Contributions to Intuitionistic Epistemic Logic

Inauguraldissertation
der Philosophisch-naturwissenschaftlichen Fakultät
der Universität Bern

vorgelegt von

Michel Marti

aus Ebersecken LU

Leiter der Arbeit:
Prof. Dr. Gerhard Jäger
Institut für Informatik

Contributions to Intuitionistic Epistemic Logic

Inauguraldissertation
der Philosophisch-naturwissenschaftlichen Fakultät
der Universität Bern

vorgelegt von

Michel Marti
aus Ebersecken LU

Leiter der Arbeit:
Prof. Dr. Gerhard Jäger
Institut für Informatik

Von der Philosophisch-naturwissenschaftlichen Fakultät angenommen.

Bern, den 4. April 2017

Der Dekan:
Prof. Dr. G. Colangelo

ISBN: 978-1-326-98481-6

Acknowledgements

I would like to thank Prof. Gerhard Jäger for his support and guidance. I would also like to thank Thomas Studer for introducing me to justification logics, and my colleagues for the many helpful and inspiring discussions.

Contents

Introduction

This thesis is about two kinds of (closely related) logics: Modal logics and justification logics, both based on intuitionistic propositional logic. Epistemology is the theory of knowledge, and epistemic logics are logics dealing with knowledge. A classical way to formally treat knowledge goes back to Hintikka [Hin62]. In this approach, modal logic is used as an epistemic logic, with "the agent i knows that" as the modality $\Box_i$ and a possible worlds semantics. Justification logics are a more recent addition to the logical landscape. In these logics, we can explicitly reason about an agents' evidence/justifications. Justification is a central epistemic concept as well, and justification logics are closely related to modal logics.

Accordingly, this thesis has two parts. The first part is about intuitionistic modal logics, the second about intuitionistic justification logics.

In the first chapter, we recall some soundness and completeness results about intuitionistic modal logic and fix notation and terminology. The logics **IK** and **IT** introduced here will serve as base logics that will later be extended by additional machinery, and the logic **IS4** will show up again in the justification logic part. The next two chapters are about extending these base logics with distributed knowledge $\mathbb{D}$ and common knowledge $\mathbb{C}$, respectively. For both these extensions, completeness will be shown using some canonical model constructions. In the case of distributed knowledge, we need to make a detour via so-called pseudo-models and strict pseudo-models. For common knowledge, we will have to work in a finite fragment and construct canonical models tailored to specific formulas.

Finally, we turn to intuitionistic justification logic. Using similar techniques as in the previous chapters, we show soundness and completeness for so-called basic modular models and modular models.

Part I.

Intuitionistic Modal Logic

Intuitionistic modal logic combines modal logic with intuitionistic propositional logic. For combining intuitionistic propositional logic with modal logic, there are several design choices to be made, and accordingly, there exist various approaches.

As two examples, Artemov and Protopopescu in [AP14] reject the axiom $\Box A \to A$, but instead argue for an axiom $A \to \Box A$, and Hirai [Hir10] uses a version with $\Box_i(A \vee B) \to \Box_i A \vee \Box_i B$. Other approaches are, for example, Williamson [Wil92] and Proietti [Pro12].

Our formalism starts off from a framework for intuitionistic modal logic presented in Fischer Servi [Fis84] and Plotkin and Stirling [PS86] and discussed from a broader perspective in Simpson [Sim94]. We extend its $\Box$-fragment to several agents. In the following chapters, we will extend our language with operators $\mathbb{D}$ for distributed knowledge and $\mathbb{C}$ for common knowledge.

1. Intuitionistic versions of K, T and S4

In this first chapter, we briefly discuss some systems of intuitionistic modal logic, mention some results from the literature and fix our notation. We will introduce the language $\mathcal{L}_K$ which can express statement about the knowledge of multiple agents, along with a proof system and a semantics. This logic will be extended to treat distributed knowledge and common knowledge in the following chapters.

In naming our logical systems, we follow the tradition in modal logics to keep the historical names of logics, like **S4**, and add an "I" for "intuitionistic". We will consider the intuitionistic variants of the classical systems **K**, **T** and **S4** and call them **IK**, **IT** and **IS4**. In this thesis, I will only treat modal logics with $\Box$-modalities.

1.1. The language $\mathcal{L}_K$ and its semantics

Definition 1.1 (The language $\mathcal{L}_K$)**.** Given a fixed but arbitrary natural number $\ell \geq 1$, the language $\mathcal{L}_K$ comprises the following primitive symbols:

(PS.1) Countably many atomic propositions p, q, r (possibly with subscripts); the collection of all atomic propositions is called Prop.

(PS.2) The logical constant $\bot$ and the logical connectives $\vee$, $\wedge$, and $\rightarrow$.

(PS.3) The modal operators $\Box_1, \ldots, \Box_\ell$.

Definition 1.2 (Formulas)**.** The *formulas* of $\mathcal{L}_K$ are inductively defined by:

(a) every atomic proposition is a formula;

(b) the constant symbol $\bot$ is a formula;

(c) If A and B are formulas, then $(A \wedge B)$, $(A \vee B)$ and $(A \to B)$ are formulas;

(d) if A is a formula, then $\Box_i A$ is a formula (for each $i = 1, \ldots, \ell$).

As is common in intuitionistic logic, we define negation $\neg A$ by $(A \to \bot)$ and equivalence $(A \leftrightarrow B)$ by $((A \to B) \wedge (B \to A))$. We often omit parentheses if there is no danger of confusion.

Given a set of formulas M we set

$$\Box_i M := \{\Box_i A \mid A \in M\} \quad \text{and} \quad \Box_i^{-1} M := \{A \mid \Box_i A \in M\}$$

and for a finite set of formulas $M = \{A_1, \ldots, A_n\}$ we set

$$\bigwedge M := \bigwedge_{i=1}^{n} A_i \quad \text{and} \quad \bigvee M := \bigvee_{i=1}^{n} A_i$$

Lemma 1.3.

$$M \subseteq N \implies \Box_i M \subseteq \Box_i N \quad \textit{and} \quad \Box_i^{-1} M \subseteq \Box_i^{-1} N.$$

Definition 1.4. An *epistemic Kripke structure (EK-structure for short) of order* ℓ is an $(\ell+3)$-tuple $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ with the following properties:

(EK.1) W is a nonempty set (the set of the so-called *worlds*, *states* or *points* of $\mathfrak{M}$) and $\leq$ is a preorder on W.

(EK.2) $R_i \subseteq W \times W$ for $i = 1, \ldots, \ell$ is a binary relation on W, called an *accessibility relation*, such that for any $w, v \in W$,

$$w \leq v \quad \implies \quad R_i[v] \subseteq R_i[w].$$

(EK.3) $V : W \to \mathcal{P}(\mathsf{Prop})$ is a function, called an *evaluation*, such that for any $w, v \in W$,

$$w \leq v \quad \implies \quad V(w) \subseteq V(v).$$

$\mathfrak{M}$ is called *a reflexive EK-structure* iff all relations $R_1, \ldots, R_\ell$ are reflexive, and called a *transitive EK-structure* iff all relations $R_1, \ldots, R_\ell$ are transitive. We will also speak of agent i for the i-th agent in the group. We call

an EK-structure a *single-agent* structure if $\ell = 1$. In this case, we simply write $\Box$ instead of $\Box_1$. Also, we often just call an EK-structure of order ℓ an EK-structure if its order is not relevant or clear from the context.

Following standard notation in modal logic, we will write wR_iv for $(w, v) \in R_i$ and set

$$R_i[w] := \{v \in W \mid wR_iv\}.$$

The accessibility relations R_i represent an agents' epistemic state: we can read wR_iv as : "at state w, the agent considers the state v to be a possible state of affairs, a possible scenario". Accordingly, $R_i[w]$ is the set of states accessible to the agent i, the set of world this agent considers possible from his viewpoint of the world w.

An agent's knowledge is then represented as follows: The agent knows A iff A is true in all worlds that he considers possible. Typically, knowledge is assumed to imply truth: We can not know things that are wrong (we can only falsely believe them). One may argue that for this reason, the logics **K** and **IK** are not really logics of knowledge, but (at best) of belief. Being aware of this, in this thesis we are more concerned with specific technical questions, so we put aside such considerations and always talk of knowledge and not of belief.

The condition (EK.2) ensures monotonicity for formulas of the form $\Box_i A$. Whenever agent i progresses along $\leq$, the collection of worlds that are accessible for i can go down, reflecting the fact that some worlds are ruled out as being accessible due to new information. If R_i is reflexive then all worlds v such that $w \leq v$ are accessible for agent i from w.

Definition 1.5 (Satisfaction)**.** We define the *satisfaction* (or *truth*) of a formula A at a point w in an EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$, written as $(\mathfrak{M}, w) \vDash A$, inductively as follows:

- $(\mathfrak{M}, w) \nvDash \bot$;
- $(\mathfrak{M}, w) \vDash p$ iff $p \in V(w)$;
- $(\mathfrak{M}, w) \vDash A \wedge B$ 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 $(\mathfrak{M}, v) \vDash A$;

- $(\mathfrak{M}, w) \vDash \Box_i A$ iff $(\mathfrak{M}, v) \vDash A$ for all $v \in R_i[w]$ for $i = 1, \ldots, \ell$.

If the EK-structure is clear form the context, we will write $w \vDash A$ for $(\mathfrak{M}, w) \vDash A$. Given an EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$, we write $\mathfrak{M} \vDash A$ if $(\mathfrak{M}, w) \vDash A$ for all $w \in W$, and given a an arbitrary but fixed number ℓ, we write $\vDash A$ for $\mathfrak{M} \vDash A$ for all EK-structures $\mathfrak{M}$ of order ℓ. We write $\vDash_{ref}$ and $\vDash_{ref,tr}$ for validity with respect to the classes of reflexive and reflexive as well as transitive EK-structures.

Definition 1.6 (Denotation)**.** We define the *denotation* of a formula A in an EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ as the set of worlds where it holds true:

$$\|A\|_{\mathfrak{M}} := \{w \in W \mid (\mathfrak{M}, w) \vDash A\}$$

This notion will be useful in the part about common knowledge, where we consider operators on sets of worlds. We will often write $\|A\|$ instead of $\|A\|_{\mathfrak{M}}$ if the model is clear from the context.

The following lemma summarizes some easy observations about the denotation of complex formulas.

Lemma 1.7 (Monotonicity)**.** *For each EK-structure* $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ *we have*

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

Proof. We proceed by induction on A.

- $A = \bot$ or $A \in \mathsf{Prop}$. Then the claim follows immediately.
- $A = B \wedge C$ or $A = B \vee C$. Then the claim follows immediately from the induction hypothesis.
- $A = B \to C$. Let $u \geq v$ such that $u \vDash B$. Since $\leq$ is transitive, we have that $u \geq w$, so it follows from the assumption $w \vDash B \to C$ that $u \vDash C$. Since u was arbitrary, it follows that $v \vDash B \to C$.
- $A = \Box_i B$. Since $w \vDash \Box_i B$, we have that $u \vDash B$ for each $u \in R_i[w]$. Since $w \leq v$, we have $R_i[v] \subseteq R_i[w]$, so $u \vDash B$ for each $u \in R_i[w]$, which means that $u \vDash \Box_i B$.

□

Lemma 1.8 (Facts about denotation)**.** *For each EK-structure* $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ *and all* $\mathcal{L}_K$*-formulas* A, B *and* C *we have*

(a) $\|A \wedge B\|_{\mathfrak{M}} = \|A\|_{\mathfrak{M}} \cap \|B\|_{\mathfrak{M}}$

(b) $\|A \vee B\|_{\mathfrak{M}} = \|A\|_{\mathfrak{M}} \cup \|B\|_{\mathfrak{M}}$

(c) $\|A \to B\|_{\mathfrak{M}} = \{w \in W \mid \{v \in W \mid w \leq v\} \cap \|A\|_{\mathfrak{M}} \subseteq \|B\|_{\mathfrak{M}}\}$

(d) $\|\Box_i A\|_{\mathfrak{M}} = \{w \in W \mid R_i[w] \subseteq \|A\|_{\mathfrak{M}}\}$

(e) $\|A \wedge B\|_{\mathfrak{M}} \subseteq \|C\|_{\mathfrak{M}} \iff \|A\|_{\mathfrak{M}} \subseteq \|B \to C\|_{\mathfrak{M}}$

(f) $W = \|B \to C\|_{\mathfrak{M}} \iff \|B\|_{\mathfrak{M}} \subseteq \|C\|_{\mathfrak{M}}$

Proof. The first four assertions follow immediately by the definitions. We proceed by showing the fifth assertion. For the direction from left to right, assume that $\|A \wedge B\|_{\mathfrak{M}} \subseteq \|C\|_{\mathfrak{M}}$, and let $w \in \|A\|_{\mathfrak{M}}$, so $w \vDash A$, and let $v \geq w$ with $v \vDash B$. By monotonicity, it follows that $v \vDash A$, so $v \vDash A \wedge B$, i.e. $v \in \|A \wedge B\|_{\mathfrak{M}}$. By our assumption, $v \in \|C\|_{\mathfrak{M}}$, i.e. $v \vDash C$. It follows that $w \vDash B \to C$,i.e. $w \in \|B \to C\|_{\mathfrak{M}}$. For the direction from right to left, assume that $\|A\|_{\mathfrak{M}} \subseteq \|B \to C\|_{\mathfrak{M}}$, and let $w \in \|A \wedge B\|_{\mathfrak{M}}$, i.e. $w \vDash A \wedge B$, so $w \vDash A$, so by our assumption $w \vDash B \to C$. Since we also have $w \vDash B$, it follows that $w \vDash C$, i.e. $w \in \|C\|_{\mathfrak{M}}$.
To show the sixth assertion, let A be a tautology. Then, using the previous result, we have

$$\begin{aligned} &\|B\|_{\mathfrak{M}} = \|A \wedge B\|_{\mathfrak{M}} \subseteq \|C\|_{\mathfrak{M}} \quad \overset{\text{(e)}}{\iff} \\ &W = \|A\|_{\mathfrak{M}} \subseteq \|B \to C\|_{\mathfrak{M}} \quad \iff \\ &W = \|B \to C\|_{\mathfrak{M}} \end{aligned}$$

□

Remark 1.9 (Metavariables). We will A, B, C, D for arbitrary formulas, M, N for sets of formulas and w, v, u for worlds, sometimes with subscripts.

