [23], and Simpson [24]. Jäger and Marti [17] provide a detailed discussion and comparison of these different approaches.

The semantics for $\mathsf{iS4}$ is given by Kripke models that use two accessibility relations: $\leq$ to model the intuitionistic base logic and R to interpret the $\Box$-modality.

Definition 2.2. An *intuitionistic Kripke model* for $\mathsf{iS4}$ is a tuple

$$\mathfrak{M} = (W, \leq, R, V)$$

such that

(i) $W \neq \varnothing$

(ii) R is a reflexive and transitive binary relation on W

(iii) $\leq$ is a partial order (reflexive and transitive) on W

(iv) $V : \mathsf{Prop} \to \mathcal{P}(W)$, and for any atomic proposition p, the set $V(p)$ is upwards closed, i.e., : $w \leq v, w \in V(p) \implies v \in V(p)$

(v) $w \leq v \implies R[v] \subseteq R[w]$

where $R[v] := \{w \in W \mid (v, w) \in R\}$.

Usually, the definition of intuitionistic Kripke models does not include Condition (ii). Since we exclusively work with Kripke models for intuitionistic $\mathsf{S4}$, we make it part of our definition in order to have a simpler terminology.

Definition 2.3 (Satisfaction in Kripke models)**.** We define the *satisfaction relation* $(\mathfrak{M}, w) \vDash A$ by induction on the $\mathcal{L}_{\mathsf{I}}$-formula A.

- $(\mathfrak{M}, w) \nvDash \bot$;
- $(\mathfrak{M}, w) \vDash p$ iff $w \in V(p)$;
- $(\mathfrak{M}, w) \vDash A \wedge B$ iff $(\mathfrak{M}, w) \vDash A$ and $(\mathfrak{M}, w) \vDash B$;
- $(\mathfrak{M}, w) \vDash A \vee B$ iff $(\mathfrak{M}, w) \vDash A$ or $(\mathfrak{M}, w) \vDash B$;
- $(\mathfrak{M}, w) \vDash A \to B$ iff $(\mathfrak{M}, v) \vDash B$ for all $v \geq w$ with $(\mathfrak{M}, v) \vDash A$;
- $(\mathfrak{M}, w) \vDash \Box A$ iff $(\mathfrak{M}, v) \vDash A$ for all $v \in R[w]$.

An $\mathcal{L}_{\mathsf{I}}$-formula A is *valid with respect to Kripke models* if for all Kripke models $\mathfrak{M} = (W, \leq, R, V)$ and all $w \in W$ we have $(\mathfrak{M}, w) \vDash A$.

Intuitionistic modal logic has the following monotonicity property.

Lemma 2.4 (Monotonicity).

$$(\mathfrak{M}, w) \vDash A \text{ and } w \leq v \quad \Longrightarrow \quad (\mathfrak{M}, v) \vDash A.$$

We will need two different deductive systems for $\mathsf{iS4}$. The system $\mathsf{HiS4}$ is a Hilbert-style calculus whereas the system $\mathsf{GiS4}$ is a Gentzen-style sequent calculus for the intuitionistic modal logic $\mathsf{iS4}$.

Definition 2.5 (The proof system $\mathsf{HiS4}$). The system $\mathsf{HiS4}$ consists of the following axioms:

- All axioms for intuitionistic propositional logic
- $\Box(A \to B) \to (\Box A \to \Box B) \quad$ (K)
- $\Box A \to A \quad$ (T)
- $\Box A \to \Box\Box A$ (4)

The rules of $\mathsf{HiS4}$ are modus ponens and necessitation:

$$\frac{A \to B \qquad A}{B}\,(\mathrm{MP}) \qquad \frac{A}{\Box A}\,(\mathrm{nec})$$

Theorem 2.6. $\mathsf{HiS4}$ is sound and complete with respect to intuitionistic Kripke models.

Proof. Soundness and completeness follow from [22, Theorem 3.2 on p. 696] and the observation that that Ono's I-models of type 0 are the same as our intuitionistic Kripke models. $\Box$

Definition 2.7 (The proof system $\mathsf{GiS4}$). A *sequent* is an expression of the form $\Gamma \supset A$, where Γ is a finite multiset of formulas and A is a formula. The Gentzen-style system $\mathsf{GiS4}$ derives sequents and consists of the following axioms and rules:

$$\Gamma \supset A \quad \text{if } A \in \Gamma \text{ or } \bot \in \Gamma$$

$$\frac{\Gamma, A \supset C \qquad \Gamma, B \supset C}{\Gamma, A \vee B \supset C}\,(\vee \supset)$$

$$\frac{\Gamma \supset A}{\Gamma \supset A \vee B}\,(\supset \vee)_1 \qquad \frac{\Gamma \supset B}{\Gamma \supset A \vee B}\,(\supset \vee)_2$$

$$\frac{\Gamma, A, B \supset C}{\Gamma, A \wedge B \supset C}\,(\wedge \supset) \qquad \frac{\Gamma \supset A \qquad \Gamma \supset B}{\Gamma \supset A \wedge B}\,(\supset \wedge)$$

$$\frac{\Gamma \supset A \qquad \Gamma, B \supset C}{\Gamma, A \to B \supset C}\,(\to\supset) \qquad \frac{\Gamma, A \supset B}{\Gamma \supset A \to B}\,(\supset\to)$$

$$\frac{A, \Gamma \supset B}{\Box A, \Gamma \supset B}\,(\Box \supset) \qquad \frac{\Box\Gamma \supset A}{\Box\Gamma \supset \Box A}\,(\supset \Box)$$

$$\frac{\Gamma \supset A}{\Gamma, \Delta \supset A}\,(\text{weakening}) \qquad \frac{\Gamma, A, A \supset B}{\Gamma, A \supset B}\,(\text{contraction})$$

In the rule $(\supset \Box)$, the expression $\Box\Gamma$ denotes the multiset $\{\Box A \mid A \in \Gamma\}$. As usual, we say that a formula A is provable in $\mathsf{GiS4}$, in symbols $\vdash_{\mathsf{GiS4}} A$, if the sequent $\supset A$ is provable.

Theorem 2.8. $\mathsf{GiS4}$ is sound and complete with respect to intuitionistic Kripke models.

Proof. In this proof, theorems and systems refer to [22]. By Theorem 3.2 the Hilbert system L_0 is complete with respect to I-models of type 0, which are the same as our intuitionistic Kripke models. By Theorem 2.1, the sequent system G_0 is equivalent to the Hilbert system L_0. The sequent systems G_0 and K_0 are equivalent, and by Theorem 3.3, we have cut-elimination for K_0. Therefore, the cut-free version of K_0 is complete with respect to intuitionistic Kripke models. Finally observe that cut-free K_0 is the same as our $\mathsf{GiS4}$. □

3 Intuitionistic Justification Logic

In this section, we introduce the syntax for the justification logic $\mathsf{iJT4_{CS}}$, which is the explicit analogue of the intuitionistic modal logic $\mathsf{iS4}$.

Definition 3.1 (Justification terms)**.** We assume a countable set of justification constants and a countable set of justification variables. The set of justification terms Tm is inductively defined by:

1. each justification constant and each justification variable is a justification term;
2. if s and t are justification terms, then so are

- $(s \cdot t)$, read s dot t,
- $(s + t)$, read s plus t,
- $!s$, read bang s.

