The internalized disjunction property for intuitionistic justification logic

Michel Marti [1]

Loria
Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy
France

Thomas Studer [2]

Institute of Computer Science
University of Bern, Neubrückstrasse 10, 3012 Bern
Switzerland

Abstract

In intuitionistic justification logic, evidence terms represent intuitionistic proofs, that is a formula r:A means r is an intuitionistic proof of A. A natural principle in this context is the internalized disjunction property (IDP), which is: for each term r there exists a term s such that r:(A or B) implies s:A or s:B.
We introduce a small extension of iJT4, in which IDP is valid. Our proof relies on a model construction that enforces sharp evidence relations and a tight connection between syntax and semantics. This makes it possible to switch between proofs and models, which will be the key to proving IDP.

Keywords: Justification logic, intuitionistic logic, disjunction property, sharp model.

1 Introduction

Justification logics feature formulas of the form $t : A$ meaning *A is known for reason t*. The evidence term t can stand for formal proof of A (say in Peano Arithmetic) [2,21] or t can represent an informal justification to believe that A [14]. This second reading turned out to be very useful for analyzing a variety of epistemic situations,see,e.g., [4,5,8,9,11,12,17].

It is a distinguishing feature of justification logics that they internalize their own notion of proof. If a formula A is provable, then there exists a term t such that $t : A$ is also provable and, additionally, the term t is a blueprint of the proof of A.

[1] `michel.marti@loria.fr`

[2] `tstuder@inf.unibe.ch`
Supported by the Swiss National Science Foundation grant 200021_165549.

In an intuitionistic setting, it is natural to ask whether an internalized version of the disjunction property holds, i.e., for each term t there exists a term s such that

$$t : (A \vee B) \to (s : A \vee s : B) \tag{IDP}$$

is valid. In this paper we introduce an intuitionistic justification logic iJ and show that iJ proves (IDP).

Our logic iJ is a light extension of ILP, which is an intuitionistic version of the Logic of Proofs. Artemov introduced ILP in one of the early papers on justification logic [3] with the aim of unifying the semantics of modalities and λ-calculus. He defined ILP by changing the propositional base of LP to intuitionistic logic while keeping the other axioms of LP. Artemov then showed that ILP can realize a λ-calculus for intuitionistic S4.

Marti und Studer [22] recently developed a possible world semantics for ILP. They introduced so-called modular models for ILP, which feature the principle *justification yields belief* [6,19].

Steren and Bonelli [24] provide an alternative term system for ILP that is based on natural deduction and hypothetical reasoning. Their aim is to reformulate the Logic of Proofs in order to explore applications in programming languages.

The axiomatization of ILP does not yield a proper intuitionistic provability semantics, which means to interpret $t : A$ as *t encodes a proof of A in Heyting Arithmetic*. Artemov and Iemhoff [7] extended ILP by axioms that introduce novel proof terms to internalize certain admissible rules of intuitionistic logic. The arithmetical completeness of that system was later established by Dashkov [13].

The above mentioned intuitionistic justification logics all study explicit versions of the $\Box$-modality. Kuznets, Marin, and Straßburger [18] provide a treatment of the intuitionistic $\Diamond$-modality in the style of justification logic. To do so, they introduce a new type of evidence terms that justifies consistency. Hence they obtain justification analogues of several constructive modal logics and establish a realization theorem for them.

The structure of the paper is as follows. In the next section we will introduce the logic iJ, which is a light extension of the intuitionistic justification logic iJT4. Then we present generated models for iJ and establish soundness of iJ. In Section 4 we define point-generated models, which are needed to prove the disjunction property. Section 5 studies atomic models, i.e. models that are completely defined by the evaluations of atomic propositions and atomic justifications. The name *atomic model* goes back to Kashev [16]; Artemov [1] uses *sharp model*. In Section 6 we define the canonical model and establish completeness of iJ with respect to atomic models. Finally, in Section 7, we prove the internalized disjunction property for iJ. In the last section we discuss future work and give some hints about the realization of Hirai's intuitionistic modal logic [15] in iJ. The appendix contains proofs of some technical lemmas.

2 The Logic $\mathsf{iJ_{CS}}$

We start with a countable set of atomic propositions Prop and a countable set of term constants Const. We define terms and formulas of our language simultaneously by the following grammar:

$$t ::= c \mid ?_n \mid t + t \mid !t \mid t \cdot_A t$$
$$A ::= \bot \mid P \mid A \wedge A \mid A \vee A \mid A \to A \mid t : A$$

where $c \in \mathsf{Const}$, $P \in \mathsf{Prop}$, and $n \in \mathbb{N}$. The set of terms is denoted by Tm, the set of formulas by Fm. We will use P, Q, R for propositions, c, d, e for constants, A, B, C, D for arbitrary formulas, and t, r, s for terms.

The system iJ has the following axioms for all $t, s \in \mathsf{Tm}$ and all $A, B \in \mathsf{Fm}$

(i) all axioms for intuitionistic propositional logic

(ii) $t : A \wedge s : (A \to B) \to (s \cdot_A t) : B$ (j)

(iii) $(s \cdot_A t) : B \to t : A \wedge s : (A \to B)$ (invj)

(iv) $t : A \vee s : A \to (t + s) : A$ (+)

(v) $(t + s) : A \to t : A \vee s : A$ (inv+)

(vi) $t : A \to !t : (t : A)$ (!)

(vii) $\neg(!t : A)$ if A is not of the form $t : B$ for any formula $B \in \mathsf{Fm}$ (inv!)

(viii) $(t : A) \to A$ truth property (t)

Definition 2.1 A *constant specification* CS is any subset

$$\mathsf{CS} \subseteq \{(c, A) \mid c \in \mathsf{Const} \text{ and } A \in \mathsf{Fm} \text{ is an axiom of } \mathsf{iJ}\}.$$

A constant specification CS is called *axiomatically appropriate* if for each axiom A of iJ, there is a constant c such that $(c, A) \in \mathsf{CS}$.

Definition 2.2 [$?_n$-form] For each natural number $n \in \mathbb{N}$, we define what it means for a formula to be of $?_n$-form as follows:

- for $n = 0$, A is of $?_0$-form iff $A = \neg(c : B)$ for some formula B with $B \notin \mathsf{Prop}$ and $(c, B) \notin \mathsf{CS}$;
- A is of $?_{(n+1)}$-form iff $A = \neg ?_n : B$ for some formula B which is not of $?_n$-form.

Definition 2.3 For a constant specification CS the deductive system $\mathsf{iJ_{CS}}$ is the Hilbert system given by the axioms (axiom schemes) above and by the following three rules:

$$\frac{A \quad A \to B}{B}\,(\mathrm{MP}) \qquad \frac{(c, A) \in \mathsf{CS}}{c : A}\,(\mathrm{AN})_{\mathsf{CS}} \qquad \frac{A \text{ is of } ?_n\text{-form}}{?_n : A}\,(?_n)$$

The system $\mathsf{iJ_{CS}}$ defines a family of logics parameterized by the constant specification CS. Hence we should denote the derivability relation of $\mathsf{iJ_{CS}}$ by $\vdash_{\mathsf{CS}}$. For simplicity, however, we will only write $\vdash$ when CS is clear from the context.