1.2. The Hilbert systems IK, IT and IS4

The Hilbert system **IK** has the following axioms and rules:

- Axioms of intuitionistic propositional logic

- the K-axioms
$$\Box_i(A \to B) \to (\Box_i A \to \Box_i B) \qquad (\mathbf{K})$$
for each $i = 1, \ldots, \ell$, and the rules modus ponens and necessitation
$$\frac{A \qquad A \to B}{B}\ (\mathbf{MP}) \qquad \text{and} \qquad \frac{A}{\Box_i A}\ (\mathbf{NEC}).$$

The system **IT** has, in addition, the truth-axioms

$$\Box_i A \to A \qquad (\mathbf{T})$$

again for $i = 1, \ldots, \ell$. Finally, we obtain the system **IS4** by adding to **IT** the (4)-axioms

$$\Box_i A \to \Box_i \Box_i A \qquad (\mathbf{4})$$

As in classical modal logic, the truth axioms correspond to reflexivity and the (4)-axioms to transitivity of the accessibility relations.

We define provability in these Hilbert systems as usual:

Definition 1.10 (Provability from assumptions)**.** Let M be a set of formulas. We say that the formula A is *provable* or *derivable* from M in a given Hilbert system, written $M \vdash A$ (often with a subscript denoting the Hilbert system) iff there are finitely many formulas $A_1, \ldots, A_n \in M$ such that $\vdash A_1 \wedge \cdots \wedge A_n \to A$.

Let $\vdash$ denote provability in one of the systems **IK**, **IT** or **IS4**. As usual, the deduction theorem for each of these systems is an immediate consequence of our notion of provability.

Lemma 1.11 (Deduction Theorem)**.** *For all formulas A, B and all sets of formulas M (of the respective languge) we have:*

$$M \cup \{A\} \vdash B \quad \Longleftrightarrow \quad M \vdash A \to B.$$

Lemma 1.12 (Soundness of **IK**, **IT** and **IS4**)**.** *The systems* **IK**, **IT** *and* **IS4** *are sound w.r.to the appropriate class of models, i.e.*

(a) $\vdash_{\mathbf{IK}} A \implies \vDash A$

(b) $\vdash_{\mathbf{IT}} A \implies \vDash_{refl.} A$

(c) $\vdash_{\mathbf{IS4}} A \implies \vDash_{\textit{refl., trans.}} A$

Proof. By straightforward inductions on the derivations of A. We just check the validity of the **K**-axioms, the other cases are left to the reader. Let $\mathfrak{M}$ be an EK-structure and $w \in W$ with $w \vDash \Box_i(A \to B)$. We show that this implies $w \vDash \Box_i A \to \Box_i B$, from which the claim follows. So let $v \geq w$ such that $v \vDash \Box_i A$. By definition this means that $u \vDash A$ for all $u \in R_i[v]$. Since $w \vDash \Box_i(A \to B)$, it follows by monotonicity that $v \vDash \Box_i(A \to B)$, i.e. $u \vDash A \to B$ for all $u \in R_i[v]$, and therefore $u \vDash B$ for all $u \in R_i[v]$, so $u \vDash \Box_i B$. □

Definition 1.13. Given any proof system $\mathcal{S}$, let $\vdash$ denote provability in this system. We call a set of formulas P *$\mathcal{S}$-prime* iff it satisfies the following conditions:

(i) P has the disjunction property, i.e., $A \vee B \in P \implies A \in P$ or $B \in P$;

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

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

If the system is clear form the context, we will also simply speak of prime sets instead of $\mathcal{S}$-prime sets.

The following lemma will be needed to show the prime lemma, which in turn is the primary tool for the completeness proof via canonical models.

Lemma 1.14 (Disjunction Lemma)**.** *Let N be an arbitrary set of formulas, A, B and C be formulas, and let $\vdash$ denote provability in one of the systems* **IK**, **IT** *or* **IS4***. If*

$$N \cup \{A\} \vdash C \text{ and } N \cup \{B\} \vdash C, \text{ then } N \cup \{A \vee B\} \vdash C.$$

Proof. Assume that $N \cup \{A\} \vdash C$ and $N \cup \{B\} \vdash C$. By definition, there are finitely many formulas $A_1, \ldots, A_n \in N \cup \{A\}$ such that $\vdash A_1 \wedge \cdots \wedge A_n \to C$ and $B_1, \ldots, B_m \in N \cup \{B\}$ such that $\vdash B_1 \wedge \cdots \wedge B_m \to C$. W.l.o.g. we can assume that $A_i \neq A$ for all $i = 1, \ldots, n$, $B_j \neq B$ for all $j = 1, \ldots, m$ and

$$\vdash A_1 \wedge \cdots \wedge A_n \wedge A \to C \quad \text{and} \quad \vdash B_1 \wedge \cdots \wedge B_m \wedge B \to C.$$

By intuitionistic propositional logic we have for all formulas D, E and F

$$((D \to F) \wedge (E \to F)) \to (D \vee E \to F)$$

so it follows by propositional reasoning that

$$\vdash (A_1 \wedge \cdots \wedge A_n \wedge A) \vee (B_1 \wedge \cdots \wedge B_m \wedge B) \to C.$$

it follows that

$$\vdash (A_1 \wedge \cdots \wedge A_n \wedge B_1 \wedge \cdots \wedge B_m \wedge A) \vee (A_1 \wedge \cdots \wedge A_n \wedge B_1 \wedge \cdots \wedge B_m \wedge B) \to C.$$

Also, in intuitionistic logic we have the distributive laws, so it follows by propositional reasoning that

$$\vdash (A_1 \wedge \cdots \wedge A_n \wedge B_1 \wedge \cdots \wedge B_m) \wedge (A \vee B) \to C.$$

Since $A_1, \ldots, A_n, B_1, \ldots, B_m \in N$, it follows by definition that

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

□

Lemma 1.15. *For each $n \geq 1$ and all formulas $A_1, \ldots, A_n$ and B:*

$$\vdash A_i \to B \text{ for all } i = 1, \ldots, n \quad \Longrightarrow \quad \vdash \bigvee_{i=1}^{n} A_i \to B$$

Proof. Using induction on n and the lemma above.

$n = 1$: Immediately.

$n \to n+1$: Assume that $\vdash A_i \to B$ for all $i = 1, \ldots, n+1$. By I.H. it follows that $\vdash \bigvee_{i=1}^{n} A_i \to B$. Using the previous lemma with $N = \varnothing$, we get that $\vdash \bigvee_{i=1}^{n} A_i \vee A_{n+1} \to B$, which is what we had to show.

□

The following prime lemma describes a crucial property of prime sets. It holds for **IK**, **IT** as well as for **IS4**.

Lemma 1.16 (Prime lemma)**.** *Suppose that $N \nvdash B$ for some set of formulas N and some formula B. Then there exists a prime set P such that $N \subseteq P$ and $P \nvdash B$.*

Proof. Let $(A_n)_{n\in\mathbb{N}}$ be an enumeration of all formulas. Now we inductively define the sets N_n for each $n \in \mathbb{N}$:

$$N_0 := N,$$

$$N_{n+1} := \begin{cases} N_n \cup \{A_n\} & \text{if } N_n \cup \{A_n\} \nvdash B, \\ N_n & \text{if } N_n \cup \{A_n\} \vdash B. \end{cases}$$

and finally

$$P := \bigcup_{n\in\mathbb{N}} N_n$$

Now we show by induction on n that for all $n \in \mathbb{N} : N_n \nvdash B$ and, therefore, $P \nvdash B$.

$n = 0$. Then $N_0 = N \nvdash B$ by assumption.

$n \to n + 1$. We proceed by the following case distinction.

1.case: $N_n \cup \{A_n\} \nvdash B$. Then by definition $N_{n+1} = N_n \cup \{A_n\} \nvdash B$.

2.case: $N_n \cup \{A_n\} \vdash B$. Then $N_{n+1} = N_n$, and by I.H. we have $N_n \nvdash B$.

It remains to show that P is prime. We have the following:

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

  $$P \vdash A \text{ but } A \notin P$$

  Since $P \vdash A$ but $P \nvdash B$, we know that

  $$P \cup \{A\} \nvdash B$$

  Otherwise, by the Deduction Theorem 3.41

  $$P \vdash A \to B \text{ and } P \vdash A$$

so by propositional reasoning,

$$P \vdash B, \text{ which contradicts our observation above.}$$

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,

$$A = A_i \in N_{i+1} \subseteq P,$$

which contradicts our assumption.

- P has the disjunction property: Assume that $C \vee D \in P$. 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

  $$P = P \cup \{C \vee D\} \nvdash B$$

  By the lemma above it follows that

  $$P \cup \{C\} \nvdash B \text{ or } P \cup \{D\} \nvdash B$$

  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 $C \in P$. The second case is analogous. □

Remark 1.17. We will use several versions of this lemma: for **IK**, **IT**, **IS4**,

for the logics with distributed knowledge **IDK** and **IDT**, and for a logic of common knowledge **ICK**. Inspecting the proof of this lemma, we see that the modal logic in question plays no role in the proof, so essentially the same proof works for all intuitionistic modal logics, and for intuitionistic justification logics as well. The prime lemma really just depends on the underlying propositional logic, in our case intuitionistic propositional logic.

Remark 1.18. In the following, we will use P, Q, R (possibly with subscripts) to denote prime sets of formulas of the relevant language.

Now we introduce syntactic EK-structures that are based on prime sets, which will serve as the worlds of the canonical models. This is a standard approach to proving completeness of intuitionistic modal systems also used in, for example, Fischer Servi [Fis84] and Simpson [Sim94].

Definition 1.19 (Canonical model for **IK**)**.** The *canonical model for* **IK** is the $(\ell + 3)$ tuple

$$\mathfrak{C} \;=\; (\mathcal{W}, \subseteq, \mathcal{R}_1, \ldots, \mathcal{R}_\ell, \mathcal{V}),$$

where we define:

(Can.1) $\mathcal{W} \;:=\; \{P \mid P \text{ is an } \mathbf{IK}\text{-prime set of formulas}\}$,

(Can.2) $P \,\mathcal{R}_i\, Q \;:\Longleftrightarrow\; \Box_i^{-1} P \subseteq Q \quad$ for $i = 1, \ldots, \ell$,

(Can.3) $\mathcal{V} : \mathcal{W} \to \mathcal{P}(\mathsf{Prop})$ is the function given by

$$\mathcal{V}(Q) \;:=\; \{p \in \mathsf{Prop} \mid p \in Q\} = \mathsf{Prop} \cap Q$$

It is easy to check that $\mathfrak{C}$ is an EK-structure of order ℓ.

Lemma 1.20. *The canonical model $\mathfrak{C}$ is an EK-structure of order ℓ.*

Proof. We have to check the three conditions (EK.1), (EK.2) and (EK.3) on EK-structures.

(EK.1) Since $\nvdash_{\mathbf{ICK}} \bot$, it follows by the prime lemma 1.16 that there is a prime set P. So $\mathcal{W} \neq \varnothing$. Also, the relation $\subseteq$ is a preorder on $\mathcal{W}$.

(EK.2) Let $P \subseteq Q$. We have to show that $\mathcal{R}_i[Q] \subseteq \mathcal{R}_i[P]$, so let $R \in \mathcal{R}_i[Q]$ which means that $Q \mathcal{R}_i R$ which by definition is $\Box_i^{-1} Q \subseteq R$. Since $P \subseteq Q$, it follows by lemma 1.3 that $\Box_i^{-1} P \subseteq \Box_i^{-1} Q$ and therefore $\Box_i^{-1} P \subseteq R$, i.e. $P \,\mathcal{R}_i\, R$ i.e. $R \in \mathcal{R}_i[P]$.

(EK.3) Assume that $P \subseteq Q$. Then we have

$$\mathcal{V}(P) = \mathsf{Prop} \cap P \subseteq \mathsf{Prop} \cap Q = \mathcal{V}(Q).$$

□

Lemma 1.21 (Truth lemma for **IK**). *Let* $\mathfrak{C} = (\mathcal{W}, \subseteq, \mathcal{R}_1, \ldots, \mathcal{R}_\ell, \mathcal{V})$ *be the canonical model for* **IK**. *Then we have for all* A *and all* $P \in \mathcal{W}$ *that*

$$A \in P \quad \Longleftrightarrow \quad (\mathfrak{C}, P) \vDash A.$$

Proof. We establish this equivalence by induction on the structure of A and distinguish the following cases.