Definition 3.2 (Formulas)**.** We start with the same set Prop of atomic propositions as in $\mathcal{L}_\mathsf{I}$. The set of formulas $\mathcal{L}_\mathsf{J}$ is inductively defined by:

1. every atomic proposition is a formula;
2. the constant symbol $\bot$ is a formula;
3. If A and B are formulas, then $(A \wedge B)$, $(A \vee B)$ and $(A \to B)$ are formulas;
4. if A is a formula and t a term, then $t : A$ is a formula.

Definition 3.3. The axioms of $\mathsf{iJT4}$ consist of the following axioms:

1. all axioms for intuitionistic propositional logic
2. $t : (A \to B) \to (s : A \to t \cdot s : B)$
3. $t : A \to t + s : A$ and $s : A \to t + s : A$
4. $t : A \to A$
5. $t : A \to\, !t : t : A$

A *constant specification* CS is any subset

$$\mathsf{CS} \subseteq \{(c, A) \mid c \text{ is a constant and } A \text{ is an axiom of } \mathsf{iJT4}\}.$$

A constant specification CS is called:

- *axiomatically appropriate* if for each axiom A of $\mathsf{iJT4}$, there is a constant c such that $(c, A) \in \mathsf{CS}$.
- *schematic* if for each constant c, the set of axioms $\{A \mid (c, A) \in \mathsf{CS}\}$ consists of all instances of several (possibly zero) axiom schemes of $\mathsf{iJT4}$.

For a constant specification CS the deductive system $\mathsf{iJT4}_\mathsf{CS}$ is the Hilbert system given by the axioms above and by the rules modus ponens and axiom necessitation:

$$\frac{A \to B \qquad A}{B}\,(\mathrm{MP}) \qquad\qquad \frac{(c, A) \in \mathsf{CS}}{c : A}\,(\mathrm{AN})$$

Remark 3.4. Although axiom necessitation is a rule without premises, it is important to consider it as a rule and not as an axiom schema. If we said that $c : A$ is an axiom for each $(c, A) \in \mathsf{CS}$, then the notion of an axiom would depend on the constant specification, which in turn would depend on the notion of an axiom. Since we want to avoid this circularity, axiom necessitation is introduced as a rule.

Remark 3.5. Let Tot be the total constant specification, i.e.

$$\mathsf{Tot} := \{(c, A) \mid c \text{ is a constant and } A \text{ is an axiom of } \mathsf{iJT4}\}.$$

Artemov's [3] intuitionistic logic of proofs $\mathcal{ILP}$ is then the same as our $\mathsf{iJT4}_{\mathsf{Tot}}$.

As usual in justification logic, we can establish the Deduction Theorem and the Lifting Lemma.

Theorem 3.6 (Deduction Theorem)**.** For every set of formulas M and all formulas A, B we have that

$$M \cup \{A\} \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} B \quad \Longleftrightarrow \quad M \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} A \to B.$$

Lemma 3.7 (Lifting Lemma)**.** Let CS be an axiomatically appropriate constant specification. For arbitrary formulas $A, B_1, \dots, B_m, C_1, \dots, C_n$ and arbitrary justification terms $r_1, \dots, r_m, s_1, \dots, s_n$, if

$$r_1 : B_1, \dots, r_m : B_m, C_1, \dots, C_n \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} A,$$

then there is a justification term t such that

$$r_1 : B_1, \dots, r_m : B_m, s_1 : C_1, \dots, s_n : C_n \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} t : A.$$

Definition 3.8 (Substitution)**.** A *substitution* is a mapping from justification variables to justification terms. Given a substitution σ and an $\mathcal{L}_{\mathsf{J}}$-formula A, the formula $A\sigma$ is obtained from A by simultaneously replacing all occurrences of x with $\sigma(x)$ in A for all justification variables x.

As usual in justification logic, we have the following substitution property for schematic constant specifications.

Lemma 3.9 (Substitution Property)**.** Let CS be a schematic constant specification. We have for any $\mathcal{L}_{\mathsf{J}}$-formula A and any substitution σ

$$B_1, \dots, B_n \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} A \quad \text{implies} \quad B_1\sigma, \dots, B_n\sigma \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} A\sigma.$$

We find that $\mathsf{iJT4}_{\mathsf{CS}}$ is a conservative extension of intuitionistic propositional logic. Hence $\mathsf{iJT4}_{\mathsf{CS}}$ is consistent.

Lemma 3.10 (Conservativity)**.** $\mathsf{iJT4_{CS}}$ is a conservative extension of intuitionistic propositional logic Int, i.e., for any formula A of intuitionistic propositional logic,

$$\vdash_{\mathsf{iJT4_{CS}}} A \quad \text{iff} \quad \vdash_{\mathsf{Int}} A.$$

Proof. The implication from right to left is trivial. For the other direction consider the mapping $(\cdot)^s$ from $\mathcal{L}_\mathsf{J}$ to formulas of intuitionistic propositional logic given by:

$$\begin{aligned} \bot^s &:= \bot & p^s &:= p \\ (A \wedge B)^s &:= A^s \wedge B^s & (A \vee B)^s &:= A^s \vee B^s \\ (A \to B)^s &:= A^s \to B^s & (t : B)^s &:= B^s \end{aligned}$$

For any formula C of $\mathcal{L}_\mathsf{J}$, we can show

$$\vdash_{\mathsf{iJT4_{CS}}} C \quad \text{implies} \quad \vdash_{\mathsf{Int}} C^s$$

by induction on the length of the $\mathsf{iJT4_{CS}}$-derivation. Thus the claim immediately follows from $A^s = A$. $\square$

Lemma 3.11 (Consistency of $\mathsf{iJT4_{CS}}$)**.** For any constant specification CS, the logic $\mathsf{iJT4_{CS}}$ is consistent.

Proof. Assume towards a contradiction that $\mathsf{iJT4_{CS}}$ were not consistent, that means $\vdash_{\mathsf{iJT4_{CS}}} \bot$. By the conservativity of $\mathsf{iJT4_{CS}}$ over propositional intuitionistic logic Int (previous lemma), it would then follow that $\vdash_{\mathsf{Int}} \bot$, which is not the case. $\square$

4 Basic Modular Models

Basic modular models are syntactic models for justification logic. Yet, our basic modular models will include possible worlds in order to deal with the intuitionistic base logic. After defining basic modular models for intuitionistic justification logic, we will prove soundness and completeness.

In this and the next section, derivability always refers to derivability in $\mathsf{iJT4_{CS}}$. Accordingly we use $\vdash$ to mean $\vdash_{\mathsf{iJT4_{CS}}}$.

For two sets of formulas S, T and a term s we write

$$\begin{aligned} &S \cdot T := \{F \mid G \to F \in S \text{ and } G \in T \text{ for some formula } G\} \\ &s : S := \{s : F \mid F \in S\} \end{aligned}$$

Definition 4.1 (Basic evaluation)**.** A *basic evaluation* is a tuple $(W, \leq, *)$ where

$$W \neq \varnothing \text{ and } \leq \text{ is a partial order on } W,$$

$$* : \mathsf{Prop} \times W \to \{0, 1\} \qquad * : \mathsf{Tm} \times W \to \mathcal{P}(\mathcal{L}_\mathsf{J})$$

(where we often write t^*_w for $*(t, w)$ and p^*_w for $*(p, w)$), such that for arbitrary $s, t \in \mathsf{Tm}$, any formula A, and every $w \in W$,

(1) $s^*_w \cdot t^*_w \subseteq (s \cdot t)^*_w$;

(2) $s^*_w \cup t^*_w \subseteq (s + t)^*_w$;

(3) $(t, A) \in \mathsf{CS} \implies A \in t^*_w$;

(4) $s : s^*_w \subseteq (!s)^*_w$.