The system $\mathsf{iJ}_{\mathsf{CS}}$ is tailored towards minimal evidence relations. This explains why we included inverse axioms (invj) and (inv+) for application and sum, respectively. In order to formulate (invj) we need a labelled application operator, which goes back to Renne [23]. These inverse axioms make it possible to reduce a justification with an application to simpler justifications, see, e.g., [20].

Our aim is to prove an internalized version of the disjunction property. In order to achieve this, we have to guarantee that a constant term can only justify an axiom (as given in the constant specification) or an atomic proposition. This could be achieved with a rule of the form

$$\frac{(c, B) \notin \mathsf{CS} \text{ and } B \notin \mathsf{Prop}}{\neg(c : B)} .$$

However, since we want to have the Lifting Lemma 2.6, we need terms to justify derivations with this rule. The is the role of the $?_n$-terms and explains the rule $(?_n)$, which can be thought of as a form of negative introspection for the constant specification.

Remark 2.4 Recall that our language does *not* include justification variables. The reason is that variables stand for arbitrary terms, which does not fit our setting. Suppose that we have variables and assume $(c, A) \in \mathsf{CS}$. Then

$$\neg(!c : x : A) \tag{1}$$

is an instance of axiom (inv!) since syntactically the term c is different from the term x. However, if we substitute c for x in (1), then we obtain $\neg(!c : c : A)$, which is provable false. So by substitution, we can transform a valid formula into a provably false formula. To avoid this, we do not include variables in our language (but we will come back to this issue in the Conclusion).

As usual in justification logic, the Deduction Theorem holds.

Theorem 2.5 (Deduction Theorem)

$$A \vdash B \quad \Longleftrightarrow \quad \vdash A \to B$$

Since the rule $(?_n)$ only introduces formulas of the form $t : A$, we can prove the following form of the Lifting Lemma as usual.

Lemma 2.6 *Let CS be an axiomatically appropriate constant specification. For all terms $t_1, \dots, t_n \in \mathsf{Tm}$ and all formulas $A_1, \dots, A_n, C \in \mathsf{Fm}$, if*

$$t_1 : A_1, \dots, t_n : A_n \vdash_{\mathsf{CS}} C,$$

then there is a term $t \in \mathsf{Tm}$ such that

$$t_1 : A_1, \dots, t_n : A_n \vdash t : C$$

3 Generated Models

We are now going to introduce a semantics for $\mathsf{iJ_{CS}}$. A *frame* $\mathcal{F} = (W, \leq)$ is a pair consisting of a set W of states and a reflexive and transitive relation $\leq$ on W. A model for $\mathsf{iJ_{CS}}$ is essentially a frame with a suitable minimal basic modular model assigned to each state. These models are called *generated* since minimality is achieved by inductively generating the models [20,25,26].

Definition 3.1 [Basis] Given a frame $\mathcal{F} = (W, \leq)$ and a constant specification CS, a basis for $\mathcal{F}$ is a familiy of sets $(\mathcal{B}_w)_{w \in W}$ such that

- $\mathcal{B}_w \subseteq \mathsf{Tm} \times \mathsf{Fm}$ for each $w \in W$,
- $w \leq v \quad \Longrightarrow \quad \mathcal{B}_w \subseteq \mathcal{B}_v \quad$ (Monotonicity).
- $(!t, A) \notin \mathcal{B}_w \quad$ if A is not of the form $t : B$ for any formula $B \in \mathsf{Fm}$.

$\mathcal{B}_w$ must be downwards closed, i.e. for each $w \in W$:

- $(t + s, A) \in \mathcal{B}_w \quad \Longrightarrow \quad (t, A) \in \mathcal{B}_w$ or $(s, A) \in \mathcal{B}_w$;
- $((t \cdot_A s), B) \in \mathcal{B}_w \quad \Longrightarrow \quad (s, A) \in \mathcal{B}_w$ and $(t, A \to B) \in \mathcal{B}_w$;
- $(!t, t : A) \in \mathcal{B}_w \quad \Longrightarrow \quad (t, A) \in \mathcal{B}_w$

Definition 3.2 [Evidence Closure] Let $B \subseteq \mathsf{Tm} \times \mathsf{Fm}$. For a set $X \subseteq \mathsf{Tm} \times \mathsf{Fm}$ we define $\mathsf{cl}_B(X)$ by

(i) if $(t, A) \in B$, then $(t, A) \in \mathsf{cl}_B(X)$;
(ii) if $(s, A) \in X$ and $(t, A \to B) \in X$, then $((t \cdot_A s), B) \in \mathsf{cl}_B(X)$;
(iii) if $(s, A) \in X$, then $((s + t), A) \in \mathsf{cl}_B(X)$;
(iv) if $(t, A) \in X$, then $((s + t), A) \in \mathsf{cl}_B(X)$;
(v) if $(t, A) \in X$, then $(!t, t : A) \in \mathsf{cl}_B(X)$;

For any $B \subseteq \mathsf{Tm} \times \mathsf{Fm}$, the operator cl_B is monotone. Therefore, cl_B has a least fixed point, which we denote *the evidence relation induced by* B.

Definition 3.3 [Evidence Relation] Let $B \subseteq \mathsf{Tm} \times \mathrm{Fm}$. Then $\mathcal{E}(B)$ is defined as the least fixed point of cl_B.

We need the following immediate properties about evidence relations.

Lemma 3.4 (Constants are in the Basis) *For all formulas A and constants c we have:*

$$(c, A) \in \mathcal{E}(\mathcal{B}_w) \quad \Longrightarrow \quad (c, A) \in \mathcal{B}_w.$$

Lemma 3.5 *If A is not of the form $t : B$, then*

$$(!t, A) \notin \mathcal{E}(\mathcal{B}_w).$$

Definition 3.6 [Generated Models] Let CS be a constant specification. A *generated model* is a structure $\mathfrak{M} = (W, \leq, V, (\mathcal{B}_w)_{w \in W})$, where

(i) $(W, \leq)$ is a frame,
(ii) $(\mathcal{B}_w)_{w \in W}$ is a basis on $(W, \leq)$,

(iii) $V : W \to \mathcal{P}(\mathsf{Prop})$ such that $w \leq v \Longrightarrow V_w \subseteq V_v$ (Monotonicity)

The model $\mathfrak{M}$ is called a CS-*model* if

(i) $\mathsf{CS} \subseteq \mathcal{B}_w$ for all $w \in W$

(ii) $(?_n, A) \in \mathcal{B}_w$ for each formula A that is of $?_n$-form

(iii) $(?_n, A) \notin \mathcal{B}_w$ for each formula A that is not of $?_n$-form

Definition 3.7 [Truth in Generated Model] Let CS be a constant specification, $\mathfrak{M} = (W, \leq, V, (\mathcal{B}_w)_{w \in W})$ a generated model and $A \in \mathsf{Fm}$ be a (variable-free!) formula. We define the relation $(\mathfrak{M}, w) \vDash A$ by