(i) It trivially holds in case that A is the logical constant $\bot$ or an atomic proposition.

(ii) $A = B \wedge C$. Assume that $B \wedge C \in P$. Since P is deductively closed, we have $B \in P$ and $C \in P$, so it follows by the induction hypothesis that $(\mathfrak{C}, P) \vDash B$ and $(\mathfrak{C}, P) \vDash C$.

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

(iii) $A = B \vee C$. Assume that $B \vee C \in P$. Since P has the disjunction property, it follows that $B \in P$ or $C \in P$, so by the induction hypothesis, $(\mathfrak{C}, P) \vDash B$ or $(\mathfrak{C}, P) \vDash C$, so $(\mathfrak{C}, P) \vDash B \vee C$.

For the other direction assume that $(\mathfrak{C}, P) \vDash B \vee C$. Then

$$(\mathfrak{C}, P) \vDash B \text{ or } (\mathfrak{C}, P) \vDash C,$$

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

(iv) A is of the form $B_1 \to B_2$. We first assume that

$$B_1 \to B_2 \in P, \qquad P \subseteq Q \in \mathcal{W}, \qquad \text{and} \qquad (\mathfrak{C}, Q) \vDash B_1.$$

Then we have $B_1 \to B_2 \in Q$ and (by the induction hypothesis) $B_1 \in Q$. Since Q is deductively closed, this yields $B_2 \in Q$ and

thus again by the induction hypothesis that $(\mathfrak{C}, Q) \models B_2$. Q has been an arbitrary superset of P within $\mathcal{W}$, and thus we conclude $(\mathfrak{C}, P) \models B_1 \to B_2$.

Now assume $(\mathfrak{C}, P) \models B_1 \to B_2$ and $B_1 \to B_2 \notin P$. Since P is deductively closed, we have $P \cup \{B_1\} \nvdash_{\mathbf{IK}} B_2$. By the prime lemma there exists a prime $Q \in \mathcal{W}$ such that

$$P \cup \{B_1\} \subseteq Q \qquad \text{and} \qquad Q \nvdash_{\mathbf{IK}} B_2, \quad \text{hence} \quad B_2 \notin Q.$$

Together with the induction hypothesis we thus obtain

$$(\mathfrak{C}, Q) \models B_1 \qquad \text{and} \qquad (\mathfrak{C}, Q) \not\models B_2.$$

Since $P \subseteq Q$, this contradicts $(\mathfrak{C}, Q) \models B_1 \to B_2$.

(v) A is of the form $\Box_i B$. For the direction from left to right assume

$$\Box_i B \in P \qquad \text{and} \qquad \Box_i^{-1} P \subseteq Q$$

for an arbitrary $Q \in \mathcal{W}$. This implies $B \in Q$, and in view of the induction hypothesis we thus have $(\mathfrak{C}, Q) \models B$. Therefore, $(\mathfrak{C}, P) \models \Box_i B$.

For the converse direction we assume $(\mathfrak{C}, P) \models \Box_i B$. We first claim that

$$\Box_i^{-1} P \vdash_{\mathbf{IK}} B. \tag{*}$$

To establish this claim, assume for a contradiction that $\Box_i^{-1} P \nvdash_{\mathbf{IK}} B$. According to the prime lemma we thus have a $Q \in \mathcal{W}$ such that $\Box_i^{-1} P \subseteq Q$ and $Q \nvdash_{\mathbf{IK}} B$. In particular, $B \notin Q$. By the induction hypothesis, this yields $(\mathfrak{C}, Q) \not\models B$; a contradiction to $(\mathfrak{C}, P) \models \Box_i B$ and $\Box_i^{-1} P \subseteq Q$.

From (*) we conclude that there are $C_1, \ldots, C_n \in \Box_i^{-1} P$ such that

$$\vdash_{\mathbf{IK}} C_1 \wedge \cdots \wedge C_n \to B.$$

Using necessitation, we have

$$\vdash_{\mathbf{IK}} \Box_i (C_1 \wedge \cdots \wedge C_n \to B)$$

and by using the K-axioms and propositional reasoning we get

$$\vdash_{\mathbf{IK}} \Box_i C_1 \wedge \cdots \wedge \Box_i C_n \to \Box_i B,$$

with $\Box_i C_1, \ldots, \Box_i C_n \in P$, implying that $P \vdash_{\mathbf{IK}} \Box_i B$. Hence $\Box_i B \in P$ since P is deductively closed.

□

For the systems **IT** and **IS4**, we proceed similarly, using the corresponding notions of derivability and prime set and checking in addition that the resulting canonical models are reflexive resp. reflexive and transitive.

Lemma 1.22 (Completeness of **IK**, **IT** and **IS4**)**.** *The systems* **IK**, **IT** *and* **IS4** *are complete w.r.to the appropriate classes of models, i.e.*

(a) $\vDash A \implies \vdash_{\mathbf{IK}} A$

(b) $\vDash_{ref} A \implies \vdash_{\mathbf{IT}} A$

(c) $\vDash_{ref,tr} A \implies \vdash_{\mathbf{IS4}} A$

Proof. We only show the first assertion and proceed by contraposition. Assume that $\nvdash_{\mathbf{IK}} A$. By the prime lemma for **IK**, there exists a prime set P such that

$$P \nvdash_{\mathbf{IK}} A$$

in particular, $A \notin P$. It follows by the truth lemma that

$$(\mathfrak{C}, P) \nvDash A,$$

which implies that $\nvDash A$.
The other assertions are shown similarly, using the respective versions of the prime lemma, canonical model and truth lemma. □

1.3. Comparison with previous approaches

In the last part of this first general chapter on intuitionistic modal logics, we compare our semantics to some common approaches in the literature, in particular that of Fischer Servi, Plotkin and Stirling, and Simpson. The material of this section is based on [JM16b]. The mentioned

authors impose certain restrictions on their frames to deal with the interplay between $\Box$- and $\Diamond$-formulas. Since we work in multi-agent versions of the $\Box$-fragment, we do not need these frame conditions. Intuitionistic logic requires monotonicity, and in Fischer Servi [Fis84], Plotkin and Stirling [PS86], and Simpson [Sim94] this is done by building it into the truth definition. To make this distinction precise, we call an $(\ell+3)$-tuple $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ a *pre-EK-structure* iff it satisfies the properties (EK.1) and (EK.3) of an EK-structure; i.e. the monotonicity condition (EK.2) is dropped. Hence pre-EK-structures correspond to multi-agent versions of the structures considered in [Fis84, PS86, Sim94]. For a pre-EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$, the notion of truth in the sense of Fischer Servi, Plotkin and Stirling, and Simpson is inductively defined in analogy to truth for EK- structures on page 9 with the only difference that now, for a pre-EK-structure $\mathfrak{M}$,

$$(\mathfrak{M}, w) \vDash^\star \Box_i A : \iff (\mathfrak{M}, u) \vDash^\star A \quad \text{for all } u \in \bigcup_{w \leq v} R_i[v]$$

These semantic differences are not substantial, however: We are now going to show that the corresponding notions of validity coincide.

Lemma 1.23. *For each EK-structure $\mathfrak{M}$, each $w \in W$ and each formula A*

$$(\mathfrak{M}, w) \vDash A \iff (\mathfrak{M}, w) \vDash^\star A$$

Proof. We proceed by induction on A. The only interesting case is when $A = \Box_i B$. Then we have
$w \vDash \Box_i B \overset{\text{def}}{\iff} u \vDash B$ for all $u \in R_i[w] \overset{I.H.}{\iff} u \vDash^\star B$ for all $u \in R_i[w]$. Now we observe that since have $w \leq v \Longrightarrow R_i[v] \subseteq R_i[w]$, it follows that

$$\bigcup_{v \leq w} R_i[w] \subseteq R_i[v] \quad \text{and therefore} \quad \bigcup_{v \leq w} R_i[w] = R_i[v]$$

so we have $u \vDash^\star B$ for all $u \in R_i[w] \iff u \vDash^\star B$ for all $u \in \bigcup_{w \leq v} R_i[v] \overset{\text{def}}{\iff} u \vDash^\star \Box_i B$. □

Clearly, there are pre-EK-structures that are not EK-structures. However, it easy to transform them into EK-structures that validate the same formulas.

Definition 1.24 (Completion of a pre-EK structure)**.** Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be a pre-EK structure. Its *completion* $\mathfrak{M}^\uparrow$ is defined as the structure

$$\mathfrak{M}^\uparrow := (W, \leq, R_1^\uparrow, \ldots, R_\ell^\uparrow, V) \quad \text{with} \quad R_i^\uparrow[w] := \bigcup_{w \leq v} R_i[v]$$

Forming the completion of a pre-EK-structure turns it into an EK-structure.

Lemma 1.25. *For each pre-EK-structure $\mathfrak{M}$, its completion $\mathfrak{M}^\uparrow$ is an EK-structure.*

Proof. We only have to check that if $w \leq v$, then $R_i^\uparrow[v] \subseteq R_i^\uparrow[w]$ for each $i = 1, \ldots, \ell$. Since $w \leq v$, we have $\{u \in W \mid v \leq u\} \subseteq \{u \in W \mid w \leq u\}$ and therefore

$$R_i^\uparrow[v] = \bigcup_{v \leq u} R_i[u] \subseteq \bigcup_{w \leq u} R_i[u] = R_i^\uparrow[w].$$

□

Corollary 1.26. *The two notions of validity $\vDash$ and $\vDash^\star$ are equivalent, i.e. for each formula A of $\mathcal{L}_K$ we have*

$$\vDash A \quad \Longleftrightarrow \quad \vDash^\star A$$

Proof. Assume that $\nvDash A$, so there is an EK-structure $\mathfrak{M}$ and a point w of $\mathfrak{M}$ such that $(\mathfrak{M}, w) \nvDash A$. By the previous lemmas, $\mathfrak{M}$ is also a pre-EK-structure and $(\mathfrak{M}, w) \nvDash^\star A$ and therefore $\nvDash^\star A$. For the other direction assume that $\nvDash^\star A$, so there is a pre-EK-structure $\mathfrak{M}$ and a point w of $\mathfrak{M}$ such that $(\mathfrak{M}, w) \nvDash^\star A$. By the lemmas above, we have that $\mathfrak{M}^\uparrow$ is an EK-structure and $(\mathfrak{M}^\uparrow, w) \nvDash A$, so $\nvDash A$. □

Since pre-EK-validity for $\mathcal{L}_K$ formulas is the same as validity defined by Fischer Servi, Plotkin and Stirling, and Simpson, our semantics for intuitionistic common knowledge builds on established semantic concepts.

2. Distributed Knowledge

In this chapter, we extend our modal language $\mathcal{L}_K$ by the modality $\mathbb{D}$ for distributed knowledge. We will show soundness and completeness for two logics of intuitionistic distributed knowledge. The results of this chapter are based on [JM16a].

Roughly, A is distributed knowledge in a group of agents if the agents could come to know A when they would combine their individual knowledge. Distributed knowledge is, so to speak, "distributed in the group of agents". Alternatively, one can think of distributed knowledge as the knowledge of a "wise man" who knows everything that the agents in the group know.

The way this is modelled in Kripke models can be thought of as follows: The group considers a world possible only if all the agents consider it possible. Put differently, the group of agents rejects all worlds as possible that (at least) one of the agents rejects. In this way they combine their ability to exclude worlds, which corresponds to them combining their knowledge.

Some authors consider operators $\mathbb{D}_G$ for each subgroup $G \subseteq \{1, \dots, \ell\}$ of the agents. We restrict ourselves to the modality $\mathbb{D}$ which corresponds to $\mathbb{D}_{\{1,\dots,\ell\}}$, that is, knowledge which is distributed in the whole group of agents.

2.1. The language $\mathcal{L}_{DK}$ and its semantics

The language $\mathcal{L}_{DK}$ is obtained from adding the modal operator $\mathbb{D}$ to the language $\mathcal{L}_K$, and we extend the inductive definition of the set of formulas by

$$\text{if } A \text{ is a formula of } \mathcal{L}_{DK}, \text{ so is } \mathbb{D}A.$$

As for the modal operators $\Box_1, \dots, \Box_\ell$, we set, for any set of formulas M,

$$\mathbb{D}M := \{\mathbb{D}A \mid A \in M\} \quad \text{and} \quad \mathbb{D}^{-1}M := \{A \mid \mathbb{D}A \in M\}$$

Given the EK-structure of order ℓ

$$\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V),$$

A is considered to be distributed knowledge in world w iff A holds in those worlds that are accessible for all agents $1, \ldots, \ell$ from w.

We extend the definition of satisfaction at a point of a model by the following clause:

Definition 2.1 (Satisfaction)**.** We extend the satisfaction / truth definition for EK-structures by

$$(\mathfrak{M}, w) \vDash \mathbb{D}A \quad \text{iff} \quad (\mathfrak{M}, v) \vDash A \ \text{ for all } v \in \bigcap_{i=1}^{n} R_i[w]$$

We briefly check that adding the $\mathbb{D}$ operator does not violate our monotonicity condition.