Furthermore, it has to satisfy the following monotonicity conditions:

(M1) $p^*_w = 1$ and $w \leq v \implies p^*_v = 1$;

(M2) $w \leq v \implies t^*_w \subseteq t^*_v$.

Strictly speaking we should use the notion of a CS basic evaluation because condition (3) depends on a given CS. However, the constant specification will always be clear from the context and we can safely omit it. The same also holds for modular models (to be introduced later).

Definition 4.2 (Truth under basic evaluation)**.** Let $\mathfrak{M} = (W, \leq, *)$ be a basic evaluation. For $w \in W$, we define $(\mathfrak{M}, w) \vDash A$ by induction on the formula A as follows:

- $(\mathfrak{M}, w) \nvDash \bot$;
- $(\mathfrak{M}, w) \vDash p$ iff $p^*_w = 1$;
- $(\mathfrak{M}, w) \vDash A \wedge B$ iff $(\mathfrak{M}, w) \vDash A$ and $(\mathfrak{M}, w) \vDash B$;
- $(\mathfrak{M}, w) \vDash A \vee B$ iff $(\mathfrak{M}, w) \vDash A$ or $(\mathfrak{M}, w) \vDash B$;
- $(\mathfrak{M}, w) \vDash A \to B$ iff $(\mathfrak{M}, v) \vDash B$ for all $v \geq w$ with $(\mathfrak{M}, v) \vDash A$;
- $(\mathfrak{M}, w) \vDash t : A$ iff $A \in t^*_w$.

We immediately obtain the monotonicity property for intuitionistic justification logic.

Lemma 4.3 (Monotonicity)**.** For any basic evaluation $\mathfrak{M} = (W, \leq, *)$, any $w, v \in W$, and any formula A:

$$(\mathfrak{M}, w) \vDash A \text{ and } w \leq v \quad \Longrightarrow \quad (\mathfrak{M}, v) \vDash A.$$

Definition 4.4 (Factive evaluation)**.** A basic evaluation $\mathfrak{M} = (W, \leq, *)$ is called *factive* iff

$$A \in t^*_w \quad \Longrightarrow \quad (\mathfrak{M}, w) \vDash A$$

for all formulas A, all justification terms t and all states $w \in W$.

Definition 4.5 (Basic modular model)**.** A *basic modular model* is a basic evaluation $(W, \leq, *)$ that is factive.

We say that a formula A is *valid with respect to basic modular models* if for all basic modular models $\mathfrak{M} = (W, \leq, *)$ and all $w \in W$ we have $(\mathfrak{M}, w) \vDash A$.

Lemma 4.6 (Soundness of $\mathsf{iJT4_{CS}}$ with respect to basic modular models)**.** For every formula A:

$$\vdash A \quad \text{implies} \quad A \text{ is valid with respect to basic modular models.}$$

In order to show completeness, we need some auxiliary definitions and lemmas.

Definition 4.7. We call a set of formulas Δ *prime* iff it satisfies the following conditions:

(i) Δ has the disjunction property, i.e., $A \vee B \in \Delta \Longrightarrow A \in \Delta$ or $B \in \Delta$;

(ii) Δ is deductively closed, i.e., for any formula A, if $\Delta \vdash A$, then $A \in \Delta$;

(iii) Δ is consistent, i.e., $\bot \notin \Delta$.

From now on, we will use Σ, Δ, Γ for prime sets of formulas.

Lemma 4.8. Let N be an arbitrary set of formulas and let A, B and C be formulas. If

$$N \cup \{A \vee B\} \nvdash C, \text{ then } N \cup \{A\} \nvdash C \text{ or } N \cup \{B\} \nvdash C.$$

Proof. By contraposition. Assume that

$$N \cup \{A\} \vdash C \text{ and } N \cup \{B\} \vdash C$$

Then there are finite subsets $N_1 \subseteq N \cup \{A\}$ and $N_2 \subseteq N \cup \{B\}$ such that

$$N_1 \vdash C \text{ and } N_2 \vdash C$$

Now let $N_1' := N_1 \setminus \{A\}$ and $N_2' := N_2 \setminus \{B\}$. Then N_1', N_2' are finite subsets of N, and

$$(N_1' \cup \{A\}) \vdash C \text{ and } (N_2' \cup \{B\}) \vdash C$$

So by the Deduction Theorem,

$$N_1' \vdash A \to C \text{ and } N_2' \vdash B \to C$$

So

$$N_1' \vdash (A \to C) \text{ and } N_2' \vdash (B \to C).$$

Strengthening the antecedent, we get

$$(N_1' \cup N_2') \vdash (A \to C) \text{ and } (N_1' \cup N_2') \vdash (B \to C)$$

and, therefore,

$$(N_1' \cup N_2') \vdash ((A \to C) \wedge (B \to C)).$$

By propositional reasoning we get

$$(N_1' \cup N_2') \vdash ((A \vee B) \to C),$$

By the Deduction Theorem it follows that

$$(N_1' \cup N_2' \cup \{A \vee B\}) \vdash C.$$

Since N_1' and N_2' are finite subsets of N, $N_1' \cup N_2' \cup \{A \vee B\}$ is a finite subset of $N \cup \{A \vee B\}$, so by definition

$$N \cup \{A \vee B\} \vdash C. \qquad \square$$

Theorem 4.9 (Prime Lemma)**.** Let B be a formula and let N be a set of formulas such that $N \nvdash B$. Then there exists a prime set Π with $N \subseteq \Pi$ and $\Pi \nvdash B$.

Proof. Let $(A_n)_{n\in\mathbb{N}}$ be an enumeration of all formulas.

Now we define $N_0 := N$,

$$N_{i+1} := \begin{cases} N_i \cup \{A_i\}, & \text{if } N_i \cup \{A_i\} \nvdash B \\ N_i, & \text{otherwise} \end{cases}$$

and finally

$$N^\star := \bigcup_{i\in\mathbb{N}} N_i$$

By induction in i, one can easily show that for all $i \in \mathbb{N} : N_i \nvdash B$ and, therefore, $N^\star \nvdash B$.