(i) $(\mathfrak{M}, w) \nvDash \bot$

(ii) $(\mathfrak{M}, w) \vDash p$ iff $p \in V_w$

(iii) $(\mathfrak{M}, w) \vDash A \wedge B$ iff $(\mathfrak{M}, w) \vDash A$ and $(\mathfrak{M}, w) \vDash B$

(iv) $(\mathfrak{M}, w) \vDash A \vee B$ iff $(\mathfrak{M}, w) \vDash A$ or $(\mathfrak{M}, w) \vDash B$

(v) $(\mathfrak{M}, w) \vDash A \to B$ iff $(\mathfrak{M}, v) \vDash B$ for all $v \geq w$ with $(\mathfrak{M}, v) \vDash A$

(vi) $(\mathfrak{M}, w) \vDash t : A$ iff $(t, A) \in \mathcal{E}(\mathcal{B}_w)$

Definition 3.8 We call a generated model *factive* iff for each term $t \in \mathsf{Tm}$ and each formula $A \in \mathsf{Fm}$:

$$(t, A) \in \mathcal{E}(\mathcal{B}_w) \quad \Longrightarrow \quad (\mathfrak{M}, w) \vDash A.$$

It is immediately clear from the truth definition that factive models satisfy Axiom (t) of $\mathsf{iJ}_{\mathsf{CS}}$. Using the fact that in generated models, evidence relations are constructed as least fixed points, we can show soundness of $\mathsf{iJ}_{\mathsf{CS}}$.

Theorem 3.9 (Soundness) *The logic* $\mathsf{iJ}_{\mathsf{CS}}$ *is sound with respect to factive generated* CS*-models, i.e.*

$$\vdash A \quad \Longrightarrow \quad \vDash_{\textit{factive generated } \mathsf{CS}\textit{-models}} A$$

4 Point-Generated Models

In this section we introduce point-generated models and show that each model has an equivalent point-generated model. These models are needed for showing the disjunction property via glueing.

Definition 4.1 [Point-Generated Model] Let $\mathfrak{M}$ be a generated model and $w \in W$. The model generated by w, denoted as $\mathfrak{M}_w = (W_w, \leq_w, V_w, \mathcal{B}(w))$ is defined by

$$\begin{aligned} W_w &:= \{v \in W \mid v \geq w\} \\ \leq_w &:= \leq \cap (W_w \times W_w) \\ V(w) &:= V\restriction_{W_w} (= V \cap (W_w \times \mathsf{Prop})) \\ \mathcal{B}(w)_v &:= \mathcal{B}_v \text{ for all } v \in W_w. \end{aligned}$$

A proof of the following lemma can be found in the appendix.

Lemma 4.2 (Invariance for Point-Generated Models) *Let $\mathfrak{M}$ be a model, $w \in W$, and $\mathfrak{M}_w$ the model generated by w. Then we have for each formula $A \in \mathsf{Fm}$ and each $v \in W_w$:*

$$(\mathfrak{M}, v) \vDash A \iff (\mathfrak{M}_w, v) \vDash A.$$

Remark 4.3 $(W_w, \leq)$ is a tree with root w.

5 Atomic Generated Models

The idea behind atomic models is that at each state, some new formulas get justifications, but those either have to be atomic, i.e., of the form $c : P$ where c is a constant and P is a propositional variable, they are part of the constant specification, or of the form $?_n : A$, where A is of $?_n$-form. You may think of $c : P$ as some bit of atomic evidence justifying some atomic fact, like a simple observation or a computation establishing some basic numeric fact.

Definition 5.1 [Atomic Model] We call a basis *atomic* iff for all $w \in W$

$$\mathcal{B}_w \subseteq (\mathsf{Const} \times \mathsf{Prop}) \cup \mathsf{CS} \cup \{(?_n, A) \mid A \text{ is of } ?_n\text{-form}\}$$

We call a generated model *atomic* iff its basis is atomic.

Lemma 5.2 *Let CS be a constant specification and $\mathfrak{M}$ a factive CS-model. If $A \notin \mathsf{Prop}$, $c \in \mathsf{Const}$, and $(c, A) \notin \mathsf{CS}$, then for all states w of $\mathfrak{M}$,*

$$(c, A) \notin \mathcal{B}_w.$$

Theorem 5.3 (Atomization) *Let CS be a constant specification and $\mathfrak{M}$ a factive CS-model with basis $\mathcal{B}$. Then there is an equivalent atomic CS-basis $\mathcal{B}'$, i.e.*

$$\mathcal{E}(\mathcal{B}_w) = \mathcal{E}(\mathcal{B}'_w) \quad \textit{for all } w \in W$$

Proof. The corresponding atomic basis is simply defined as the atomic part of the original basis, i.e.

$$\mathcal{B}'_w := \{(c, P) \in \mathsf{Const} \times \mathsf{Prop} \mid (c, P) \in \mathcal{B}_w\} \cup \mathsf{CS} \cup \{(?_n, A) \mid A \text{ is of } ?_n\text{-form}\}$$

Then it follows immediately that

- $w \leq v \Longrightarrow \mathcal{B}'_w \subseteq \mathcal{B}'_v$ (Monotonicity)
- $\mathcal{B}'$ is atomic
- $\mathcal{B}'_w \subseteq \mathcal{B}_w$ and therefore $\mathcal{E}(\mathcal{B}'_w) \subseteq \mathcal{E}(\mathcal{B}_w)$

It remains to show that $\mathcal{E}(\mathcal{B}_w) \subseteq \mathcal{E}(\mathcal{B}'_w)$. We show that for each evidence pair $(t, A) \in \mathcal{E}(\mathcal{B}_w)$, we have $(t, A) \in \mathcal{E}(\mathcal{B}'_w)$ and proceed by induction on the build-up of $\mathcal{E}(\mathcal{B}_w)$.

Base case. $(t, A) \in \mathcal{B}_w$. We continue by induction on t.

- If $t = c \in \mathsf{Const}$, then we distinguish the following three cases:
  - · $A = P \in \mathsf{Prop}$. Then by the definition of $\mathcal{B}'$ we have that $(t, A) = (c, P) \in \mathcal{B}'_w \subseteq \mathcal{E}(\mathcal{B}'_w)$.

· $(c, A) \in \mathsf{CS}$. Then we have $(c, A) \in \mathcal{B}'_w \subseteq \mathcal{E}(\mathcal{B}'_w)$.

· $A \notin \mathsf{Prop}$ and $(c, A) \notin \mathsf{CS}$. By the previous lemma, this case can not happen.