The next lemma states the monotonicity for formulas of the form $\mathbb{D}A$.

Lemma 2.2. *For all EK-structures $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ of order ℓ, all elements $w, v \in W$, and all formulas A of $\mathcal{L}_{DK}$ we have that*

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

Proof. Assume that $(\mathfrak{M}, w) \vDash \mathbb{D}A$ and $w \leq v$. Now let $u \in \bigcap_{i=1}^{\ell} R_i[v]$. Since $R_i[v] \subseteq R_i[w]$ for all $i = 1, \ldots, \ell$, it follows that $\bigcap_{i=1}^{\ell} R_i[v] \subseteq \bigcap_{i=1}^{\ell} R_i[w]$ and therefore $u \in \bigcap_{i=1}^{\ell} R_i[w]$, so by our assumption we have $(\mathfrak{M}, u) \vDash A$ and therefore $(\mathfrak{M}, v) \vDash \mathbb{D}A$. □

It follows that we still have monotonicity.

Lemma 2.3 (Monotonicity for intuitionistic distributed knowledge)**.** *For every formula A of $\mathcal{L}_{DK}$ we have that*

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

Proof. By a simple induction on A. The only interesting case is when $A = \mathbb{D}B$, which is treated in the lemma above. □

2.2. The Hilbert systems IDK and IDT

We now introduce the Hilbert system **IDK**. It has all the axioms and rules of inference of the system **IK** for the extended language $\mathcal{L}_{DK}$, and in addition the following two axioms:

$$\mathbb{D}(A \to B) \to (\mathbb{D}A \to \mathbb{D}B), \tag{\textbf{D1}}$$

$$\Box_i A \to \mathbb{D}A, \tag{\textbf{D2}}$$

always for all $i = 1, \ldots, \ell$ and all formulas A, B of $\mathcal{L}_{DK}$. Because of (**D1**) the operator $\mathbb{D}$ is normal, which means that distributed knowledge is closed under logical inference. Also, in view of (**D2**) anything known by any agent is distributed knowledge.

Because of (**D2**) and (**NEC**) the necessitation rule for $\mathbb{D}$

$$\frac{A}{\mathbb{D}A}$$

is derivable in **IDK** : Assume that $\vdash_{\mathbf{IDK}} A$. Then by necessitation $\vDash \Box_i A$. By **D2** we have $\vDash \Box_i A \to \mathbb{D}A$, so by modus ponens we have $\vdash_{\mathbf{IDK}} \mathbb{D}A$.

The axioms **D1** and **D2** are EK-valid, which follows from the intersection-interpretation of $\mathbb{D}$. This is shown in the following two lemmas.

Lemma 2.4 (Validity of **D1**)**.** *For all formulas A and B we have*

$$\vDash \mathbb{D}(A \to B) \to (\mathbb{D}A \to \mathbb{D}B)$$

Proof. Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be an EK-structure, $w \in W$ and assume that $w \vDash \mathbb{D}(A \to B)$. We show that this implies $w \vDash \mathbb{D}A \to \mathbb{D}B$. So let $v \geq w$ with $v \vDash \mathbb{D}A$, and let $u \in \bigcap_{i=1}^{\ell} R_i[v]$. It follows by definition that $u \vDash A$. Since $w \leq v$, we have $R_i[v] \subseteq R_i[w]$ for each $i = 1, \ldots, \ell$, and therefore $\bigcap_{i=1}^{\ell} R_i[v] \subseteq \bigcap_{i=1}^{\ell} R_i[w]$. So $u \in \bigcap_{i=1}^{\ell} R_i[w]$ and therefore $u \vDash A \to B$, and finally $u \vDash B$. By definition, we have $v \vDash \mathbb{D}B$, so we have shown $w \vDash \mathbb{D}A \to \mathbb{D}B$. We have shown that for each $w \in W$, $w \vDash \mathbb{D}(A \to B)$ implies $w \vDash \mathbb{D}A \to \mathbb{D}B$. It follows that for each $w \in W$ we have $w \vDash \mathbb{D}(A \to B) \to (\mathbb{D}A \to \mathbb{D}B)$. □

Lemma 2.5 (Validity of **D2**)**.** *For all formulas A and all $i = 1, \ldots, \ell$ we*

have

$$\vDash \Box_i A \to \mathbb{D}A$$

Proof. Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be an EK-structure, $w \in W$ and $i \in \{1, \ldots, \ell\}$. Assume that $w \vDash \Box_i A$. By definition we have $v \vDash A$ for all $v \in R_i[w]$. Since $\bigcap_{i=1}^{\ell} R_i[w] \subseteq R_i[w]$ for each $i = 1, \ldots, \ell$, it follows that $v \vDash A$ for each $v \in \bigcap_{i=1}^{\ell} R_i[w]$, so by definition $w \vDash \mathbb{D}A$. It follows that $w \vDash \Box_i A \to \mathbb{D}A$ for each $w \in W$ and each $i = 1, \ldots, \ell$. □

The theory **IDT** is obtained from **IDK** by adding the truth axiom for distributed knowledge which states that the distributed knowledge of A implies A, i.e.,

$$\mathbb{D}A \to A \qquad (\mathbf{T})$$

for all A. In view of (**D2**) this implies the truth property $\Box_i A \to A$ for all operators $\Box_i$.

As for individual knowledge $\Box_i$, one could argue that the truth axiom is needed for distributed knowledge, and that **IDK** is at best a theory of distributed belief (which may be an interesting concept in itself) than of distributed knowledge. Again, we put such considerations aside and speak of distributed knowledge only.

Those EK-structures of order ℓ in which all (**T**)-axioms are valid are called *(**T**)-models*. The intended structures for **IDT** are reflexive EK-structures, and (**T**) is obviously valid in those. However, there are non-reflexive EK-structures of order ℓ in which all (**T**)-axioms are valid.

Lemma 2.6. *Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be a reflexive EK-structure. Then*

$$(\mathfrak{M}, w) \vDash \mathbb{D}A \to A.$$

Proof. Let w be a point of $\mathfrak{M}$ with $w \vDash \mathbb{D}A$. We show that $w \vDash A$, from which the claim follows. By definition, $w \vDash \mathbb{D}A$ means that $v \vDash A$ for all $v \in \bigcap_{i=1}^{\ell} R_i[w]$. Since R_i is reflexive for each $i = 1, \ldots, \ell$, we have $w \in R_i[w]$ for each $i = 1, \ldots, \ell$, so $w \in \bigcap_{i=1}^{\ell} R_i[w]$ and therefore $w \vDash A$. □

We can now easily show the soundness of our systems **IDK** and **IDK**.

Theorem 2.7 (Soundness of **IDK** and **IDT**)**.** *For all formulas A of $\mathcal{L}_{DK}$ we have:*

(a) $\vdash_{\mathbf{IDK}} A \implies \vDash A$.

(b) $\vdash_{\mathbf{IDT}} A \implies \vDash_{ref} A$.

Proof. By straightforward inductions on the derivations of A. The cases where A is an axiom **D1** or **D2** is covered by the two previous lemmas. □

As mentioned above, there exist non-reflexive (**T**)-models. Nevertheless, validity of (**T**) in EK-structures is closely related to reflexivity, as shown in the following lemma. First we define the reflexive extension of a model, which just replaces all accessibility relations with their reflexive closures.

Definition 2.8. Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be an EK-structure of order ℓ. The *reflexive extension* $\overline{\mathfrak{M}}$ of $\mathfrak{M}$ is defined to be the structure

$$(W, \leq, \overline{R}_1, \ldots, \overline{R}_\ell, V),$$

where (for $1 = 1, \ldots, \ell$) the relation $\overline{R}_i$ is defined to be the reflexive closure of R_i, i.e.,

$$\overline{R}_i := R_i \cup \{(w, w) \mid w \in W\}$$

It is an easy observation that any (**T**)-model can be extendend to a reflexive EK-structure of the same order.

Lemma 2.9. *If $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ is a (**T**)-model, then $\overline{\mathfrak{M}}$ is a reflexive EK-structure, and for all worlds $w \in W$ and all formulas A we have that*

$$(\overline{\mathfrak{M}}, w) \vDash A \iff (\mathfrak{M}, w) \vDash A.$$

Proof. The reflexivity of $\overline{\mathfrak{M}}$ is clear. The second part is proved by induction on A. If A is the logical constant $\bot$ or an atomic proposition, the assertion is obvious; if A is a disjunction, a conjunction, or an implication it follows directly from the induction hypothesis. Hence we can concentrate on the cases that A is of the form $\Box_i B$ or $\mathbb{D}B$.

(i) Let A be the formula $\Box_i B$. The direction from left to right is evident. So asssume $(\mathfrak{M}, w) \vDash \Box_i B$, from which we obtain

$$(\mathfrak{M}, v) \vDash B \quad \text{for all } v \in R_i[w].$$

$\mathfrak{M}$ is a (**T**)-model, thus $\Box_i B \to B$ is valid in $\mathfrak{M}$ and our assumption also yields $(\mathfrak{M}, w) \vDash B$. From the induction hypothesis we obtain $(\overline{\mathfrak{M}}, u) \vDash B$ for all $u \in R_i[w] \cup \{w\} = \overline{R}_i[w]$. Therefore, $(\overline{\mathfrak{M}}, w) \vDash \Box_i B$.

(ii) Let A be the formula $\mathbb{D}B$. The direction from left to right is evident again. To show the converse direction, let $(\mathfrak{M}, w) \vDash \mathbb{D}B$. Hence we have

$$(\mathfrak{M}, v) \vDash B \quad \text{for all } v \in \bigcap_{i=1}^{\ell} R_i[w].$$

Since $\mathfrak{M}$ is a (**T**)-model, we also have $(\mathfrak{M}, w) \vDash B$. Hence the induction hypothesis implies $(\overline{\mathfrak{M}}, u) \vDash B$ for all $u \in \bigcap_{i=1}^{\ell} R_i[w] \cup \{w\} = \bigcap_{i=1}^{\ell} \overline{R}_i[w]$. This is what we had to show. □

In order to avoid a trivial situation, we will assume in this section that $\ell \geq 2$. In the case where $\ell = 1$, the notion of distributed knowledge is trivial in the sense that distributed knowledge in a group with a single agent is the same as the knowledge of that single agent, i.e.

$$\ell = 1 \quad \Longrightarrow \quad \vDash \Box_1 A \leftrightarrow \mathbb{D}A$$

thus the completeness proof in that case is the same as for single-agent **IK**.

Remark 2.10. In this section, we assume that

the number of agents ℓ is at least 2.

2.3. Pseudo-validity

Now we build up some machinery that will lead to the canonical models and the completeness proofs for the systems **IDK** and **IDT** in the next section. Our method is motivated by the approach presented in Fagin, Halpern, and Vardi [FHV92] and Wang and Ågotnes [WÅ11]. However, our version is a significant simplification, tailored for the treatment of **IDK** and **IDT**.

Our approach is based on the notion of pseudo-validity. We will interpret the formulas of $\mathcal{L}_{DK}$ in so-called pseudo-structures. These are EK-structures of order $(\ell+1)$ where the operator $\mathbb{D}$ is interpreted by the additional binary accessibility relation $R_{\ell+1}$. Afterwards we will extend these EK-structures of order $(\ell+1)$ to strict EK-structures of order $(\ell+1)$ and then collapse these strict EK-structures of order $(\ell+1)$ to EK-structures of order ℓ, suitable for our purpose.

Definition 2.11. Given an EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ of order $(\ell + 1)$, the notion of *pseudo-satisfaction* $\vDash^{ps}$ of a formula A at a point of a model is inductively defined as follows: the clauses not involving $\mathbb{D}$ are as in 1.5, and the clause for distributed knowledge in 2.1 is replaced by

$$(\mathfrak{M}, w) \vDash^{ps} \mathbb{D}A \quad :\Longleftrightarrow \quad (\mathfrak{M}, v) \vDash^{ps} A \quad \text{for all } v \in R_{\ell+1}[w]$$

As can be seen by a trivial induction on A we also have monotonicity for pseudo-satisfaction.

Lemma 2.12. *For every EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ of order $(\ell + 1)$, all elements $w, v \in W$, and all A we have that*

$$(\mathfrak{M}, w) \vDash^{ps} A \;\; \textit{and} \;\; w \leq v \quad \Longrightarrow \quad (\mathfrak{M}, v) \vDash^{ps} A.$$

We say that A is *pseudo-valid in the EK-structure* $\mathfrak{M}$ of order $(\ell+1)$, written $\mathfrak{M} \vDash^{ps} A$, iff $(\mathfrak{M}, w) \vDash^{ps} A$ for all worlds w of $\mathfrak{M}$.

Since the operator $\mathbb{D}$ is interpreted by the relation $R_{\ell+1}$ in an EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ of order $(\ell + 1)$, the axioms (**D2**) are not necessarily pseudo-valid in $\mathfrak{M}$. Those EK-structures of order $(\ell+1)$ in which all (**D2**)-axioms are pseudo-valid are called *(**D2**)-pseudo-models*. An EK-structure $\mathfrak{M}$ of order $(\ell+1)$ is a *(**D2T**)-pseudo-model* iff all (**D2**)-axioms and all (**T**)-axioms are pseudo-valid in $\mathfrak{M}$.