It remains to show that $N^\star$ is prime. We have the following:

- $\bot \notin N^\star$: We have $N^\star \nvdash B$, hence $\bot \notin N^\star$.
- $N^\star$ is deductively closed: Assume it is not, i.e., there is a formula A with

  $$N^\star \vdash A \text{ but } A \notin N^\star$$

  Since $N^\star \vdash A$ but $N^\star \nvdash B$, we know that

  $$N^\star \cup \{A\} \nvdash B$$

  Otherwise, by the Deduction Theorem 3.6

  $$N^\star \vdash A \to B \text{ and } N^\star \vdash A$$

  so by propositional reasoning,

  $$N^\star \vdash B, \text{ which contradicts our observation above.}$$

  Since $(A_n)_{n\in\mathbb{N}}$ is an enumeration of all formulas, there is some i such that $A = A_i$. But then

  $$N_i \cup \{A_i\} \nvdash B.$$

  So by construction

  $$N_{i+1} = N_i \cup \{A_i\}$$

  and, therefore,

  $$A = A_i \in N_{i+1} \subseteq N^\star,$$

  which contradicts our assumption.
- $N^\star$ has the disjunction property: Assume that $C \vee D \in N^\star$. Then there is some i such that $C \vee D = A_i$ and there are i_1, i_2 such that

  $$C = A_{i_1} \text{ and } D = A_{i_2}$$

  Now we have

  $$N^\star = N^\star \cup \{C \vee D\} \nvdash B$$

  By the lemma above it follows that

  $$N^\star \cup \{C\} \nvdash B \text{ or } N^\star \cup \{D\} \nvdash B$$

In the first case, we have that

$$N_{i_1} \cup \{A_{i_1}\} \nvdash B$$

so by the definition of N_{i_1+1},

$$N_{i_1+1} = N_{i_1} \cup \{A_{i_1}\} = N_{i_1} \cup \{C\}$$

which means that $C \in N_{i_1+1}$ and therefore $C \in N^\star$. The second case is analogous. $\square$

Lemma 4.10. Let Δ be a prime set and t be a justification term. Then

$$t^{-1}\Delta := \{A \mid t : A \in \Delta\} \subseteq \Delta.$$

Proof. Let $A \in t^{-1}\Delta$. Then $t : A \in \Delta$. Since Δ is deductively closed, it contains all axioms, thus $t : A \to A \in \Delta$. Again, since Δ is deductively closed, it follows by (MP) that $A \in \Delta$. $\square$

Definition 4.11 (Canonical basic modular model)**.** The canonical basic modular model is

$$B^{can} := (W^{can}, \leq^{can}, *^{can})$$

where

(i) $W^{can} \quad := \quad \{\Delta \subseteq \mathcal{L}_{\mathsf{J}} \mid \Delta \text{ is prime}\}$

(ii) $\leq^{can} \quad := \quad \subseteq$

(iii) $*^{can}(p, \Delta) = 1$ iff $p \in \Delta$

(iv) $*^{can}(t, \Delta) := t^{-1}\Delta$

Lemma 4.12. B^{can} is a basic evaluation.

Proof. $W \neq \varnothing$: By the consistency of $\mathsf{iJT4_{CS}}$ we have that $\varnothing \nvdash \bot$, it follows by the Prime Lemma 4.9 that there exists a prime set, so $W^{can} \neq \varnothing$.

Next, we check the conditions on the sets of formulas $t^{*^{can}}_{\Delta}$.

(1) $s^{*^{can}}_{\Delta} \cdot t^{*^{can}}_{\Delta} \subseteq (s \cdot t)^{*^{can}}_{\Delta}$. Let $A \in s^{*^{can}}_{\Delta} \cdot t^{*^{can}}_{\Delta}$. Then there is a formula $B \in t^{*^{can}}_{\Delta}$ such that $B \to A \in s^{*^{can}}_{\Delta}$. So $s : B \to A \in \Delta$ and $t : B \in \Delta$. Since Δ is a prime set, it is deductively closed, so it contains the axiom

$$s : (B \to A) \to (t : B \to s \cdot t : A).$$

Again since Δ is deductively closed, it follows by (MP) that $s \cdot t : A \in \Delta$, so $A \in (s \cdot t)^{-1}\Delta = (s \cdot t)^{*^{can}}_{\Delta}$.

(2) $s_\Delta^{*^{can}} \cup t_\Delta^{*^{can}} \subseteq (s+t)_\Delta^{*^{can}}$. Let $A \in s_\Delta^{*^{can}} \cup t_\Delta^{*^{can}}$. Case 1: $A \in s_\Delta^{*^{can}} = s^{-1}\Delta$. Then $s : A \in \Delta$. Since Δ is deductively closed, it contains the axiom

$$s : A \to (s+t) : A.$$

Thus by (MP) we find $(s+t) : A \in \Delta$, i.e., $A \in (s+t)^{-1}\Delta = (s+t)_\Delta^{*^{can}}$. The second case is analogous.

(3) $(t, A) \in \mathsf{CS} \implies A \in t_\Delta^{*^{can}}$. By axiom necessitation we find that $\vdash t : A$, so $\Delta \vdash t : A$. Since Δ is deductively closed, it follows that $t : A \in \Delta$, so $A \in t^{-1}\Delta = t_\Delta^{*^{can}}$.

(4) $s : s_\Delta^{*^{can}} \subseteq (!s)_\Delta^{*^{can}}$. Let $A \in s : s_\Delta^{*^{can}}$. Then A is of the form $s : B$ for some formula $B \in s_\Delta^{*^{can}} = s^{-1}\Delta$, i.e., $s : B \in \Delta$. We find that the axiom $(s : B) \to\ !s : (s : B) \in \Delta$, so $!s : (s : B) \in \Delta$, which means $s : B \in (!s)^{-1}\Delta = (!s)_\Delta^{*^{can}}$.

Now we check the monotonicity conditions.

(M1) Assume that $p_\Gamma^{*^{can}} = 1$ and $\Gamma \subseteq \Delta$. By the definition of $*^{can}$ we have that $p \in \Gamma$, so $p \in \Delta$ hence $p_\Delta^{*^{can}} = 1$.

(M2) Now assume that $\Gamma \subseteq \Delta$. Then $t^{-1}\Gamma \subseteq t^{-1}\Delta$, which is $t_\Gamma^{*^{can}} \subseteq t_\Delta^{*^{can}}$. □

Lemma 4.13 (Truth Lemma)**.** For any formula A and any prime set Δ :

$$A \in \Delta \iff (\mathcal{B}^{can}, \Delta) \vDash A.$$

Proof. By induction on the formula A. We distinguish the following cases.

1. $A = p$ or $A = \bot$. By definition.

2. $A = B \wedge C$. Assume that $B \wedge C \in \Delta$. Since Δ is deductively closed, we have $B \in \Delta$ and $C \in \Delta$, so it follows by the induction hypothesis that $(\mathcal{B}^{can}, \Delta) \vDash B$ and $(\mathcal{B}^{can}, \Delta) \vDash C$.

   For the other direction assume that $(\mathcal{B}^{can}, \Delta) \vDash B \wedge C$, so $(\mathcal{B}^{can}, \Delta) \vDash B$ and $(\mathcal{B}^{can}, \Delta) \vDash C$. By the induction hypothesis, we get that $B \in \Delta$ and $C \in \Delta$. Since Δ is deductively closed, it follows that $B \wedge C \in \Delta$.

3. $A = B \vee C$. Assume that $B \vee C \in \Delta$. Since Δ has the disjunction property, it follows that $B \in \Delta$ or $C \in \Delta$, so by the induction hypothesis, $(\mathcal{B}^{can}, \Delta) \vDash B$ or $(\mathcal{B}^{can}, \Delta) \vDash C$, so $(\mathcal{B}^{can}, \Delta) \vDash B \vee C$.

For the other direction assume that $(B^{can}, \Delta) \vDash B \vee C$. Then

$$(B^{can}, \Delta) \vDash B \text{ or } (B^{can}, \Delta) \vDash C,$$

so by the induction hypothesis, $B \in \Delta$ or $C \in \Delta$. Since Δ is deductively closed, it follows that $B \vee C \in \Delta$.

4. $A = B \to C$. Assume that $B \to C \in \Delta$. We have to show $(B^{can}, \Delta) \vDash B \to C$, so let Γ be a prime set such that $\Delta \subseteq \Gamma$ and $(B^{can}, \Gamma) \vDash B$. It follows by the induction hypothesis that $B \in \Gamma$, and since $B \to C \in \Gamma$ and Γ is deductively closed, we have that $C \in \Gamma$. Applying the induction hypothesis again, we get that $(B^{can}, \Gamma) \vDash C$.