- $t = ?_n$. Since $\mathfrak{M}$ is a CS-model, A has to be of $?_n$-form. It follows by the definition of $\mathcal{B}'$ that $(?_n, A) \in \mathcal{B}'_w \subseteq \mathcal{E}(\mathcal{B}'_w)$.
- $t = !s$. By Lemma 3.5, A has to be of the form $s : B$ for some formula B. So we have $(!s, s : B) \in \mathcal{B}_w$, and since a basis is downwards closed, it follows that $(s, B) \in \mathcal{B}_w$. It follows by the I.H. that $(s, B) \in \mathcal{E}(\mathcal{B}'_w)$ and therefore $(!s, s : B) \in \mathcal{E}(\mathcal{B}'_w)$.
- $t = r + s$, so $(r + s, A) \in \mathcal{B}_w$. Since a basis is downwards closed, it follows that $(r, A) \in \mathcal{B}_w$ or $(s, A) \in \mathcal{B}_w$. It follows by the I.H. that $(r, A) \in \mathcal{E}(\mathcal{B}'_w)$ or $(s, A) \in \mathcal{E}(\mathcal{B}'_w)$, and therefore $(r + s, A) \in \mathcal{E}(\mathcal{B}'_w)$.
- $t = r \cdot_B s$. Again, since a basis is downwards closed, we have $(r, B \to A) \in \mathcal{B}_w$ and $(s, B) \in \mathcal{B}_w$. It follows by the I.H. that $(r, B \to A) \in \mathcal{E}(\mathcal{B}'_w)$ and $(s, B) \in \mathcal{E}(\mathcal{B}'_w)$ and therefore $(r \cdot_B s, A) \in \mathcal{E}(\mathcal{B}'_w)$.

Inductive step.

- $t = r + s$, and $(r, A) \in \mathcal{E}(\mathcal{B}_w)$ or $(s, A) \in \mathcal{E}(\mathcal{B}_w)$. It follows by the I.H. (outer induction on the build-up of $\mathcal{E}(\mathcal{B}_w)$) that $(r, A) \in \mathcal{E}(\mathcal{B}'_w)$ or $(s, A) \in \mathcal{E}(\mathcal{B}'_w)$ and therefore $(r + s, A) \in \mathcal{E}(\mathcal{B}'_w)$.
- $t = !s$, $A = s : B$ and $(s, B) \in \mathcal{E}(\mathcal{B}_w)$. It follows by the I.H. that $(s, B) \in \mathcal{E}(\mathcal{B}'_w)$ and therefore $(!s, s : B) \in \mathcal{E}(\mathcal{B}'_w)$.
- $t = r \cdot_B s$, $(r, B \to A) \in \mathcal{E}(\mathcal{B}_w)$ and $(s, B) \in \mathcal{E}(\mathcal{B}_w)$. It follows by the I.H. that $(r, B \to A) \in \mathcal{E}(\mathcal{B}'_w)$ and $(s, B) \in \mathcal{E}(\mathcal{B}'_w)$ and therefore $(r \cdot_B s, A) \in \mathcal{E}(\mathcal{B}'_w)$.

□

Corollary 5.4 *For each factive generated model, there is an equivalent atomic factive generated model.*

Definition 5.5 [Subformulas] For a formula A, its set of subformulas $\mathrm{subf}(A)$ is defined inductively as follows:

- $\mathrm{subf}(\bot) = \{\bot\}$
- $\mathrm{subf}(P) = \{P\}$ for $P \in \mathsf{Prop}$
- $\mathrm{subf}(A \odot B) := \{A \odot B\} \cup \mathrm{subf}(A) \cup \mathrm{subf}(B)$ for each $\odot \in \{\wedge, \vee, \to\}$
- $\mathrm{subf}(c : A) := \{c : A\} \cup \mathrm{subf}(A)$
- $\mathrm{subf}(!t : A) := \{!t : A\} \cup \mathrm{subf}(A)$
- $\mathrm{subf}(t + s : A) := \{t + s : A\} \cup \mathrm{subf}(t : A) \cup \mathrm{subf}(s : A)$
- $\mathrm{subf}(t \cdot_B s : A) := \{t \cdot_B s : A\} \cup \mathrm{subf}(t : B \to A) \cup \mathrm{subf}(s : B)$

Observe how we use the annotation in the application operator to catch the subformulas of B. By induction on the structure of formulas, we show that the set of subformulas of any given formula is finite.

Lemma 5.6 (Set of Subformulas is Finite) *For each formula A, its set of subformulas* $\mathrm{subf}(A)$ *is finite.*

The next lemma allows us to connect the truth of a justification formula at a point of an atomic model with the provability of that formula from the atomic information of that state. The proof of this lemma is in the appendix.

Lemma 5.7 (Connection Lemma) *Let* CS *be a constant specification,* $\mathfrak{M}$ *an atomic model and* $w \in W$. *Then we have for all formulas* $A, B \in \mathsf{Fm}$ *and each term* $t \in \mathsf{Tm}$

(i) $(\mathfrak{M}, w) \vDash t : A \quad \Longrightarrow \quad \{c : P \in \mathrm{subf}(t : A) \mid w \vDash c : P\} \vdash t : A.$

(ii) *If* $\mathfrak{M}$ *is a* CS*-model, then* $\{c : P \in \mathrm{subf}(A) \mid w \vDash c : P\} \cup \{P \in \mathrm{subf}(A) \mid w \vDash P\} \vdash B \quad \Longrightarrow$ $(\mathfrak{M}, w) \vDash B$

6 Canonical Model

In this section we perform a canonical model construction to establish completeness of $\mathsf{iJ}_{\mathsf{CS}}$. We only state the lemmas needed to obtain the final completeness result. The proofs are straightforward and left to the reader.

Definition 6.1 Given a constant specification CS, we call a set of formulas $\Delta \subseteq \mathsf{Fm}$ *prime* iff it satisfies the following conditions:

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

(ii) Δ is deductively closed with respect to CS i.e., for any formula B, if $\Delta \vdash B$, then $B \in \Delta$

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

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

We need a prime lemma relative to a fixed constant specification CS, since our relevant notion of provability involves a constant specification by using the rule of axiom necessitation and the $(?_n)$-rule.

Theorem 6.2 (Prime Lemma) *Let* CS *be a constant specification,* $B \in \mathsf{Fm}$ *be a formula ,* $N \subseteq \mathsf{Fm}$ *a set of formulas such that* $N \nvdash B$. *Then there exists a prime set* $\Delta \subseteq \mathsf{Fm}$ *with* $N \subseteq \Delta$ *and* $\Delta \nvdash B$.

Definition 6.3 [Canonical Generated Model] We define the canonical generated model $\mathfrak{M} = (W, \subseteq, V, (\mathcal{B}_\Delta)_{\Delta \in W})$ as follows:

(i) $W := \{\Delta \subseteq \mathrm{Fm} \mid \Delta \text{ is prime }\}$,

(ii) $V(\Delta) := \Delta \cap \mathsf{Prop}$

(iii) for every term $t \in \mathsf{Tm}$ we set $(t, A) \in \mathcal{B}_\Delta \quad :\Longleftrightarrow \quad t : A \in \Delta$

Lemma 6.4 $\mathcal{B}_\Delta$ *is downwards closed.*

Lemma 6.5 *The canonical generated model is a generated model indeed.*

Since our prime sets are deductively closed, it follows that the canonical basis is identical to its closure.