Of course, for every EK-structure $\mathfrak{M}$ of order ℓ there is an EK-structure $\mathfrak{M}'$ of order $(\ell+1)$ such that validity in $\mathfrak{M}$ is equivalent to pseudo-validity in $\mathfrak{M}'$. The following lemma is an immediate consequence of Definition 2.1 and Definition 2.11.

Lemma 2.13. *Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be an EK-structure of order ℓ and define*

$$\mathfrak{M}' \;:=\; (W, \leq, R_1, \ldots, R_\ell, \bigcap_{i=1}^{\ell} R_i, V).$$

Then $\mathfrak{M}'$ is an EK-structure of order $(\ell + 1)$ and for all $w \in W$ and all A we have that

$$(\mathfrak{M}, w) \vDash A \quad \Longleftrightarrow \quad (\mathfrak{M}', w) \vDash^{ps} A.$$

*In particular, $\mathfrak{M}'$ is a (**D2**)-pseudo-model and if $\mathfrak{M}$ is a (**T**)-model, then $\mathfrak{M}'$ is a (**D2T**)-pseudo-model.*

Our next step is to transform a given EK-structure of order $(\ell+1)$ into an extended structure, called its strict extension. The purpose of this extension is to enforce a well-controlled behavior of the intersection of the accessibility relations. From now on we write I for the set $\{1,\ldots,(\ell+1)\}$.

Definition 2.14 (Strict extension)**.** Given an EK-structure

$$\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$$

of order $(\ell+1)$, its *strict extension* is defined to be the structure

$$\mathfrak{M}^\sharp \;=\; (W^\sharp, \leq^\sharp, R_1^\sharp, \ldots, R_{\ell+1}^\sharp, V^\sharp),$$

where we set:

($\sharp$1) $W^\sharp \;:=\; W \times I$,

($\sharp$2) $\leq^\sharp := \{((w,i),(v,j)) \mid w \leq v \text{ and } i,j \in I\}$,

($\sharp$3) $R_i^\sharp \;:=\; \{((w,j),(v,i)) \mid v \in R_i[w] \text{ and } j \in I\}$ for any $i \in I$,

($\sharp$4) $V^\sharp((w,i)) \;:=\; V(w)$ for any $(w,i) \in W^\sharp$.

It is obvious that $\mathfrak{M}^\sharp$ is an EK-structure of order $(\ell+1)$. Further properties of strict extensions are summarized in the following lemma.

Lemma 2.15. *Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ be an EK-structure of order $(\ell+1)$. Then we have:*

(a) If i and j are different elements of I, then $R_i^\sharp[(w,k)] \cap R_j^\sharp[(w,k)] = \varnothing$ for any $(w,k) \in W^\sharp$.

(b) $\bigcap_{i=1}^{\ell} R_i^\sharp[(w,k)] = \varnothing$ for any $(w,k) \in W^\sharp$.

Proof. The second assertion is an immediate consequence of the first since we deal with at least two agents. The first assertion follows from ($\sharp$3), which claims that all elements of $W^\sharp$ accessible from (w,k) via $R_i^\sharp$ are of the form (v,i) and those accessible from (w,k) via $R_j^\sharp$ are of the form (u,j). □

The following important lemma shows that the strict extension of an EK-structure of order $(\ell+1)$ does not affect the class of pseudo-valid formulas.

Lemma 2.16. *Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ be an EK-structure of order $(\ell+1)$. Then we have for all $(w,i) \in W^\sharp$ and all A that*

$$(\mathfrak{M}, w) \models^{ps} A \quad \Longleftrightarrow \quad (\mathfrak{M}^\sharp, (w,i)) \models^{ps} A.$$

Proof. We show this claim by induction on the structure of A and distinguish the following cases.

(i) A is the logical constant $\bot$ or an atomic proposition. Then the situation is clear.

(ii) A is a disjunction or a conjunction. Then we simply have to apply the induction hypothesis.

(iii) A is of the form $B \to C$. To show the direction from left to right we assume $(\mathfrak{M}, w) \models^{ps} B \to C$ and thus have

$$(\mathfrak{M}, v) \models^{ps} B \quad \Longrightarrow \quad (\mathfrak{M}, v) \models^{ps} C \quad \text{for all } v \text{ such that } w \leq v. \tag{2.1}$$

In order to prove $(\mathfrak{M}^\sharp, (w,i)) \models^{ps} B \to C$, we pick an arbitrary $(u,j) \in W^\sharp$ for which $(w,i) \leq^\sharp (u,j)$ and $(\mathfrak{M}^\sharp, (u,j)) \models^{ps} B$. By the induction hypothesis we obtain $(\mathfrak{M}, u) \models^{ps} B$, and in view of the definition of $\leq^\sharp$ we also have $w \leq u$. Hence 2.1 gives us $(\mathfrak{M}, u) \models^{ps} C$, and a further application of the induction hypothesis yields $(\mathfrak{M}^\sharp, (u,j)) \models^{ps} C$, as we had to show. The proof of the converse directions follows exactly the same pattern.

(iv) A is of the form $\Box_j B$. For establishing the direction from left to right assume $(\mathfrak{M}, w) \models^{ps} \Box_j B$, yielding that

$$(\mathfrak{M}, v) \models^{ps} B \quad \text{for all } v \in R_j[w]. \tag{2.2}$$

Now we pick an arbitrary element (u,k) of $R_j^\sharp[(w,i)]$. According to the definition of $R_j^\sharp$ this implies that $u \in R_j[w]$, and in view of 2.2, we thus obtain $(\mathfrak{M}, u) \models^{ps} B$. Now we can apply the induction hypothesis and have $(\mathfrak{M}^\sharp, (u,k)) \models^{ps} B$. Therefore, $(\mathfrak{M}^\sharp, (w,i)) \models^{ps} \Box_j B$.

For the converse direction we proceed from $(\mathfrak{M}^\sharp, (w,i)) \models^{ps} \Box_j B$, i.e. from

$$(\mathfrak{M}^\sharp, (v,j)) \models^{ps} B \quad \text{for all } (v,j) \in R_j^\sharp[(w,i)]. \tag{2.3}$$

Given any element u of $R_j[w]$, we obtain $(u,j) \in R_j^\sharp[(w,i)]$, so 2.3 implies $(\mathfrak{M}^\sharp, (u,j)) \models^{ps} B$. Applying the induction hypothesis then immediately

leads to $(\mathfrak{M}, u) \models^{ps} B$. Hence we have $(\mathfrak{M}, w) \models^{ps} \Box_j B$.
(v) A is of the form $\mathbb{D}B$. This case can be handled as the previous case since $\mathbb{D}$ is interpreted by the relations $R_{\ell+1}$ and $R^\sharp_{\ell+1}$, respectively. □

An immediate consequence of this lemma is that the property of being a (**D2**)-pseudo-model or a (**D2T**)-pseudo-model is inherited from an EK-structure $\mathfrak{M}$ to its strict extension $\mathfrak{M}^\sharp$.

Corollary 2.17. *If $\mathfrak{M}$ is a (**D2**)-pseudo-model, then $\mathfrak{M}^\sharp$ is a (**D2**)-pseudo-model as well; if $\mathfrak{M}$ is a (**D2T**)-pseudo-model, then also $\mathfrak{M}^\sharp$ is a (**D2T**)-pseudo-model.*

The strict extensions of (**D2**)-pseudo-models have a further property that will be needed in the proof of Lemma 2.20.

Lemma 2.18. *Let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ be a (**D2**)-pseudo-model and j one of the numbers $1, \ldots, \ell$. Then we have for all $(w, i), (v, k) \in W^\sharp$ and all A that*

$$\left.\begin{array}{l} (\mathfrak{M}^\sharp, (w,i)) \models^{ps} \Box_j A \ \text{ and} \\ (v,k) \in (R_j^\sharp \cup R^\sharp_{\ell+1})[(w,i)] \end{array}\right\} \implies (\mathfrak{M}^\sharp, (v,k)) \models^{ps} A.$$

Proof. Since $\mathfrak{M}^\sharp$ is a (**D2**)-pseudo-model, $(\mathfrak{M}^\sharp, (w,i)) \models^{ps} \mathbb{D}A$ follows from the assumption $(\mathfrak{M}^\sharp, (w,i)) \models^{ps} \Box_j A$. In this pseudo-model the operator $\mathbb{D}$ is interpreted by means of the accessibility relation $R^\sharp_{\ell+1}$, hence the conclusion is an immediate consequence. □

EK-structures of order $(\ell+1)$ provide only intermediate tools for the canonical model construction. In the end we are interested in EK-stuctures of order ℓ, and in order to build those, we now collapse EK-structures $\mathfrak{M}$ of order $(\ell+1)$ to so-called associated structures $\mathfrak{M}^\star$ of order ℓ, via their strict extensions $\mathfrak{M}^\sharp$.

Definition 2.19 (Associated structure)**.** Given an EK-structure

$$\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$$

of order $(\ell+1)$, the structure *associated with* $\mathfrak{M}$ is defined to be the structure

$$\mathfrak{M}^\star \ = \ (W^\star, \leq^\star, R_1^\star, \ldots, R_\ell^\star, V^\star),$$

where we set:

(a) $W^\star := W^\sharp, \quad \leq^\star := \leq^\sharp, \quad V^\star := V^\sharp,$

(b) $R_i^\star := R_i^\sharp \cup R_{\ell+1}^\sharp \quad$ for $i = 1, \ldots, \ell$.

It is clear that $\mathfrak{M}^\star$ is an EK-structure of order ℓ. The decisive property of this construction is that validity with respect to the structure associated with an EK-structure $\mathfrak{M}$ of order $(\ell + 1)$ coincides with pseudo-validity with respect to its strict extension $\mathfrak{M}^\sharp$.

Lemma 2.20. *Given a (**D2**)-pseudo-model $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$, we have for all $(w, i) \in W^\sharp$ and all A that*

$$(\mathfrak{M}^\star, (w, i)) \vDash A \quad \Longleftrightarrow \quad (\mathfrak{M}^\sharp, (w, i)) \vDash^{ps} A.$$

Proof. The proof of this equivalence is by induction on the structure of A. We distinguish the following cases:

(i) A is the logical constant $\bot$ or an atomic proposition. Then the claim follows immediately.

(ii) A is a disjunction, a conjunction, or an implication. Then we simply have to apply the induction hypothesis.

(iii) A is of the form $\Box_j B$. In view of the definition of $R_j^\star$, the direction from left to right is obtained by a straightforward application of the induction hypothesis. For proving the converse direction, assume $(\mathfrak{M}^\sharp, (w, i)) \vDash^{ps} \Box_j B$. However, then Lemma 2.18 implies $(\mathfrak{M}^\sharp, (v, k)) \vDash^{ps} B$ for all elements (v, k) of $(R_j^\sharp \cup R_{\ell+1}^\sharp)[(w, i)] = R_j^\star[(w, i)]$. For all those (v, k) the induction hypothesis yields $(\mathfrak{M}^\star, (v, k)) \vDash B$, and thus we have $(\mathfrak{M}^\star, (w, i)) \vDash \Box_j B$.

(iv) A is of the form $\mathbb{D}B$. Now we observe that

$$\begin{aligned} \bigcap_{j=1}^{\ell} R_j^\star[(w, i)] &= \bigcap_{j=1}^{\ell} (R_j^\sharp \cup R_{\ell+1}^\sharp)[(w, i)] \\ &= \underbrace{(\bigcap_{j=1}^{\ell} R_j^\sharp[(w, i)])}_{=\varnothing} \cup R_{\ell+1}^\sharp[(w, i)] = R_{\ell+1}^\sharp[(w, i)], \end{aligned}$$

where $\bigcap_{j=1}^{\ell} R_j^\sharp[(w, i)]) = \varnothing$ follows from Lemma 2.15. Hence the operator $\mathbb{D}$ is interpreted in $\mathfrak{M}^\star$ as in $\mathfrak{M}^\sharp$, and our assertion is immediate from the induction hypothesis. □

We now come to the main theorem of this section. It is an immediate consequence of Lemma 2.16 and the previous lemma.

Theorem 2.21. *If $\mathfrak{M} = (W, \leq, R_1, \ldots, R_{\ell+1}, V)$ is a (**D2**)-pseudo-model, then we have for all $(w, i) \in W^\sharp$ and all formulas A of $\mathcal{L}_{DK}$ that*

$$(\mathfrak{M}, w) \vDash^{ps} A \quad \Longleftrightarrow \quad (\mathfrak{M}^\star, (w, i)) \vDash A.$$

*In particular, if $\mathfrak{M}$ is a (**D2T**)-pseudo-model, then $\mathfrak{M}^\star$ is a (**T**)-model.*

2.4. Prime sets and completeness

In the following, we let **ID•** stand for one of the theories **IDK** or **IDT** so we can talk about both of them at once.

In the following, we adapt the standard approach of proving completeness for intuitionistic modal systems to our logic with distributed knowledge.

The following prime lemma can be shown in a similar way than the prime lemma for **IK**.

Lemma 2.22 (Prime lemma)**.** *Suppose that $N \nvdash_{\mathbf{ID}\bullet} A$ for some set of formulas N and some formula A. Then there exists an **ID•**-prime set P such that $N \subseteq P$ and $P \nvdash_{\mathbf{ID}\bullet} A$.*

Relative to the theory **ID•** we now introduce the canonical EK-structure $\mathfrak{C}$. In order to keep the notation readable, we refrain from explicitly mentioning **ID•** (for example as sub- or superscript), but it should always be clear from the context to which theory we refer.