   For the other direction assume that $(B^{can}, \Delta) \vDash B \to C$. We have to show that $B \to C \in \Delta$. Assume for a contradiction that $B \to C \notin \Delta$. Since Δ is deductively closed, it follows that $\Delta \nvdash B \to C$. It follows by the Deduction Theorem 3.6 that $\Delta \cup \{B\} \nvdash C$. By the Prime Lemma 4.9, there is a prime set Γ such that $\Delta \cup \{B\} \subseteq \Gamma$ and $\Gamma \nvdash C$, so in particular, $C \notin \Gamma$. By the induction hypothesis it follows that $(B^{can}, \Gamma) \vDash B$ and $(B^{can}, \Gamma) \nvDash C$, contradicting our assumption that $(B^{can}, \Delta) \vDash B \to C$.

5. $A = t : B$. We have

$$t : B \in \Delta \quad \Longleftrightarrow \quad B \in t^{-1}\Delta = *^{can}(t, \Delta) \quad \Longleftrightarrow \quad (B^{can}, \Delta) \vDash t : B.$$

□

Lemma 4.14. B^{can} is a basic modular model.

Proof. We only have to show factivity, for which we use the Truth Lemma. Assume that

$$A \in *^{can}(t, \Delta) = t^{-1}\Delta.$$

By Lemma 4.10 we know that $t^{-1}\Delta \subseteq \Delta$, so we have $A \in \Delta$. By the Truth Lemma for the canonical basic modular model, we can conclude that $(B^{can}, \Delta) \vDash A$. So factivity is shown. □

Theorem 4.15 (Completeness of $\mathsf{iJT4_{CS}}$ with respect to basic modular models)**.** For any formula A:

$$A \text{ is valid with respect to basic modular models} \quad \text{implies} \quad \vdash A.$$

Proof. By contraposition. Assume that $\nvdash A$. By the Prime Lemma 4.9, there exists a prime set Δ such that $\Delta \nvdash A$. In particular, $A \notin \Delta$. By the Truth Lemma 4.13, it follows that

$$(B^{can}, \Delta) \nvDash A$$

since this structure is a basic modular model, it follows that A is not valid with respect to basic modular models. □

5 Modular Models

In this section, we introduce modular models for intuitionistic justification logic. Modular models are epistemic models in the sense that they feature possible worlds to model the notion of knowledge. The main principle of these logics is called *justification yields belief*, which means that if there is a justification for a formula A, then that formula must hold in all accessible worlds.

Modular models may seem too expressive as our language does not include a $\Box$-operator. However, these models explain the connection between implicit and explicit notions of belief. The main feature of modular models is that they provide a clear ontological separation of justification and truth, see, e.g., [6, 19].

In the second part of this section, we study so-called *fully explanatory* modular models. These models additionally require that if a formula holds in all accessible worlds, then there must be a justification for that formula. This principle can be seen as the reverse direction of justification yields belief.

Definition 5.1 (Quasimodels)**.** A *quasimodel* is a tuple

$$\mathfrak{M} = (W, \leq, R, *),$$

such that $(W, \leq, *)$ is a basic evaluation, and R is a binary relation on W.

Definition 5.2 (Truth in quasimodels)**.** We define what it means for a formula A to hold at a world $w \in W$ of a quasimodel $\mathfrak{M} = (W, \leq R, *)$, written $(\mathfrak{M}, w) \vDash A$, inductively as follows:

- $(\mathfrak{M}, w) \nvDash \bot$;
- $(\mathfrak{M}, w) \vDash p$ iff $p^*_w = 1$;
- $(\mathfrak{M}, w) \vDash A \wedge B$ iff $(\mathfrak{M}, w) \vDash A$ and $(\mathfrak{M}, w) \vDash B$;
- $(\mathfrak{M}, w) \vDash A \vee B$ iff $(\mathfrak{M}, w) \vDash A$ or $(\mathfrak{M}, w) \vDash B$;

- $(\mathfrak{M}, w) \vDash A \to B$ iff $(\mathfrak{M}, v) \vDash B$ for all $v \geq w$ with $(\mathfrak{M}, v) \vDash A$;
- $(\mathfrak{M}, w) \vDash t : A$ iff $A \in t^*_w$.

Further we define $\Box_w := \{A \in \mathcal{L}_\mathsf{J} \mid (\mathfrak{M}, v) \vDash A$ for all $v \in R[w]\}$.

Lemma 5.3 (Locality of truth in quasimodels)**.** Let $\mathfrak{B} = (W, \leq, *)$ be a basic evaluation and $\mathfrak{M} = (W, \leq, R, *)$ be a quasimodel. We find that for each $w \in W$ and each formula A,

$$(\mathfrak{M}, w) \vDash A \quad \Longleftrightarrow \quad (\mathfrak{B}, w) \vDash A.$$

Definition 5.4 (Factive quasimodel)**.** A quasimodel $\mathfrak{M} = (W, \leq, R, *)$ is called *factive* if $A \in t^*_w$ implies $(\mathfrak{M}, w) \vDash A$ for all $w \in W, t \in \mathsf{Tm}$, and formulas A.

Definition 5.5 (Modular models)**.** A quasimodel $\mathfrak{M} = (W, \leq\ R, *)$ is called a *modular model* if it meets the following conditions:

(1) $t^*_w \subseteq \Box_w$ for all $t \in \mathsf{Tm}$ and $w \in W$ (JYB);

(2) R is reflexive;

(3) R is transitive;

(4) $w \leq v \implies R[v] \subseteq R[w]$ (Compatibility of $\leq$ with R).

We say that a formula A is *valid with respect to modular models* if for each modular model $\mathfrak{M} = (W, \leq, *)$ and all $w \in W$ we have $(\mathfrak{M}, w) \vDash A$.

The abbreviation JYB stands for *justification yields belief*, which is the main principle of modular models. This notion goes back to Artemov [6].

Lemma 5.6 (Modular models are factive)**.** All modular models are factive.

Proof. Whenever $A \in t^*_w$ for some formula A, some $t \in \mathsf{Tm}$, and some $w \in W$, we have $A \in \Box_w$ by JYB. Since $R(w, w)$ by the reflexivity of R, we obtain $(\mathfrak{M}, w) \vDash A$ from the definition of $\Box_w$. □

Corollary 5.7 (Factivity of basic evaluations used in modular models)**.** For any modular model $\mathfrak{M} = (W, \leq, R, *)$ we have that the basic evaluation $\mathfrak{B} := (W, \leq, *)$ is factive and, hence, a basic modular model.

Proof. Assume that for the basic evaluation $(W, \leq, *)$, we have $A \in t^*_w$ for some formula A, some point $w \in W$ and some term $t \in \mathsf{Tm}$. Then $A \in t^*_w$ in the modular model notation. By the previous lemma, we get $(\mathfrak{M}, w) \vDash A$, from which we conclude $(\mathfrak{B}, w) \vDash A$ by Lemma 5.3. □

Lemma 5.8 (Justifications remain relevant)**.** Let $\mathfrak{M} = (W, \leq, R, *)$ be a modular model. Then for any $t \in \mathsf{Tm}$ and for arbitrary $w, v \in W$, if $R(w, v)$, then $t^*_w \subseteq t^*_v$, i.e., justifications remain relevant in accessible worlds.