Lemma 6.6 *We have*

$$\mathcal{B}_\Delta = \mathcal{E}(\mathcal{B}_\Delta).$$

Lemma 6.7 (Canonical Evidence) *For all terms $t \in \mathsf{Tm}$ and all prime sets Δ, we have*

$$t : A \in \Delta \quad\Longleftrightarrow\quad (t, A) \in \mathcal{E}(\mathcal{B}_\Delta).$$

Lemma 6.8 *The canonical model is a* CS*-model.*

Lemma 6.9 *The canonical model is a factive generated model, i.e., for all $t \in \mathsf{Tm}$ and all $A \in \mathsf{Fm}$:*

$$(t, A) \in \mathcal{B}_\Delta \quad\Longrightarrow\quad \Delta \vDash A.$$

Theorem 6.10 (Completeness w.r.to to Factive Generated Models) *Let CS be a constant specification. The logic $\mathsf{iJ}_{\mathsf{CS}}$ is complete with respect to factive generated CS-models, i.e. for every formula $A \in \mathsf{Fm}$ we have*

$$\vDash_{\textit{factive generated } \mathsf{CS}\textit{-models}} A \quad\Longrightarrow\quad \vdash A.$$

For each factive generated CS-model, we find an equivalent atomic model by Corollary 5.4. It follows that there is an atomic model that is equivalent to the canonical one, and, therefore, we have completeness with respect to atomic factive generated CS-models.

Corollary 6.11 *Let CS be a constant specification. The logic $\mathsf{iJ}_{\mathsf{CS}}$ is complete with respect to atomic factive generated CS-models, i.e., for every formula A we have*

$$\vDash_{\textit{atomic factive generated } \mathsf{CS}\textit{-models}} A \quad\Longrightarrow\quad \vdash A.$$

7 Disjunction Properties

Our justification logic has the disjunction property. To prove this, we adapt the usual glueing technique, see, e.g., [10], to the framework of justification logic. In order to internalize the disjunction property later, we now have to consider derivations from a finite set of assumptions of the form $c : P$.

Theorem 7.1 (Disjunction Property) *Let CS be any constant specification and A, B formulas. Then we have:*

$$\begin{aligned} & c_1 : P_1, \ldots, c_n : P_n \vdash A \lor B \\ \Longrightarrow \quad & c_1 : P_1, \ldots, c_n : P_n \vdash A \quad \textit{or} \quad c_1 : P_1, \ldots, c_n : P_n \vdash B \end{aligned}$$

Proof. We proceed by contraposition. Suppose that

$$c_1 : P_1, \ldots, c_n : P_n \nvdash A \quad\text{and}\quad c_1 : P_1, \ldots, c_n : P_n \nvdash B.$$

By the Deduction Theorem we obtain

$$\nvdash \bigwedge_{i=1}^{n} (c_i : P_i) \to A \quad\text{and}\quad \nvdash \bigwedge_{i=1}^{n} (c_i : P_i) \to B.$$

By completeness for generated models, we find that there are factive generated CS-models $\mathfrak{M}^A$, $\mathfrak{M}^B$ with states w_A and w_B such that

$$(\mathfrak{M}^A, w_A) \nvDash \bigwedge_{i=1}^{n}(c_i : P_i) \to A \quad \text{and} \quad (\mathfrak{M}^B, w_B) \nvDash \bigwedge_{i=1}^{n}(c_i : P_i) \to B$$

which means that there are states $v_A \geq w_A$ and $v_B \geq w_B$ such that

$$(\mathfrak{M}^A, v_A) \vDash \bigwedge_{i=1}^{n} c_i : P_i \quad \text{and} \quad (\mathfrak{M}^A, v_A) \nvDash A$$

and

$$(\mathfrak{M}^B, v_B) \vDash \bigwedge_{i=1}^{n} c_i : P_i \quad \text{and} \quad (\mathfrak{M}^B, v_B) \nvDash B.$$

Now we consider the submodels of $\mathfrak{M}^A$ and $\mathfrak{M}^B$ generated by the points v_A and v_B, respectively. Call them $\mathfrak{M}^A_{v_A}$ and $\mathfrak{M}^B_{v_B}$. These models are factive CS-models; further they are trees with roots v_A and v_B and agree with the original models on all their states.

Next we construct a new model $\mathfrak{M}$ by

$$W := \{(0,0)\} \cup \{(1,a) \mid a \in W^A_{v_A}\} \cup \{(2,b) \mid b \in W^B_{v_B}\}$$

$$(x_1, y_1) \leq_{\mathfrak{M}} (x_2, y_2) :\Longleftrightarrow \begin{cases} x_1 = 0, \\ x_1 = x_2 = 1 \text{ and } y_1 \leq_A y_2, \\ x_1 = x_2 = 2 \text{ and } y_1 \leq_B y_2. \end{cases}$$

$$V(x,y) := \begin{cases} \{P_1, \ldots, P_n\}, \text{ if } (x,y) = (0,0), \\ V_A(y), \text{ if } x = 1, \\ V_B(y), \text{ if } x = 2. \end{cases}$$

and its basis is defined by

$$\mathcal{B}_{(x,y)} := \begin{cases} \{(c_1, P_1), \ldots, (c_n, P_n)\} \cup \mathsf{CS} \cup \\ \qquad\qquad \{(?_n, A) \mid A \text{ is of } ?_n\text{-form}\}, \text{ if } (x,y) = (0,0), \\ \mathcal{B}_{A,y}, \text{ if } x = 1, \\ \mathcal{B}_{B,y}, \text{ if } x = 2. \end{cases}$$

Claim: $\mathfrak{M}$ is a factive generated CS-model. We have to check that our glueing does not violate the monotonicity conditions on the valuation and on the basis. We have that

$$(\mathfrak{M}^A, v_A) \vDash c_i : P_i \quad \text{and} \quad (\mathfrak{M}^B, v_B) \vDash c_i : P_i \qquad \text{for } i = 1, \ldots, n,$$

which means

$$(c_i, P_i) \in \mathcal{E}(\mathcal{B}_{A,v_A}) \quad \text{and} \quad (c_i, P_i) \in \mathcal{E}(\mathcal{B}_{B,v_B}) \qquad \text{for } i = 1, \ldots, n. \tag{2}$$

It follows by Lemma 3.4 that

$$\{(c_i, P_i) \mid i = 1, \dots, n\} \subseteq \mathcal{B}_{A,v_A} \text{ and } \{(c_i, P_i) \mid i = 1, \dots, n\} \subseteq \mathcal{B}_{B,v_B}.$$

Hence $\mathcal{B}_{(0,0)} \subseteq \mathcal{B}_{(x,y)}$ for each $(x, y) \geq_{\mathfrak{M}} (0, 0)$, so the monotonicity for the basis is established.

Also the monotonicity condition for the valuation is satisfied. Indeed, since $\mathfrak{M}^A$ and $\mathfrak{M}^B$ are factive, (2) implies

$$(\mathfrak{M}^A, v_A) \vDash P_i \quad \text{and} \quad (\mathfrak{M}^B, v_B) \vDash P_i \qquad \text{for } i = 1, \dots, n.$$

Thus we find

$$V(0, 0) = \{P_1, \dots, P_n\} \subseteq V(x, y) \quad \text{if } (0, 0) \leq_{\mathfrak{M}} (x, y).$$

Last but not least observe that $\mathfrak{M}$ is factive since the new state $(0, 0)$ satisfies factivity by definition.