Definition 2.23 (Canonical structure)**.** The *canonical structure for* **ID•** is the $(\ell + 4)$ tuple

$$\mathfrak{C} \;=\; (\mathcal{W}, \subseteq, \mathcal{R}_1, \ldots, \mathcal{R}_{\ell+1}, \mathcal{V}),$$

where we define:

(a) $\mathcal{W} \;:=\; \{P \mid P \text{ is an } \mathbf{ID}\bullet\text{-prime set of formulas}\}$,

(b) $P \,\mathcal{R}_i\, Q \;:\Longleftrightarrow\; \Box_i^{-1} P \subseteq Q \quad$ for any $i = 1, \ldots, \ell$,

(c) $P \,\mathcal{R}_{\ell+1}\, Q \;:\Longleftrightarrow\; \mathbb{D}^{-1} P \subseteq Q$,

(d) $\mathcal{V} : \mathcal{W} \to \mathcal{P}(\mathsf{Prop})$ is the function given by

$$\mathcal{V}(Q) \;:=\; \{p \in \mathsf{Prop} \mid p \in Q\}.$$

It is evident that $\mathfrak{C}$ is an EK-structure of order $(\ell + 1)$. All further relevant properties follow more or less directly from the following truth property.

Lemma 2.24 (Truth lemma)**.** *Let* $\mathfrak{C} = (\mathcal{W}, \subseteq, \mathcal{R}_1, \ldots, \mathcal{R}_{\ell+1}, \mathcal{V})$ *be the canonical structure for* **ID•**. *Then we have for all* A *and all* $P \in \mathcal{W}$ *that*

$$A \in P \quad \Longleftrightarrow \quad (\mathfrak{C}, P) \models^{ps} A.$$

Proof. We establish this equivalence by induction on the structure of A and distinguish the following cases.

(i) It trivially holds in case that A is the logical constant $\bot$ or an atomic proposition.

(ii) If A is a disjunction or a conjunction it follows from the induction hypothesis and the properties of **ID•**-prime sets.

(iii) A is of the form $B_1 \to B_2$. We first assume that

$$B_1 \to B_2 \in P, \qquad P \subseteq Q \in \mathcal{W}, \qquad \text{and} \qquad (\mathfrak{C}, Q) \models^{ps} B_1.$$

Then we have $B_1 \to B_2 \in Q$ and (by the induction hypothesis) $B_1 \in Q$. Since Q is deductively closed, this yields $B_2 \in Q$ and thus again by the induction hypothesis that $(\mathfrak{C}, Q) \models^{ps} B_2$. Q has been an arbitrary superset of P within $\mathcal{W}$, and thus we conclude $(\mathfrak{C}, P) \models^{ps} B_1 \to B_2$.

Now assume $(\mathfrak{C}, P) \models^{ps} B_1 \to B_2$ and $B_1 \to B_2 \notin P$. Since P is deductively closed, we have $P \cup \{B_1\} \nvdash_{\mathbf{ID\bullet}} B_2$. By the prime lemma there exists a $Q \in \mathcal{W}$ such that

$$P \cup \{B_1\} \subseteq Q \qquad \text{and} \qquad Q \nvdash_{\mathbf{ID\bullet}} B_2, \quad \text{hence} \quad B_2 \notin Q.$$

Together with the induction hypothesis we thus obtain

$$(\mathfrak{C}, Q) \models^{ps} B_1 \qquad \text{and} \qquad (\mathfrak{C}, Q) \not\models^{ps} B_2.$$

Since $P \subseteq Q$, this contradicts $(\mathfrak{C}, Q) \models^{ps} B_1 \to B_2$.

(iv) A is of the form $\Box_i B$. For the direction from left to right assume

$$\Box_i B \in P \qquad \text{and} \qquad \Box_i^{-1} P \subseteq Q$$

for an arbitrary $Q \in \mathcal{W}$. This implies $B \in Q$, and in view of the induction hypothesis we thus have $(\mathfrak{C}, Q) \vDash^{ps} B$. Therefore, $(\mathfrak{C}, P) \vDash^{ps} \Box_i B$.
For the converse direction we assume $(\mathfrak{C}, P) \vDash^{ps} \Box_i B$. We first claim that

$$\Box_i^{-1} P \vdash_{\mathbf{ID}\bullet} B. \tag{*}$$

To establish this claim, assume for a contradiction that $\Box_i^{-1} P \nvdash_{\mathbf{ID}\bullet} B$. According to the prime lemma we thus have a $Q \in \mathcal{W}$ such that $\Box_i^{-1} P \subseteq Q$ and $Q \nvdash_{\mathbf{ID}\bullet} B$. In particular, $B \notin Q$. By the induction hypothesis, this yields $(\mathfrak{C}, Q) \nvDash^{ps} B$; a contradiction to $(\mathfrak{C}, P) \vDash^{ps} \Box_i B$ and $\Box_i^{-1} P \subseteq Q$.
From (*) we conclude that there are $C_1, \ldots, C_n \in \Box_i^{-1} P$ such that

$$\vdash_{\mathbf{ID}\bullet} (C_1 \wedge \cdots \wedge C_n) \to B.$$

Thus we also have

$$\vdash_{\mathbf{ID}\bullet} (\Box_i C_1 \wedge \cdots \wedge \Box_i C_n) \to \Box_i B,$$

with $\Box_i C_1, \ldots, \Box_i C_n \in P$, implying that $P \vdash_{\mathbf{ID}\bullet} \Box_i B$. Hence $\Box_i B \in P$ since P is deductively closed.
(v) A is of the form $\mathbb{D}B$. Because of the pseudo-validity interpretation of $\mathbb{D}$, this case is treated exactly as the previous cases. □

Corollary 2.25.

(a) If $\mathfrak{C}$ is the canonical structure for **IDK***, then $\mathfrak{C}$ is a (**D2**)-pseudo-model.*

(b) If $\mathfrak{C}$ is the canonical structure for **IDT***, then $\mathfrak{C}$ is a (**D2T**)-pseudo-model.*

Proof. We only have to remember that an **IDK**-prime set of formulas P is deductively closed with respect to derivability in **IDK** and, therefore, contains $\Box_i A \to \mathbb{D}A$ for all $i = 1, \ldots, \ell$ and all A. Analogously, any **IDT**-prime set of formulas Q contains, in addition, the formulas $\mathbb{D}A \to A$ for any A. Thus the truth lemma implies our assertions. □

Now the stage is set, and combining what we have obtained so far, we can state the following first main result.

Theorem 2.26. *Let* $\mathfrak{C} = (\mathcal{W}, \subseteq, \mathcal{R}_1, \ldots, \mathcal{R}_{\ell+1}, \mathcal{V})$ *be the canonical structure for* **ID•** *and* $\mathfrak{C}^\star$ *the EK-structure of order* ℓ *associated with* $\mathfrak{C}$*. Then we have for all* **ID•***-prime sets of formulas* P*, all* A*, and all* $i = 1, \ldots, \ell$ *that*

$$A \in P \iff (\mathfrak{C}^\star, (P, i)) \vDash A.$$

Proof. In view of the truth lemma and Lemma 2.16 we have

$$A \in P \iff (\mathfrak{C}, P) \vDash^{ps} A \iff (\mathfrak{C}^\sharp, (P, i)) \vDash^{ps} A$$

for the strict extension $\mathfrak{C}^\sharp$ of $\mathfrak{C}$. Furthermore, $\mathfrak{C}^\sharp$ is a (**D2**)-pseudo-model according to the previous corollary. Hence we can apply Lemma 2.20 and see that

$$(\mathfrak{C}^\star, (P, i)) \vDash A \iff (\mathfrak{C}^\sharp, (P, i)) \vDash^{ps} A.$$

Therefore, we have what we want. □

Theorem 2.27 (Completeness)**.** *For all* $\mathcal{L}_{DK}$*-formulas* A *we have:*

(a) $\vDash A \implies \vdash_{\mathbf{IDK}} A$*.*

(b) $\vDash_{ref} A \implies \vdash_{\mathbf{IDT}} A$*.*

Proof. For the first assertion, assume $\vDash A$ and $\nvdash_{\mathbf{IDK}} A$. Note that then the prime lemma thus tells us that there exists an **IDK**-prime set P for which $P \nvdash_{\mathbf{IDK}} A$. Hence $A \notin P$. Consider the canonical structure $\mathfrak{C}$ for **IDK** and the EK-structure $\mathfrak{C}^\star$ associated with $\mathfrak{C}$. According to Theorem 2.26 we have $(\mathfrak{C}^\star, (P, i)) \nvDash A$ for $i = 1, \ldots, \ell$. This is a contradiction to $\vDash A$.

We come to the second assertion. Now we assume $\vDash_{ref} A$ and $\nvdash_{\mathbf{IDT}} A$. In this case the prime lemma gives us an **IDT**-prime set Q for which $Q \nvdash_{\mathbf{IDK}} A$ and, consequently, $A \notin Q$. Now we work with the canonical structure $\mathfrak{C}$ for **IDT** and the EK-structure $\mathfrak{C}^\star$ associated with $\mathfrak{C}$. We see that $\mathfrak{C}$ is a (**D2T**)-pseudomodel by Corollary 2.25 and, consequently, $\mathfrak{C}^\star$ is a (**T**)-model by Theorem 2.21. In view of Theorem 2.26 we also have $(\mathfrak{C}^\star, (Q, i)) \nvDash A$ for any $i = 1, \ldots, \ell$. It only remains to move to the reflexive extension $\overline{\mathfrak{C}^\star}$ of $\mathfrak{C}^\star$ and to apply Lemma 2.9. It follows that $(\overline{\mathfrak{C}^\star}, (Q, i)) \nvDash A$. Since $\overline{\mathfrak{C}^\star}$ is reflexive, this is a contradiction to $\vDash_{ref} A$. □

Together with Theorem 2.7 we thus have that **IDK** and **IDT** are sound and complete formalizations of intuitionistic distributed knowledge.

3. Common Knowledge

This chapter is about intuitionistic common knowledge. We will present two Hilbert systems and show their soundness and completeness with respect to EK-structures and reflexive EK-structures, respectively.

Intuitively, A is common knowledge in a group of agents iff everbody knows A, everybody knows that everybody knows A, and so on. Alternatively, A is common knowledge iff the agents are in a situation S, everybody knows A, and everybody knows that they are in the situation S. As we will see later, a formal counterpart of this idea lies at the core of the completeness proof for common knowledge. This chapter is based on [JM16b].

3.1. The language $\mathcal{L}_{CK}$ and its semantics

The formulas of $\mathcal{L}_{CK}$ are defined as the formulas of $\mathcal{L}_K$ with the additional clause

$$\text{if } A \text{ is a formula, then } \mathbb{C}A \text{ is a formula.}$$

In the following, we will use the abbreviation

$$\mathbb{E}(A) \;:=\; \Box_1 A \wedge \cdots \wedge \Box_\ell A$$

in order to express that "everybody knows A" or "everybody believes A", depending on what the $\Box_i A$ are supposed to formalize. Again we will often omit parentheses by writing $\mathbb{E}A$ instead of $\mathbb{E}(A)$.

In the traditional approach, put forward, for example, in Fagin, Halpern, Moses, and Vardi [FHMV95], common knowledge $\mathbb{C}A$ of A is interpreted as the infinite conjunction $\bigwedge\{\mathbb{E}^n(A) \mid n \geq 1\}$ of the iterations of everybody knows A, where

$$\mathbb{E}^0(A) := A \quad \text{ and } \quad \mathbb{E}^{n+1}(A) := \mathbb{E}(\mathbb{E}^n(A)).$$

This is appropriate as a semantic characterization of common knowledge,

but there is a problem: Since our language is finite, we cannot have an axiom of the form

$$\mathbb{C}A \;\leftrightarrow\; \bigwedge_{n\geq 1} \mathbb{E}^n(A).$$

To overcome this complication, $\mathbb{C}A$ is typically axiomatized via the fixed point characterization

$$\mathbb{C}A \;\leftrightarrow\; \mathbb{E}(A \wedge \mathbb{C}A),$$

more precisely as the greatest fixed point of this equivalence. We will show that, as for classical common knowledge, these two semantic approaches are equivalent.

For the classical treatment of common knowledge, see Fagin, Halpern, Moses, and Vardi [FHMV95], Meyer and van der Hoek [MvdH04], and Sillari and Vanderschraaf [VG13]. See also [MSnt] for an overview of the proof theory of common knowledge.

Definition 3.1. Assume that $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ is an EK-structure and n a natural number.

(a) We say that there exists an $\mathfrak{M}$-path of length n from world $w \in W$ to world $v \in W$ – written $Path_{\mathfrak{M}}(w, v, n)$ – iff there exist $u_0, \ldots, u_n \in W$ such that $w = u_0$, $v = u_n$, and $u_{i+1} \in \bigcup_{j=1}^{\ell} R_j[u_i]$ for $i = 0, \ldots, n-1$.