Proof. Assume $R(w, v)$ and $A \in t^*_w$ for some formula A. Then we have $t : A \in (!t)^*_w$ because $(W, \leq, *)$ is a basic evaluation. Therefore, $t : A \in \Box_w$ by JYB and, in particular, $(\mathfrak{M}, v) \vDash t : A$ by the definition of $\Box_w$, which means that $A \in t^*_v$. $\Box$

Theorem 5.9 (Soundness and completeness: modular models)**.** For any constant specification CS and any formula A we have

$$\vdash A \quad\Longleftrightarrow\quad \text{A is valid with respect to modular models.}$$

Proof. Soundness. Let $\mathfrak{M} = (W, \leq, R, *)$ be a modular model. We need to show that any formula A such that $\vdash A$ holds at any world $w \in W$. By Corollary 5.7, we know that $\mathfrak{B} := (W, \leq, *)$ is a basic modular model. By soundness of $\mathsf{iJT4_{CS}}$ with respect to basic modular models, we get $(\mathfrak{B}, w) \vDash A$. Hence, $(\mathfrak{M}, w) \vDash A$ by the locality of truth in quasimodels (Lemma 5.3).

Completeness. For the opposite direction, suppose $\nvdash A$. By completeness of $\mathsf{iJT4_{CS}}$ with respect to basic modular models, there exists a basic modular model $\mathfrak{B} = (W, \leq, *)$ and a world $w \in W$ such that $(\mathfrak{B}, w) \nvDash A$. We define a quasimodel $\mathfrak{M} := (W, \leq, R, *)$ with $R :=\leq$. By locality of truth for quasimodels (Lemma 5.3), we have that $(\mathfrak{M}, w) \nvDash A$, and it only remains to show that $\mathfrak{M}$ is a modular $\mathsf{iJT4_{CS}}$-model, i.e., that all the restrictions on R and the condition JYB are met. The reflexivity and transitivity of R are trivial. We check condition (4) (Compatibility of $\leq$ with R), i.e., $w \leq v \implies R[v] \subseteq R[w]$. Assume $w \leq v$ and $u \in R[v]$. This means that $v \leq u$, so by transitivity of $\leq$ we have $w \leq u$ which means that $u \in R[w]$. Let us finish the proof by demonstrating JYB. Assume that $A \in t^*_w$ and $R(w, v)$. From this we get that $(\mathfrak{B}, w) \vDash t : A$ and $w \leq v$. By monotonicity for basic modular models, it follows that $(\mathfrak{B}, v) \vDash t : A$, so $A \in t^*_v$. By the factivity of basic modular models, we get that $(\mathfrak{B}, v) \vDash A$, and by the locality of truth in quasimodels, $(\mathfrak{M}, v) \vDash A$. Since v was arbitrary, we conclude that $A \in \Box_w$. $\Box$

Definition 5.10 (Fully explanatory modular models)**.** A modular model $\mathfrak{M} = (W, \leq, R, *)$ is *fully explanatory* if for any $w \in W$,

$$\Box_w \subseteq \bigcup_{t \in \mathsf{Tm}} t^*_w,$$

i.e., $A \in \Box_w$ implies $A \in t^*_w$ for some $t \in \mathsf{Tm}$.

We need the following auxiliary definition.

Definition 5.11. $\Gamma/\sharp := \{A \in \mathcal{L}_{\mathsf{J}} \mid t : A \in \Gamma \quad \text{for some } t \in \mathsf{Tm}\}$.

Lemma 5.12.

$$\Gamma \subseteq \Delta \quad \Longrightarrow \quad \Gamma/\sharp \subseteq \Delta/\sharp$$

Proof. Assume that $\Gamma \subseteq \Delta$ and let $A \in \Gamma/\sharp$. By definition, there exists a term t, such that $t : A \in \Gamma$, so $t : A \in \Delta$ and $A \in \Delta/\sharp$. □

Lemma 5.13 (Soundness and completeness: fully explanatory modular models)**.** Let CS be an axiomatically appropriate constant specification. Then $\mathsf{iJT4_{CS}}$ is sound and complete with respect to fully explanatory modular models.

Proof. Soundness immediately follows from soundness with respect to all modular models (and holds independently of whether CS is axiomatically appropriate).

We define the canonical model as

$$\mathfrak{M}^{can} := (W^{can}, \leq^{can}, R^{can}, *^{can})$$

where

(i) $W^{can} := \{\Delta \subseteq \mathcal{L}_{\mathsf{J}} \mid \Delta \text{ is prime}\}$

(ii) $\leq^{can} := \subseteq$

(iii) $*^{can}(p, \Delta) = 1$ iff $p \in \Delta$

(iv) $*^{can}(t, \Delta) := t^{-1}\Delta$

(v) $R^{can}(\Gamma, \Delta)$ iff $\Gamma/\sharp \subseteq \Delta$

To show that $\mathfrak{M}^{can}$ is a modular $\mathsf{iJT4_{CS}}$-model, it remains to establish that the set W^{can} is non-empty, that R^{can} is reflexive and transitive, that $\leq^{can}$ is compatible with R^{can} and that the condition JYB is satisfied. We start with showing $W^{can} \neq \varnothing$. We have already shown that the empty set is $\mathsf{iJT4_{CS}}$-consistent, so by the Prime Lemma 4.9, there exists a prime set extending $\varnothing$, which is an element of W^{can}.

To show that $\leq^{can}$ is compatible with R^{can}, assume that $\Gamma \subseteq \Delta$. We need to show that $R^{can}[\Delta] \subseteq R^{can}[\Gamma]$, so we pick $\Pi \in R^{can}[\Delta]$ and show that $\Pi \in R^{can}[\Gamma]$. $\Pi \in R^{can}[\Delta]$ means that $\Delta/\sharp \subseteq \Pi$. By the lemma above, we have that $\Gamma/\sharp \subseteq \Delta/\sharp$, and therefore $\Gamma/\sharp \subseteq \Pi$, i.e., $\Pi \in R^{can}[\Gamma]$.

To show JYB, assume $A \in t_{\Gamma}^{*^{can}}$ for some formula A , some $t \in \mathsf{Tm}$, and some $\Gamma \in W^{can}$. We need to show that $A \in \Box_{\Gamma}$, i.e., that $(\mathfrak{M}^{can}, \Delta) \vDash A$ whenever $R^{can}(\Gamma, \Delta)$. Consider any such $\Delta \in W^{can}$. We have $t : A \in \Gamma$ by the definition of $t_{\Gamma}^{*^{can}}$ and $A \in \Delta$ by the definition of R^{can} . By the truth lemma for basic evaluations, it follows that $(\mathfrak{B}^{can}, \Delta) \vDash A$ where $\mathfrak{B}^{can} = (W^{can}, \leq^{can}, *^{can})$. By the locality of truth in quasimodels, we have $(\mathfrak{M}^{can}, \Delta) \vDash A$.

To show that R^{can} is reflexive, consider any $\Gamma \in W^{can}$. Assume that $A \in \Gamma/\sharp$, i.e., that $t : A \in \Gamma$ for some $t \in \mathsf{Tm}$. Since Γ is prime, it is deductively closed. $t : A \to A$ is an axiom, so $t : A \to A \in \Gamma$. Again, since Γ is deductively closed, it follows by (MP) that $A \in \Gamma$. Therefore, $\Gamma/\sharp \subseteq \Gamma$, which means that $R^{can}(\Gamma, \Gamma)$.