Now we show that $(\mathfrak{M}, (0, 0)) \nvDash (\bigwedge_{i=1}^n c_i : P_i) \to (A \vee B)$. By the definition of the basis of $\mathfrak{M}$ we immediately have

$$(\mathfrak{M}, (0, 0)) \vDash \bigwedge_{i=1}^{n} c_i : P_i.$$

By the monotonicity of $\leq_{\mathfrak{M}}$ we find $(\mathfrak{M}, (0, 0)) \nvDash A$ and $(\mathfrak{M}, (0, 0)) \nvDash B$, which implies $(\mathfrak{M}, (0, 0)) \nvDash A \vee B$. Therefore,

$$(\mathfrak{M}, (0, 0)) \nvDash (\bigwedge_{i=1}^{n} c_i : P_i) \to (A \vee B).$$

By soundness we get

$$\nvdash (\bigwedge_{i=1}^{n} c_i : P_i) \to (A \vee B)$$

and finally, by the deduction theorem,

$$\{c_1 : P_1, \dots, c_n : P_n\} \nvdash A \vee B$$

□

Now we can prove a first version of the internalized disjunction property, which we call *local*. It is local in the sense that it is shown semantically for a given state in the model and the term s depends on that state.

Lemma 7.2 (Local Internalized Disjunction Property) *Let* CS *be an axiomatically appropriate constant specification. Let* $\mathfrak{M}$ *be an atomic* CS*-model,* $w \in W$*. For each term* $t \in \mathsf{Tm}$ *and all formulas* A, B*, there exists a term* $s = s_{t,A,B,w}$ *such that*

$$(\mathfrak{M}, w) \vDash t : (A \vee B) \to (s : A \vee s : B)$$

Proof. Assume that $(\mathfrak{M}, w) \vDash t : A \vee B$. By the first part of the Connection Lemma 5.7 we get

$$\{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash t : A \vee B.$$

Using the axiom (t), we obtain

$$\{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash A \vee B.$$

By Lemma 5.6, the set $\mathrm{subf}(t : A \vee B)$ is finite. Hence by the disjunction property, Theorem 7.1, we get

$$\begin{array}{ll} \{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash A & \text{or} \\ \{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash B. & \end{array} \tag{3}$$

Assume that $\{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash A$, the other case being similar. We now apply the Lifting Lemma 2.6 to find an $s \in \mathsf{Tm}$ such that

$$\{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P\} \vdash s : A.$$

Therefore,

$$\{c : P \in \mathrm{subf}(t : A \vee B) \mid w \vDash c : P)\} \cup \{P \in \mathrm{subf}(t : A \vee B) \mid w \vDash P\} \vdash s : A$$

Using the second part of the Connection Lemma 5.7, we get $(\mathfrak{M}, w) \vDash s : A$. Finally, combining the two cases of (3) yields $(\mathfrak{M}, w) \vDash s : A \vee s : B$. □

The above version of the internalization propery is local in the sense that the term s depends on the world w. In the next lemma, we provide a global version of the internalized disjuction property, which does not have this dependency. In its proof, we make crucial use of the + operator to collect all possible justification terms for the disjuncts.

Lemma 7.3 (Global Internalized Disjunction Property) *Let* CS *be an axiomatically appropriate constant specification. For each term* $t \in \mathsf{Tm}$ *and all formulas* $A, B \in \mathsf{Fm}$*, there exists a term* $s \in \mathsf{Tm}$ *such that for each atomic* CS*-model* $\mathfrak{M}$ *and each* $w \in W$*:*

$$(\mathfrak{M}, w) \vDash t : (A \vee B) \to (s : A \vee s : B)$$

Proof. In the proof of the above lemma, the term s only depends on which of the (finitely many) $c_i : P_i \in \mathrm{subf}(t : (A \vee B))$ do hold at w. Hence there are finitely many terms $s_{A,1}, \ldots, s_{A,m}$ and $s_{B,1}, \ldots, s_{B,m}$ such that for each w there exists $1 \leq j \leq m$ with

$$(\mathfrak{M}, w) \vDash s_{A,j} : A \quad \text{or} \quad (\mathfrak{M}, w) \vDash s_{B,j} : B.$$

Therefore, for all w we have

$$(\mathfrak{M}, w) \vDash s_{A,1} : A \vee \cdots \vee s_{A,m} : A \quad \text{or} \quad (\mathfrak{M}, w) \vDash s_{B,1} : B \vee \cdots \vee s_{B,m} : B.$$

Now we let

$$s := s_{A,1} + \cdots + s_{A,m} + s_{B,1} + \cdots + s_{B,m}$$

and obtain that for all w,

$$(\mathfrak{M}, w) \vDash s : A \vee s : B.$$

$\square$

By completeness for atomic models, we immediately get the following corollary.

Corollary 7.4 (Internalized Disjunction Property) *Let* CS *be an axiomatically appropriate constant specification. For all formulas* $A, B \in \mathsf{Fm}$ *and all* $t \in \mathsf{Tm}$ *there exists* $s \in \mathsf{Tm}$ *such that*

$$\vdash t : (A \vee B) \to (s : A \vee s : B).$$

8 Conclusion and further work

We introduced the intuitionistic justification logic iJ, which is a light extension of $\mathsf{iJT4}$. We defined atomic models and established completeness of iJ with respect to that class of models. This made it possible to prove the internalized disjunction property for iJ.

Hirai [15] introduced an intuitionistic modal logic based on $\mathsf{S4}$ with the additional axiom

$$\square(A \vee B) \to (\square A \vee \square B),$$

which is the modal version of the internalized disjunction property. So it is a natural question whether we can realize his logic into iJ, i.e., given a modal formula A provable in Hirai's logic, is there a realization A^r provable in iJ where A^r is A with $\square$-operators replaced by suitable terms.

It turns out that such a realization is possible but it requires a heavy technical apparatus. First of all, we need a cut-free sequent system for Hirai's logic. Then we can perform Artemov's syntactic realization procedure to obtain the realization A^r. To do so, we need justification variables to realize $\square$-operators occurring in negative positions. However, this is problematic as we have observed in Remark 2.4. The solution is to add variables to the language but to keep the formulation for the axioms, i.e., axioms are stated only for variable free terms. Instead we define provability of a formula with variables as provability of all its (variable-free) substitution instances, i.e.,

$$\vdash A[x_1, \ldots, x_n] \quad :\Longleftrightarrow \quad \vdash A[t_1, \ldots, t_n] \text{ for all variable-free terms } t_1, \ldots, t_n.$$

The realization result will be published in full detail somewhere else.

References

[1] S. Artemov, *Justification awareness models*, in: S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science* (2018), pp. 22–36.