(b) $Reach_{\mathfrak{M}}(w, n)$ and $Reach_{\mathfrak{M}}(w)$ are defined to be the collections of all elements of W that are reachable from $w \in W$ by an $\mathfrak{M}$-path of length n and any $\mathfrak{M}$-path, respectively,

$$Reach_{\mathfrak{M}}(w, n) \;:=\; \{v \in W \mid Path_{\mathfrak{M}}(w, v, n)\},$$

$$Reach_{\mathfrak{M}}(w) \;:=\; \bigcup_{m\geq 1} Reach_{\mathfrak{M}}(w, m).$$

Remark 3.2. We make the following observations, where each one implies the next:

- $w \leq w' \implies \bigcup_{j=1}^{\ell} R_j[w'] \subseteq \bigcup_{j=1}^{\ell} R_j[w]$
- $Path_{\mathfrak{M}}(w', v, 1),\ w \leq w' \implies Path_{\mathfrak{M}}(w, v, 1)$

- $Path_{\mathfrak{M}}(w', v, n),\ w \leq w' \implies Path_{\mathfrak{M}}(w, v, n)$ for each $n \in \mathbb{N}$
- $w \leq w' \implies Reach_{\mathfrak{M}}(w', n) \subseteq Reach_{\mathfrak{M}}(w, n)$ for each $n \in \mathbb{N}$
- $w \leq w' \implies Reach_{\mathfrak{M}}(w') \subseteq Reach_{\mathfrak{M}}(w)$

Definition 3.3 (Satisfaction)**.** We extend the definition of satisfaction 1.5 of $\mathcal{L}_K$ by the following clause:

$$(\mathfrak{M}, w) \vDash \mathbb{C}A \iff (\mathfrak{M}, v) \vDash A \quad \text{for all } v \in Reach_{\mathfrak{M}}(w)$$

Remark 3.4. Alternatively, we could define satisfaction in the following equivalent way:

$$R := \bigcup_{i=1}^{\ell} R_i \quad \text{and let } R^\star \text{ be the transitive closure of } R.$$

Then

$$(\mathfrak{M}, w) \vDash \mathbb{C}A \iff (\mathfrak{M}, v) \vDash A \quad \text{for all } v \in R^\star[w].$$

The next lemma states monotonicity for formulas of the form $\mathbb{C}A$ and follows immediately by the remark about paths and reachability 3.2 above.

Lemma 3.5.

$$(\mathfrak{M}, w) \vDash \mathbb{C}A,\ w \leq v \implies (\mathfrak{M}, v) \vDash \mathbb{C}A.$$

Again, we check that monotonicity still holds.

Lemma 3.6 (Monotonicity)**.** *For each formula A of $\mathcal{L}_{CK}$*

$$(\mathfrak{M}, w) \vDash A,\ w \leq v \implies (\mathfrak{M}, v) \vDash A$$

Proof. By induction on A. The only interesting case is when $A = \mathbb{C}B$, which is covered by the lemma above. □

Next, we will have a closer look at the semantics of fixpoints and prefixpoints. The main result will be that the denotation of common knowledge is the greatest postfixpoint of a certain operator, which allows us to show the soundness of the co-closure axiom and the induction rule. We follow the approach in [FHMV95], adapted to our notations.

Definition 3.7 (The operator $\mathcal{O}_A$)**.** Let A be a formula of $\mathcal{L}_{CK}$ and $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ an EK-structure. Then the operator

$$\mathcal{O}_A : \mathcal{P}(W) \to \mathcal{P}(W)$$

is defined by

$$\mathcal{O}_A(X) \;:=\; \|\mathbb{E}(A)\|_{\mathfrak{M}} \cap \left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq X \right\}$$

for all $X \subseteq W$.

The monotonicity of this operator follows immediately from the definition:

Lemma 3.8. *For each EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ and each formula A, the operator $\mathcal{O}_A$ is monotone, i.e. for all $X, Y \subseteq W$*

$$X \subseteq Y \quad \Longrightarrow \quad \mathcal{O}_A(X) \subseteq \mathcal{O}_A(Y)$$

For a function $f : X \to X$ we make use of the usual notation for function iteration:

$$f^0(x) := x \quad \text{and} \quad f^{n+1}(x) := f(f^n(x))$$

We recall the standard definitions of fixpoints and postfixpoints:

Definition 3.9 (Fixpoint and postfixpoint)**.** Let X be a set partially ordered by $\leq$ and $f : X \to X$ a function.

- $x \in X$ is a *fixpoint* of f iff $f(x) = x$.
- $x \in X$ is a *postfixpoint* of f iff $x \leq f(x)$.

We quote the following classical result by Knaster and Tarski, which will allow us to speak of the greatest fixpoint of our operator $\mathcal{O}_A$.

Theorem 3.10 (Knaster-Tarski)**.** *Let W be an arbitrary set. Each monotone operator on $f : \mathcal{P}(W) \to \mathcal{P}(W)$ has a greatest postfixpoint which is its greatest fixpoint.*

Now, since our operator $\mathcal{O}_A$ is monotone, we can immediately apply the theorem of Knaster-Tarski to it.

Corollary 3.11. *For each formula A and each EK-structure $\mathfrak{M}$, the operator $\mathcal{O}_A$ has a greatest postfixpoint which is its greatest fixpoint.*

Definition 3.12. Let W be an arbitrary set. $f : \mathcal{P}(W) \to \mathcal{P}(W)$ is called *downwards continuous* iff for all descending sequences $N_0 \supseteq N_1 \supseteq N_2 \ldots$ ($N_i \subseteq W$ for each $i \in \mathbb{N}$) we have that

$$f\left(\bigcap_{n\in\mathbb{N}} N_n\right) = \bigcap_{n\in\mathbb{N}} f\left(N_n\right)$$

Lemma 3.13. *If W is a set and $f : \mathcal{P}(W) \to \mathcal{P}(W)$ is downwards continuous, then f is monotone.*

Proof. Assume that f is downwards continuous, and let $X, Y \in \mathcal{P}(W)$ with $X \subseteq Y$. Then we have

$$Y \supseteq X \supseteq X \supseteq \ldots$$

so it follows by the downwards continuity of f that

$$f(X) \cap f(Y) = f(X \cap Y) = f(X) \quad \text{and therefore} \quad f(X) \subseteq f(Y).$$

□

The next lemma gives us a nice explicit description of the greatest fixpoint of downwards closed operators.

Lemma 3.14. *If W is a set and $f : \mathcal{P}(W) \to \mathcal{P}(W)$ is downwards continuous, then*

$$\mathsf{gfp}(f) = \bigcap_{n\in\mathbb{N}} f^n(W)$$

Proof. We first show that $(f^n(W))_{n\in\mathbb{N}}$ forms a descending chain, i.e. $f^0(W) \supseteq f^1(W) \supseteq f^2(W) \supseteq \ldots$. We show by induction on n that $f^n(W) \supseteq f^{n+1}(W)$.

$n = 0$. Then $f^0(W) = W \supseteq f^1(W)$.

$n \to n+1$. By I.H. we have that $f^n(W) \supseteq f^{n+1}(W)$. Since f is downwards continuous, it follows by the previous lemma 3.13 that f is monotone, and therefore

$$f^{n+1}(W) = f(f^n(W)) \supseteq f(f^{n+1}(W)) = f^{n+2}(W).$$

Next, we show that $\bigcap_{n\in\mathbb{N}} f^n(W)$ is a fixpoint of f. Because f is downwards continuous, we have

$$f\left(\bigcap_{n\in\mathbb{N}} f^n(W)\right) = \bigcap_{n\in\mathbb{N}} f(f^n(W)) = \bigcap_{n\in\mathbb{N}} f^{n+1}(W)) \bigcap_{n\in\mathbb{N}} f^n(W)$$

Finally, we show that $\bigcap_{n\in\mathbb{N}} f^n(W)$ is the greatest fixpoint of f. Let F be an arbitrary fixpoint of f. We show that $F \subseteq f^n(W)$ for each $n \in \mathbb{N}$. Again we use induction on n.

$n = 0$. Then $F \subseteq W = f^0(W)$.

$n \to n+1$. By the I.H. we have $F \subseteq f^n(W)$. Since f is monotone, it follows that $F \overset{\text{fixpoint}}{=} f(F) \subseteq f(f^n(W)) = f^{n+1}(W)$.

From this it follows immediately that

$$F \subseteq \bigcap_{n\in\mathbb{N}} f^n(W)$$

so $\bigcap_{n\in\mathbb{N}} f^n(W)$ is the greatest fixpoint of f. □

Lemma 3.15. *For each formula A of $\mathcal{L}_{CK}$ and each EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$, the operator $\mathcal{O}_A : \mathcal{P}(W) \to \mathcal{P}(W)$ is downwards continuous.*

Proof. Let $M_n \subseteq W$ for all $n \in \mathbb{N}$, and let $M_0 \supseteq M_1 \supseteq \ldots$ be a descending

chain. Then we have

$$\begin{aligned}
\mathcal{O}_A\left(\bigcap_{n\in\mathbb{N}} M_n\right) &= \|\mathbb{E}A\|_{\mathfrak{M}} \cap \left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq \bigcap_{n\in\mathbb{N}} M_n \right\} \\
&= \|\mathbb{E}A\|_{\mathfrak{M}} \cap \bigcap_{n\in\mathbb{N}} \left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq M_n \right\} \\
&= \bigcap_{n\in\mathbb{N}} \left(\|\mathbb{E}A\|_{\mathfrak{M}} \cap \left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq M_n \right\} \right) \\
&= \bigcap_{n\in\mathbb{N}} \mathcal{O}_A\left(M_n\right)
\end{aligned}$$

□

It follows that we can apply lemma 3.14 to our operator $\mathcal{O}_A$ to get a nice characterization of its greatest fixpoint.

Corollary 3.16. *For each formula A of $\mathcal{L}_{CK}$ and each EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$*

$$\mathsf{gfp}(\mathcal{O}_A) = \bigcap_{n\in\mathbb{N}} \mathcal{O}_A^n(W).$$

Lemma 3.17. *For each formula A of $\mathcal{L}_{CK}$ and each EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$*

$$\mathcal{O}_A^n(W) = \|\mathbb{E}(A)\|_{\mathfrak{M}} \cap \|\mathbb{E}^n(A)\|_{\mathfrak{M}} \text{ for all } n \geq 1$$

Proof. We proceed by induction on n.

$n = 1$. Then

$$\begin{aligned}
\mathcal{O}_A^1(W) = \mathcal{O}_A(W) = &\|\mathbb{E}(A)\| \cap \underbrace{\left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq W \right\}}_{=W} \\
&= \|\mathbb{E}(A)\| = \|\mathbb{E}(A)\| \cap \|\mathbb{E}^1(A)\|
\end{aligned}$$

$n \to n+1$. We can argue as follows:

$$\begin{aligned}
\mathcal{O}_A^{n+1}(W) &= \mathcal{O}_A(\mathcal{O}_A^n(W)) \overset{\text{I.H.}}{=} \mathcal{O}_A(\|\mathbb{E}^n(A)\|) \\
&= \|\mathbb{E}(A)\| \cap \underbrace{\left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq \|\mathbb{E}^n(A)\| \right\}}_{=\|\mathbb{E}^{n+1}(A)\|} = \\
&= \|\mathbb{E}(A)\| \cap \|\mathbb{E}^{n+1}(A)\|.
\end{aligned}$$

□

Corollary 3.18. *For each formula A of $\mathcal{L}_{CK}$ and each EK-structure $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$*

$$\mathsf{gfp}(\mathcal{O}_A) = \bigcap_{n \geq 1} \|\mathbb{E}^n(A)\|_{\mathfrak{M}}$$

Proof. Combining the previous observations, we have

$$\begin{aligned}
&\mathsf{gfp}(\mathcal{O}_A) \overset{3.16}{=} \bigcap_{n \in \mathbb{N}} \mathcal{O}_A^n(W) = \mathcal{O}_A^0(W) \cap \bigcap_{n \geq 1} \mathcal{O}_A^n(W) = \\
&= W \cap \bigcap_{n \geq 1} \mathcal{O}_A^n(W) = \bigcap_{n \geq 1} \mathcal{O}_A^n(W) \overset{3.17}{=} \bigcap_{n \geq 1} (\|\mathbb{E}(A)\| \cap \|\mathbb{E}^n(A)\|) = \\
&= \bigcap_{n \geq 1} \|\mathbb{E}^n(A)\|.
\end{aligned}$$

□

The following lemma tells us that also over our (intuitionistic) EK-structures common knowledge is handled as in the case of classical logic. The proof of this lemma is similar to the classical case. For ease of notation, it is formulated using the denotations of formulas, i.e. the set of worlds where a formula holds true.

Lemma 3.19. *For all EK-structures $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$, all $v \in W$, and all natural numbers n we have:*

(a) $w \in \|\mathbb{E}^n(A)\|_{\mathfrak{M}} \iff \mathit{Reach}_{\mathfrak{M}}(w,n) \subseteq \|A\|_{\mathfrak{M}}$.

(b) $\|\mathbb{C}A\|_{\mathfrak{M}} = \bigcap_{m\geq 1} \|\mathbb{E}^m(A)\|_{\mathfrak{M}}$.