To show that R^{can} is transitive, consider arbitrary $\Gamma, \Delta, \Pi \in W^{can}$ such that $R^{can}(\Gamma, \Delta)$ and $R^{can}(\Delta, \Pi)$. Assume that $A \in \Gamma/\sharp$, i.e., that $t : A \in \Gamma$ for some $t \in \mathsf{Tm}$. Since Γ is prime, it is deductively closed, and since $t : A \to\, !t : t : A$ is an axiom of $\mathsf{iJT4}_{\mathsf{CS}}$, we conclude $!t : t : A \in \Gamma$. Hence $t : A \in \Gamma/\sharp \subseteq \Delta$ and $A \in \Delta/\sharp \subseteq \Pi$. Therefore, $\Gamma/\sharp \subseteq \Pi$, which means $R^{can}(\Gamma, \Pi)$.

Finally, we show that $\mathfrak{M}^{can}$ is fully explanatory. Assume that $A \in \Box_\Gamma$ for some formula A and prime set Γ. Then

$$\Gamma/\sharp \vdash A \tag{1}$$

Indeed, assume for a contradiction that $\Gamma/\sharp \nvdash A$. By the Prime Lemma, there exists a prime set Δ such that $\Gamma/\sharp \subseteq \Delta$ and $\Delta \nvdash A$. By the definition of R^{can}, we have $R^{can}(\Gamma, \Delta)$, and from $\Delta \nvdash A$ we get that $A \notin \Delta$. By the Truth Lemma for basic evaluations, it follows that $(\mathfrak{B}^{can}, \Delta) \nvDash A$. By the locality of truth in quasimodels, we have $(\mathfrak{M}^{can}, \Delta) \nvDash A$, contradicting our assumption that $A \in \Box_\Gamma$. By (1), it follows that there are a finite set $G_1, \ldots, G_n \in \Gamma/\sharp$, such that

$$G_1, \ldots, G_n \vdash A.$$

Since each $G_i \in \Gamma/\sharp$, there must exist terms $s_i \in \mathsf{Tm}$ such that $s_i : G_i \in \Gamma$ for each $1 \leq i \leq n$.

By Lemma 3.7, given the axiomatic appropriateness of CS, there exists a term t such that

$$s_1 : G_1, \ldots, s_n : G_n \vdash t : A$$

By the Deduction Theorem

$$\vdash s_1 : G_1 \to (s_2 : G_2 \to \cdots \to (s_n : G_n \to t : A) \ldots).$$

Γ is prime, so it is deductively closed, and therefore $t : A \in \Gamma$ and finally

$$A \in t^{-1}\Gamma = t_\Gamma^{*^{can}}.$$

So $\mathfrak{M}^{can}$ is fully explanatory. $\square$

6 Realization

We establish in this section that the justification logic iJT4 is the explicit counterpart of the intuitionistic modal logic iS4. This is simply a reformulation of [3, Section 3] using axiomatically appropriate and schematic constant specifications.

First we show that iS4 is the forgetful projection of iJT4. We need the following definition: if A is a formula of $\mathcal{L}_\mathsf{J}$, then A° is the formula of $\mathcal{L}_\mathsf{I}$ that is the result of replacing all occurrences of $t :$ in A with $\Box$. We immediately get the following theorem.

Theorem 6.1 (Forgetful projection)**.** Let CS be an arbitrary constant specification. For each $\mathcal{L}_\mathsf{J}$-formula A,

$$\vdash_{\mathsf{iJT4}_\mathsf{CS}} A \quad \text{implies} \quad \vdash_{\mathsf{HiS4}} A^\circ.$$

Proof. By induction on the length of the $\mathsf{iJT4}_\mathsf{CS}$ derivation.

It is easy to see that for each axiom A of $\mathsf{iJT4}_\mathsf{CS}$, we have $\vdash_{\mathsf{HiS4}} A^\circ$.

If A is the conclusion of an application of modus ponens from premises B and $B \to A$, then by induction hypothesis and the definition of $\cdot^\circ$ we get

$$\vdash_{\mathsf{HiS4}} B^\circ \quad \text{and} \quad \vdash_{\mathsf{HiS4}} B^\circ \to A^\circ$$

and thus $\vdash_{\mathsf{HiS4}} A^\circ$ by modus ponens.

If A is the conclusion of an instance of axiom necessitation, then A has the form $c : B$ for some axiom B of $\mathsf{iJT4}_\mathsf{CS}$. Therefore, as shown above, $\vdash_{\mathsf{HiS4}} B^\circ$. An application of necessitation yields $\vdash_{\mathsf{HiS4}} \Box B^\circ$, which is $\vdash_{\mathsf{HiS4}} A^\circ$. $\Box$

Now we show the converse direction, namely that iJT4 realizes iS4. For this, we need the following definition: a *realization* r is a mapping from $\mathcal{L}_\mathsf{I}$ to $\mathcal{L}_\mathsf{J}$ such that for each $\mathcal{L}_\mathsf{I}$-formula A we have that

$$(r(A))^\circ = A.$$

A realization is *normal* if all negative occurrences of $\Box$ are realized by justification variables.

Theorem 6.2 (Realization)**.** Let CS be an axiomatically appropriate and schematic constant specification. Then there exists a realization r such that for each $\mathcal{L}_\mathsf{I}$-formula A we have

$$\vdash_{\mathsf{GiS4}} A \quad \text{implies} \quad \vdash_{\mathsf{iJT4}_\mathsf{CS}} r(A).$$

Proof. It turns out that Artemov's original realization proof for LP [2] also works in the intuitionistic case. We will only give a proof sketch here.

We start with defining positive and negative occurrences of $\Box$ in a sequent as usual. Observe that the rules of $\mathsf{GiS4}$ respect these polarities so that $(\supset \Box)$ introduces positive occurrences of $\Box$ and $(\Box \supset)$ introduces negative occurrences of $\Box$. Occurrences of $\Box$ are *related* if they occur in related formulas of premises and conclusions of rules; we close this relationship of related occurrences under transitivity. All occurrences of $\Box$ in a $\mathsf{GiS4}$-derivation naturally split into disjoint *families* of related occurrences. We call a family *essential* if at least one of its members is introduced by a $(\supset \Box)$ rule. Note that an essential family is positive (i.e. contains only positive occurrences).

Now let $\mathcal{D}$ be the $\mathsf{GiS4}$ derivation that proves A. The desired $\mathcal{L}_{\mathsf{J}}$-formula $r(A)$ is constructed by the following three steps. We reserve a large enough set of justification variables as *provisional variables.*

1. For each negative family and each non-essential positive family, replace all $\Box$ occurrences by x : where we choose a fresh justification variable for each family.

2. Pick an essential family f. Enumerate all occurrences of $(\supset \Box)$ rules that introduce a $\Box$-operator to this family. Replace each $\Box$ with a justification term

$$v_1 + \cdots + v_{n_f}$$

   where each v_i is a fresh provisional variable. Do this for each essential family. The resulting tree $\mathcal{D}'$ is labelled by $\mathcal{L}_{\mathsf{J}}$-formulas.

3. Replace the provisional variables starting with the leaves and working toward the root. By induction on the depth of a node in $\mathcal{D}'$ we establish that after the process passes a node, the sequent assigned to this node becomes derivable in $\mathsf{iJT4}_{\mathsf{CS}}$ where derivability of $\Gamma \supset A$ means $\Gamma \vdash_{\mathsf{iJT4}_{\mathsf{CS}}} A$. We distinguish the following cases.