[2] S. N. Artemov, *Explicit provability and constructive semantics*, BSL **7** (2001), pp. 1–36.

[3] S. N. Artemov, *Unified semantics for modality and λ-terms via proof polynomials*, in: K. Vermeulen and A. Copestake, editors, *Algebras, Diagrams and Decisions in Language, Logic and Computation*, CSLI Lecture Notes **144**, CSLI Publications, Stanford, 2002 pp. 89–118.

[4] S. N. Artemov, *Justified common knowledge*, TCS **357** (2006), pp. 4–22.

[5] S. N. Artemov, *The logic of justification*, RSL **1** (2008), pp. 477–513.

[6] S. N. Artemov, *The ontology of justifications in the logical setting*, Technical Report TR–2011008, CUNY Ph.D. Program in Computer Science (2011).

[7] S. N. Artemov and R. Iemhoff, *The basic intuitionistic logic of proofs*, JSL **72** (2007), pp. 439–451.

[8] S. N. Artemov and E. Nogina, *Introducing justification into epistemic logic*, Journal of Logic and Computation **15** (2005), pp. 1059–1073.

[9] A. Baltag, B. Renne and S. Smets, *The logic of justified belief, explicit knowledge, and conclusive evidence*, APAL **165** (2014), pp. 49–81, published online in August 2013.

[10] P. Blackburn, M. de Rijke and Y. Venema, "Modal Logic," Cambridge Tracts in Theoretical Computer Science **53**, Cambridge University Press, 2002.

[11] S. Bucheli, R. Kuznets and T. Studer, *Justifications for common knowledge*, Applied Non-Classical Logics **21** (2011), pp. 35–60.

[12] S. Bucheli, R. Kuznets and T. Studer, *Realizing public announcements by justifications*, Journal of Computer and System Sciences **80** (2014), pp. 1046–1066.

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

[14] M. Fitting, *The logic of proofs, semantically*, APAL **132** (2005), pp. 1–25.

[15] Y. Hirai, *An intuitionistic epistemic logic for sequential consistency on shared memory*, in: *Proceedings of the 16th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, LPAR'10 (2010), pp. 272–289.
URL `http://dl.acm.org/citation.cfm?id=1939141.1939157`

[16] A. Kashev, "Justification with Nominals," Ph.D. thesis, University of Bern (2016).
URL `http://www.iam.unibe.ch/ltgpub/2016/kas16.pdf`

[17] I. Kokkinis, Z. Ognjanović and T. Studer, *Probabilistic justification logic*, in: S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science* (2016), pp. 174–186.

[18] R. Kuznets, S. Marin and L. Straßburger, *Justification logic for constructive modal logic*, IMLA 2017 - 7th Workshop on Intuitionistic Modal Logic and Applications (2017).
URL `https://hal.inria.fr/hal-01614707`

[19] R. Kuznets and T. Studer, *Justifications, ontology, and conservativity*, in: T. Bolander, T. Braüner, S. Ghilardi and L. Moss, editors, *Advances in Modal Logic, Volume 9*, College Publications, 2012 pp. 437–458.

[20] R. Kuznets and T. Studer, *Update as evidence: Belief expansion*, in: S. N. Artemov and A. Nerode, editors, *LFCS 2013*, LNCS **7734**, Springer, 2013 pp. 266–279.

[21] R. Kuznets and T. Studer, *Weak arithmetical interpretations for the logic of proofs*, Logic Journal of the IGPL (2016).

[22] M. Marti and T. Studer, *Intuitionistic modal logic made explicit*, IfCoLog Journal of Logics and their Applications **3** (2016), pp. 877–901.

[23] B. Renne, *Evidence elimination in multi-agent justification logic*, in: A. Heifetz, editor, *Theoretical Aspects of Rationality and Knowledge, Proceedings of the Twelfth Conference (TARK 2009)* (2009), pp. 227–236.

[24] G. Steren and E. Bonelli, *Intuitionistic hypothetical logic of proofs*, in: V. de Paiva, M. Benevides, V. Nigam and E. Pimentel, editors, *Proceedings of the 6th Workshop on Intuitionistic Modal Logic and Applications (IMLA 2013) in association with UNILOG 2013, Rio de Janeiro, Brazil, 7 April 2013*, number 300 in Electronic Notes in Theoretical Computer Science, Elsevier, 2014 pp. 89–103.

[25] T. Studer, *Lectures on justification logic* (2012), lecture notes.

[26] T. Studer, *Decidability for some justification logics with negative introspection*, Journal of Symbolic Logic **78** (2013), pp. 388–402.

Appendix

A Proof of Lemma 4.2

Lemma 4.2 (Invariance for Point-Generated Models) Let $\mathfrak{M}$ be a model, $w \in W$, and $\mathfrak{M}_w$ the model generated by w. Then we have for each formula $A \in \mathsf{Fm}$ and each $v \in W_w$:

$$(\mathfrak{M}, v) \vDash A \iff (\mathfrak{M}_w, v) \vDash A.$$

Proof. By induction on A.

(i) $A = \bot$. Follows immediately.

(ii) $A = P \in \mathsf{Prop}$. Then the claim follows immediately by the definition of V_w.

(iii) $A = B \wedge C$ or $A = B \vee C$. Then the claim follows immediately by the I.H.

(iv) $A = B \rightarrow C$. For the direction from left to right, assume that $(\mathfrak{M}, v) \vDash B \rightarrow C$. We have to show that $(\mathfrak{M}_w, v) \vDash B \rightarrow C$, so let $u \geq_w v$ with $(\mathfrak{M}_w, u) \vDash B$. We have that $u \in W_w$, so it follows by the I.H. that $(\mathfrak{M}, u) \vDash B$, so $(\mathfrak{M}, u) \vDash C$. Applying the I.H. again, we get that $(\mathfrak{M}_w, u) \vDash C$. Since u was arbitrary, it follows that $(\mathfrak{M}_w, v) \vDash B \rightarrow C$.

For the direction from right to left, assume that $(\mathfrak{M}_w, v) \vDash B \rightarrow C$. We have to show that $(\mathfrak{M}, v) \vDash B \rightarrow C$, so let $u \geq v$ with $(\mathfrak{M}, u) \vDash B$. Since $u \geq v \geq w$, it follows by the transitivity of $\leq$ that $u \geq w$, so by definition we have that $u \in W_w$. It follows by the I.H. that $(\mathfrak{M}_w, u) \vDash B$. It also follows that $u \geq_w v$, and therefore $(\mathfrak{M}_w, u) \vDash C$. Applying the I.H. again, we obtain $(\mathfrak{M}, u) \vDash C$. Since u was arbitrary, it follows that $(\mathfrak{M}, v) \vDash B \rightarrow C$.

(v) $A = t : B$. We just observe that since $\mathcal{B}(w)_v = \mathcal{B}_v$ for all $v \in W_w$, we have $\mathcal{E}(\mathcal{B}(w)_v) = \mathcal{E}(\mathcal{B}_v)$ for all $v \in W_w$. Then the claim follows immediately by the definition of truth in a model.

□

B Proof of Lemma 5.2

Lemma 5.2 Let CS be a constant specification and $\mathfrak{M}$ a factive CS-model. If $A \notin \mathsf{Prop}$, $c \in \mathsf{Const}$, and $(c, A) \notin \mathsf{CS}$, then for all states w of $\mathfrak{M}$,

$$(c, A) \notin \mathcal{B}_w.$$

Proof. If $A \notin \mathsf{Prop}$, $c \in \mathsf{Const}$, and $(c, A) \notin \mathsf{CS}$, then by definition, $\neg(c : A)$ is of $?_0$-form. By the definition of CS-basis, we have that

$$(?_0, \neg c : A) \in \mathcal{B}_w \subseteq \mathcal{E}(\mathcal{B}_w).$$

Since the model is factive, it follows that $(\mathfrak{M}, w) \vDash \neg c : A$. Thus $(\mathfrak{M}, w) \nvDash c : A$, which finally is

$$(c, A) \notin \mathcal{B}_w.$$

□

C Proof of Lemma 5.7

Lemma 5.7 (Connection Lemma) Let CS be a constant specification, $\mathfrak{M}$ an atomic model and $w \in W$. Then we have for all formulas $A, B \in \mathsf{Fm}$ and each term $t \in \mathsf{Tm}$

(i) $(\mathfrak{M}, w) \vDash t : A \quad \Longrightarrow \quad \{c : P \in \mathrm{subf}(t : A) \mid w \vDash c : P\} \vdash t : A.$

(ii) If $\mathfrak{M}$ is a CS-model, then
$\{c : P \in \mathrm{subf}(A) \mid w \vDash c : P\} \cup \{P \in \mathrm{subf}(A) \mid w \vDash P\} \vdash B \quad \Longrightarrow$ $(\mathfrak{M}, w) \vDash B$

Proof. First statement. By the truth definition,

$$(\mathfrak{M}, w) \vDash t : A \quad \Longleftrightarrow \quad (t, A) \in \mathcal{E}(\mathcal{B}_w)$$

so we proceed by induction on $\mathcal{E}(\mathcal{B}_w)$.

Base case. $(t, A) \in \mathcal{B}_w$. Since $\mathcal{B}$ is atomic, there are three subcases.

(i) (t, A) is of the form (c, P). Then the claim follows immediately.

(ii) (t, A) is of the form $(c, A) \in \mathsf{CS}$. Again, the claim follows immediately.

(iii) $(t, A) = (?_n, A)$ and A is of $?_n$-form. Again, the claim follows immediately.

Inductive step.

- $t = r + s$, and
$$(r, A) \in \mathcal{E}(\mathcal{B}_w) \quad \text{or} \quad (s, A) \in \mathcal{E}(\mathcal{B}_w)$$
It follows by the I.H. that
$$\{c : P \in \mathrm{subf}(r : A) \mid w \vDash c : P\} \vdash r : A$$
or
$$\{c : P \in \mathrm{subf}(s : A) \mid w \vDash c : P\} \vdash s : A$$
it follows that
$$\{c : P \in \mathrm{subf}(r + s : A) \mid w \vDash c : P\} \vdash r : A$$
or
$$\{c : P \in \mathrm{subf}(r + s : A) \mid w \vDash c : P\} \vdash s : A$$
it follows by propositional reasoning that
$$\{c : P \in \mathrm{subf}(r + s : A) \mid w \vDash c : P\} \vdash r : A \lor s : A.$$
and by the axiom (+) and some more propositional reasoning we get
$$\{c : P \in \mathrm{subf}(r + s : A) \mid w \vDash c : P\} \vdash (r + s) : A$$

- $t = s \cdot_B r$, and
$$(s, B \to A) \in \mathcal{E}(\mathcal{B}_w) \quad \text{and} \quad (r, B) \in \mathcal{E}(\mathcal{B}_w)$$

It follows by the I.H. that

$$\{c : P \in \mathrm{subf}(s : B \to A) \mid w \vDash c : P\} \vdash s : B \to A$$

and

$$\{c : P \in \mathrm{subf}(r : B) \mid w \vDash c : P\} \vdash r : B$$

and therefore by the axiom (j)

$$\{c : P \in \mathrm{subf}(s : B \to A) \cup \mathrm{subf}(r : B) \mid w \vDash c : P\}$$
$$\vdash (s \cdot_B r) : A$$

and since

$$\{c : P \in \mathrm{subf}(s : B \to A) \ \cup \ \mathrm{subf}(r : B)\} = \{c : P \in \mathrm{subf}((s \cdot_B r) : A)\}$$

we have that

$$\{c : P \in \mathrm{subf}(s \cdot_B r : A) \mid w \vDash c : P\} \vdash (s \cdot_B r) : A.$$

- $t = !s$, $A = s : B$, and
$$(s, B) \in \mathcal{E}(\mathcal{B}_w).$$
Then it follows by the I.H. that
$$\{c : P \in \mathrm{subf}(s : B) \mid w \vDash c : P\} \vdash s : B$$
so it follows by the axiom (!) that
$$\{c : P \in \mathrm{subf}(s : B) \mid w \vDash c : P\} \vdash !s : (s : B)$$
i.e.
$$\{c : P \in \mathrm{subf}(s : B) \mid w \vDash c : P\} \vdash t : A.$$

Second Statement. We proceed by induction on the derivation of B.

- B is an axiom. Then the claim follows by soundness.
- $B \in \{c : P \in \mathrm{subf}(A) \mid w \vDash c : P\} \cup \{P \in \mathrm{subf}(A) \mid w \vDash P\}$. Then the claim follows immediately.
- B is of the form $c : D$ with $(c, D) \in \mathsf{CS}$ and was derived by $(\mathrm{AN})_{\mathsf{CS}}$. Since $\mathfrak{M}$ is a CS-model, we have by definition that $\mathsf{CS} \subseteq \mathcal{B}_w \subseteq \mathcal{E}(\mathcal{B}_w)$, and therefore $(\mathfrak{M}, w) \vDash c : D$.
- B was derived by the rule $(?_n)$. Then $B = ?_n : C$ for some formula C of $?_n$-form. Again, since $\mathfrak{M}$ is a CS-model, we have that $(?_n, C) \in \mathcal{B}_w \subseteq \mathcal{E}(\mathcal{B}_w)$ and therefore $(\mathfrak{M}, w) \vDash ?_n : C$.

- B was derived by (MP). Then there is a formula C such that

$$\{c : P \in \mathrm{subf}(A) \mid w \vDash c : P\} \cup \{P \in \mathrm{subf}(A) \mid w \vDash P\} \vdash C$$

and

$$\{c : P \in \mathrm{subf}(A) \mid w \vDash c : P\} \cup \{P \in \mathrm{subf}(A) \mid w \vDash P\} \vdash C \to B$$

Then it follows by the I.H. (since these derivations are shorter) that

$$(\mathfrak{M}, w) \vDash C \to B \quad \text{and} \quad (\mathfrak{M}, w) \vDash C, \quad \text{so } (\mathfrak{M}, w) \vDash B.$$

□