   (a) The axioms $\Gamma \supset A$ with $A \in \Gamma$ or $\bot \in \Gamma$ are derivable in $\mathsf{iJT4}_{\mathsf{CS}}$.

   (b) For every rule other than $(\supset \Box)$ we do not change the term assignment and establish that the conclusion of the rule is derivable in $\mathsf{iJT4}_{\mathsf{CS}}$ if the premises are.

   (c) Let an occurrence of a $(\supset \Box)$ rule have number i in the enumeration of all $(\supset \Box)$ rules in a given family f. The corresponding node in $\mathcal{D}'$ is labelled by

$$\frac{y_1 : B_1, \ldots, y_k : B_k \supset A}{y_1 : B_1, \ldots, y_k : B_k \supset u_1 + \cdots + u_{n_f} : A}$$

where the y's are justification variables, the u's are justification terms, and u_i is a provisional variable. By the induction hypothesis

$$y_1 : B_1, \ldots, y_k : B_k \supset A$$

is derivable in $\mathsf{iJT4_{CS}}$. Using the Lifting Lemma, we construct a term t such that

$$y_1 : B_1, \ldots, y_k : B_k \vdash_{\mathsf{iJT4_{CS}}} t : A.$$

Thus

$$y_1 : B_1, \ldots, y_k : B_k \vdash_{\mathsf{iJT4_{CS}}} u_1 + \cdots + u_{i-1} + t + u_{i+1} + \cdots + u_{n_f} : A.$$

Substitute t for u_i everywhere in $\mathcal{D}'$. By Lemma 3.9, this does not affect the already established derivability results.

Eventually, all provisional variables are replaced with terms of non-provisional variables in $\mathcal{D}'$ and we have established that its root sequent $r(A)$ is derivable in $\mathsf{iJT4_{CS}}$. The realization r built by this construction is normal. □

7 Conclusion

We have established that if we take the classical Logic of Proofs and change the underlying classical propositional logic to intuitionistic propositional logic, then we obtain an explicit counterpart of the intuitionistic modal logic $\mathsf{iS4}$. This is an interesting result since the logic of proofs of Heyting arithmetic includes additional axioms that introduce special justification terms for all admissible rules of intuitionistic logic. This seems necessary to obtain completeness with respect to provability semantics where the justification relation is interpreted by formal provability in Heyting Arithmetic.

Our results now show that these additional axioms and justification terms are not needed if we are interested in the explicit counterpart of intuitionistic modal logic and the corresponding possible world semantics for justification logic.

Moreover, we believe that intuitionistic justification logics will help to understand intuitionistic modal logics better. In particular, they will help to clarify the role of additional principles for the $\Box$-modality and the corresponding conditions on the accessibility relation. However, this is left for future research.

References

[1] Sergei N. Artemov. Operational modal logic. Technical Report MSI 95–29, Cornell University, December 1995.

[2] Sergei N. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, March 2001.

[3] Sergei N. Artemov. Unified semantics for modality and λ-terms via proof polynomials. In Kees Vermeulen and Ann Copestake, editors, *Algebras, Diagrams and Decisions in Language, Logic and Computation*, volume 144 of *CSLI Lecture Notes*, pages 89–118. CSLI Publications, Stanford, 2002.

[4] Sergei [N.] Artemov. Justified common knowledge. *Theoretical Computer Science*, 357(1–3):4–22, July 2006.

[5] Sergei [N.] Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, December 2008.

[6] Sergei N. Artemov. The ontology of justifications in the logical setting. *Studia Logica*, 100(1–2):17–30, April 2012. Published online February 2012.

[7] Sergei [N.] Artemov and Rosalie Iemhoff. The basic intuitionistic logic of proofs. *Journal of Symbolic Logic*, 72(2):439–451, June 2007.

[8] Sergei [N.] Artemov and Elena Nogina. Introducing justification into epistemic logic. *Journal of Logic and Computation*, 15(6):1059–1073, December 2005.

[9] Alexandru Baltag, Bryan Renne, and Sonja Smets. The logic of justified belief, explicit knowledge, and conclusive evidence. *Annals of Pure and Applied Logic*, 165(1):49–81, January 2014. Published online in August 2013.

[10] Samuel Bucheli, Roman Kuznets, and Thomas Studer. Justifications for common knowledge. *Journal of Applied Non-Classical Logics*, 21(1):35–60, January–March 2011.

[11] Samuel Bucheli, Roman Kuznets, and Thomas Studer. Partial realization in dynamic justification logic. In Lev D. Beklemishev and Ruy de Queiroz, editors, *Logic, Language, Information and Computation, 18th International Workshop, WoLLIC 2011, Philadelphia, PA, USA, May 18–20, 2011, Proceedings*, volume 6642 of *Lecture Notes in Artificial Intelligence*, pages 35–51. Springer, 2011.

[12] Samuel Bucheli, Roman Kuznets, and Thomas Studer. Realizing public announcements by justifications. *Journal of Computer and System Sciences*, 80(6):1046–1066, 2014.

[13] Evgenij Dashkov. Arithmetical completeness of the intuitionistic logic of proofs. *Journal of Logic and Computation*, 21(4):665–682, August 2011. Published online August 2009.

[14] G. Fischer Servi. Axiomatizations for some intuitionistic modal logics. *Rendiconti del Seminario Matematico Universita‘ e Politecnico di Torino*, 42:179–194, 1984.

[15] Melvin Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132(1):1–25, February 2005.

[16] Meghdad Ghari. Pavelka-style fuzzy justification logics. *Logic Journal of the IGPL*, 24(5):743–773, 2016.

[17] Gerhard Jäger and Michel Marti. Intuitionistic common knowledge or belief. *Journal*

of Applied Logic, 18:150–163, 2016.

[18] Ioannis Kokkinis, Petar Maksimović, Zoran Ognjanović, and Thomas Studer. First steps towards probabilistic justification logic. *Logic Journal of IGPL*, 23(4):662–687, 2015.

[19] Roman Kuznets and Thomas Studer. Justifications, ontology, and conservativity. In Thomas Bolander, Torben Braüner, Silvio Ghilardi, and Lawrence Moss, editors, *Advances in Modal Logic, Volume 9*, pages 437–458. College Publications, 2012.

[20] Roman Kuznets and Thomas Studer. Update as evidence: Belief expansion. In Sergei [N.] Artemov and Anil Nerode, editors, *Logical Foundations of Computer Science, International Symposium, LFCS 2013, San Diego, CA, USA, January 6–8, 2013, Proceedings*, volume 7734 of *Lecture Notes in Computer Science*, pages 266–279. Springer, 2013.

[21] Roman Kuznets and Thomas Studer. Weak arithmetical interpretations for the logic of proofs. *Logic Journal of the IGPL*, 24(3):424–440, 2016.

[22] Hiroakira Ono. On some intuitionistic modal logics. *Publications of the Research Institute for Mathematical Sciences*, 13(3):687–722, 1977.

[23] Gordon Plotkin and Colin Stirling. A framework for intuitionistic modal logics: Extended abstract. In *Proceedings of the 1986 Conference on Theoretical Aspects of Reasoning About Knowledge*, TARK '86, pages 399–406. Morgan Kaufmann Publishers Inc., 1986.

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

Received \jreceived