(c) $\|\mathbb{C}A\|_{\mathfrak{M}} = \mathsf{gfp}\,(\mathcal{O}_A)$

(d) $\|\mathbb{C}A\|_{\mathfrak{M}} = \|\mathbb{E}A\|_{\mathfrak{M}} \cap \|\mathbb{E}(\mathbb{C}A)\|_{\mathfrak{M}}$

Proof. (a) By induction on n.

$n = 0$. Then $\mathbb{E}^0 A = A$, and $v \in \mathit{Reach}_{\mathfrak{M}}(w,0) \iff w = v$, so the claim follows immediately.

$n \to n+1$.

$$w \vDash \mathbb{E}^{n+1}A \iff w \vDash \mathbb{E}(\mathbb{E}^n A) \iff$$
$$v \vDash \mathbb{E}^n A \quad \text{for all } v \in \bigcup_{i=1}^{\ell} R_i[w] \overset{\text{I.H.}}{\iff}$$
$$u \vDash A \quad \text{for all } v \in \bigcup_{i=1}^{\ell} R_i[w] \text{ and all } u \in \mathit{Reach}_{\mathfrak{M}}(v,n)$$
$$u \vDash A \quad \text{for all } u \in \mathit{Reach}_{\mathfrak{M}}(w,n+1)$$

(b)

$$\bigcap_{m\geq 1} \|\mathbb{E}^m A\| = \bigcap_{m\geq 1} \left\{ w \in W \;\middle|\; v \vDash A \text{ for all } v \in \mathit{Reach}_{\mathfrak{M}}(w,m) \right\} =$$
$$= \left\{ w \in W \;\middle|\; v \vDash A \text{ for all } v \in \bigcup_{m\geq 1} \mathit{Reach}_{\mathfrak{M}}(w,m) \right\} = \|\mathbb{C}A\|.$$

(c)

$$\|\mathbb{C}A\| \overset{\text{(b)}}{=} \bigcap_{m\geq 1} \|\mathbb{E}^m A\| \overset{3.18}{=} \mathsf{gfp}(\mathcal{O}_A).$$

(d)

$$\|\mathbb{C}A\| \overset{(c)}{=} \mathcal{O}_A(\|\mathbb{C}A\|) = \|\mathbb{E}A\| \cap \left\{ w \in W \;\middle|\; \bigcup_{i=1}^{\ell} R_i[w] \subseteq \|\mathbb{C}A\| \right\} =$$
$$= \|\mathbb{E}A\| \cap \|\mathbb{E}(\mathbb{C}A)\|.$$

□

As for **IK** in chapter one, we call an $\mathcal{L}_{CK}$ formula A *valid in the EK-structure* $\mathfrak{M}$ iff $\mathfrak{M} \vDash A$. Accordingly, the *EK-valid* formulas are those $\mathcal{L}_{CK}$ formulas that are valid in all EK–structures. The question now is whether there exists a deductive system that proves exactly the EK-valid formulas.

3.2. The Hilbert systems ICK and ICKT

There exist numerous formalisms for intuitionistic modal logic, ranging from Hilbert-style systems to sequent calculi and frameworks dealing with nested sequents. A series of those is presented in, e.g., Simpson [Sim94] and Marin and Straßburger [MS14].

Since our goal is to show completeness via a canonical model construction, we choose to use a Hilbert system for ease of presentation.

Definition 3.20 (The systems **ICK** and **ICKT**)**.** The system **ICK** has all axioms and rules of **IK** for the language $\mathcal{L}_{CK}$, and in addition the axiom

$$\mathbb{C}A \;\to\; \mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A) \qquad (\mathbf{CCL})$$

and the induction rule for common knowledge

$$\frac{B \to \mathbb{E}A \wedge \mathbb{E}B}{B \to \mathbb{C}A} \quad (\mathbf{IND}).$$

The system **ICKT** has, in addition, the truth axioms

$$\Box_i A \;\to\; A \qquad (\mathbf{T})$$

The following theorem list a series of important properties of **ICK** and **ICKT**.

Theorem 3.21. *Let* $\mathbf{ICK}^\bullet$ *be the system* **ICK** *or the system* **ICKT**. *For all* $\mathcal{L}_{CK}$ *formulas* A, B *and all sets* M, N *of* $\mathcal{L}_{CK}$ *formulas we have:*

(a) $\vdash_{\mathbf{ICK}^\bullet} A \implies \vdash_{\mathbf{ICK}^\bullet} \mathbb{E}A$.

(b) $\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(A \to B) \to (\mathbb{E}A \to \mathbb{E}B)$.

(c) $\vdash_{\mathbf{ICK}^\bullet} A \implies \vdash_{\mathbf{ICK}^\bullet} \mathbb{C}A$.

(d) $\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(A) \wedge \mathbb{E}(\mathbb{C}A) \to \mathbb{C}A$.

(e) $\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(A) \wedge \mathbb{E}(\mathbb{C}A) \leftrightarrow \mathbb{C}A$.

Proof. (a) Assume that $\vdash_{\mathbf{ICK}^\bullet} A$. By applying necessitation, we get $\vdash_{\mathbf{ICK}^\bullet} \Box_i A$ for each $i = 1, \ldots, \ell$. It follows by propositional reasoning that $\vdash_{\mathbf{ICK}^\bullet} \bigwedge_{i=1}^{\ell} \Box_i A$, i.e. $\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}A$.

(b) By the K-axioms we have $\vdash_{\mathbf{ICK}^\bullet} \Box_i(A \to B) \to (\Box_i A \to \Box_i B)$ for all $i = 1, \ldots, \ell$. It follows by propositional reasoning in intuitionistic logic that

$$\begin{aligned}
&\vdash_{\mathbf{ICK}^\bullet} \bigwedge_{j=1}^{\ell} \Box_j(A \to B) \to (\Box_i A \to \Box_i B) \text{ for all } i = 1, \ldots, \ell \\
\implies &\vdash_{\mathbf{ICK}^\bullet} \bigwedge_{i=1}^{\ell} \Box_i(A \to B) \to \bigwedge_{i=1}^{\ell} (\Box_i A \to \Box_i B) \\
\implies &\vdash_{\mathbf{ICK}^\bullet} \bigwedge_{i=1}^{\ell} \Box_i(A \to B) \to (\bigwedge_{i=1}^{\ell} \Box_i A \to \bigwedge_{i=1}^{\ell} \Box_i B) \\
\implies &\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(A \to B) \to (\mathbb{E}A \to \mathbb{E}B).
\end{aligned}$$

(c) Assume that $\vdash_{\mathbf{ICK}^\bullet} A$. By (a) it follows that $\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}A$. Now let $\top$ denote $\neg\bot$. Then we have that $\vdash_{\mathbf{ICK}^\bullet} \top \to (\mathbb{E}A \wedge \mathbb{E}\top)$. Applying the induction rule we get $\vdash_{\mathbf{ICK}^\bullet} \top \to \mathbb{C}A$, so $\vdash_{\mathbf{ICK}^\bullet} \mathbb{C}A$.

(d) By the co-closure axiom we have that $\vdash_{\mathbf{ICK}^\bullet} \mathbb{C}A \to (\mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A))$. It follows by (a) that

$$\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(\mathbb{C}A \to (\mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A)))$$

and then by (b) that

$$\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}(\mathbb{C}A) \to \mathbb{E}(\mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A)).$$

By propositional reasoning we get

$$\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A) \to \mathbb{E}A \wedge \mathbb{E}(\mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A)).$$

Finally, we can apply the induction rule and obtain

$$\vdash_{\mathbf{ICK}^\bullet} \mathbb{E}A \wedge \mathbb{E}(\mathbb{C}A) \to \mathbb{C}A.$$

(e) Follows immediately by (d) and the co-closure axiom.

□

Lemma 3.22 (Soundness of co-closure)**.** *The co-closure axiom holds in all EK-structures:*

$$\vDash \mathbb{C}A \to \mathbb{E}(A) \wedge \mathbb{E}(\mathbb{C}A)$$

Proof. By lemma 1.8 it suffices to show that for each EK-structure $\mathfrak{M}$

$$\|\mathbb{C}A\|_{\mathfrak{M}} \subseteq \|\mathbb{E}A\|_{\mathfrak{M}} \cap \|\mathbb{E}(\mathbb{C}A)\|_{\mathfrak{M}}$$

which follows from lemma 3.19. □

Lemma 3.23 (Soundness of induction rule)**.** *The induction rule is sound, i.e.*

$$\vDash B \to \mathbb{E}(A) \wedge \mathbb{E}(B) \quad \Longrightarrow \quad \vDash B \to \mathbb{C}A$$

Proof. Assume that $\vDash B \to \mathbb{E}(A) \wedge \mathbb{E}(B)$. Now let $\mathfrak{M} = (W, \leq, R_1, \ldots, R_\ell, V)$ be an EK-structure. Then we have $W = \|B \to \mathbb{E}(A) \wedge \mathbb{E}(B)\|_{\mathfrak{M}}$. According to lemma 1.8, this is equivalent to

$$\|B\|_{\mathfrak{M}} \subseteq \|\mathbb{E}(A) \wedge \mathbb{E}(B)\|_{\mathfrak{M}}.$$

We also observe that

$$\mathcal{O}_A(\|B\|_{\mathfrak{M}}) = \|\mathbb{E}(A) \wedge \mathbb{E}(B)\|_{\mathfrak{M}}$$

and therefore $\|B\|_{\mathfrak{M}}$ is a postfixpoint of the operator $\mathcal{O}_A$. By lemma 3.19,

$\|\mathbb{C}A\|_{\mathfrak{M}}$ is the greatest postfixpoint of this operator which means that

$$\|B\|_{\mathfrak{M}} \subseteq \|\mathbb{C}A\|_{\mathfrak{M}}$$

so it follows by lemma 1.8 that

$$\|B \to \mathbb{C}A\|_{\mathfrak{M}} = W$$

i.e.

$$\mathfrak{M} \vDash B \to \mathbb{C}A$$

and since $\mathfrak{M}$ was arbitrary, we have that

$$\vDash B \to \mathbb{C}A.$$

□

Using these lemmas, we can easily establish the soundness of the systems **ICK** and **ICKT**.

Theorem 3.24 (Soundness of **ICK** and **ICKT**)**.** *Let A a formula of $\mathcal{L}_{CK}$.*

(a) $\vdash_{\mathbf{ICK}} A \implies \vDash A$

(b) $\vdash_{\mathbf{ICKT}} A \implies \vDash_{ref} A$

Proof. By inductions on the length of the derivations. The cases where A is an instance of the co-closure axiom or was derived by the induction rule are covered in lemma 3.22 and 3.23. □

3.3. Completeness of ICK and ICKT

In this section we show that **ICK** is complete with respect to EK-structures and **ICKT** is complete with respect to reflexive EK-structures. Our approach is an adaptation of the completeness proof presented in Fagin, Halpern, Moses, and Vardi [FHMV95] for a system of classical common knowledge.

Until the end of this section we fix an $\mathcal{L}_{CK}$ formula A and build the so-called canonical model with respect to A.

First, we define the fragment with respect to A. This is the finite set of formulas from which we will build the worlds of the canonical model.

Definition 3.25. Given a formula A of $\mathcal{L}_{CK}$, the fragment $\mathsf{Frag}(A)$ is the collection of all $\mathcal{L}_{CK}$ formulas that is inductively generated as follows:

(a) $A, \bot \in \mathsf{Frag}(A)$.

(b) If $B \in \mathsf{Frag}(A)$, then all subformulas of B belong to $\mathsf{Frag}(A)$.

(c) If $\mathbb{C}(B) \in \mathsf{Frag}(A)$, then $\mathbb{E}(B)$ and $\mathbb{E}(\mathbb{C}(B))$ belong to $\mathsf{Frag}(A)$.

We observe that $\mathsf{Frag}(A)$ is a finite set. The most important ingredients of our canonical model with respect to A are the A-prime sets of formulas. These are defined similarly as the prime sets of formulas but live in the fragment $\mathsf{Frag}(A)$.

Definition 3.26 (A-prime)**.** A set P of $\mathcal{L}_{CK}$ formulas is called *A-prime* iff it satisfies the following conditions:

(P.1) $P \subseteq \mathsf{Frag}(A)$.

(P.2) P is deductively closed w.r. to $\mathsf{Frag}(A)$:
$B \in \mathsf{Frag}(A)$ and $P \vdash_{\mathbf{ICK}} B \implies B \in P$.

(P.3) P has the disjunction property:
$B \vee C \in P \implies B \in P$ or $C \in P$.

(P.4) P is consistent: $\bot \notin P$.

Similar as for the logic **IK**, where we used prime sets of formulas as the worlds of the canonical model, the A-prime sets of $\mathcal{L}_{CK}$ formulas will form the worlds of the canonical model depending on A. The next lemma is an analogue of the prime lemma, formulated for A-prime sets. Its can be proved in a similar way to the prime lemma for $\mathcal{L}_K$.

Lemma 3.27 (A-Prime lemma)**.** *Suppose that $N \subseteq \mathsf{Frag}(A)$ and $N \nvdash_{\mathbf{ICK}} B$ for some $\mathcal{L}_{CK}$ formula B; observe that it is not assumed that $B \in \mathsf{Frag}(A)$. Then there exists an A-prime set P such that $N \subseteq P$ and $P \nvdash_{\mathbf{ICK}} B$.*

Proof. Let $A_0, \ldots, A_k$ be an enumeration of the elements of $\mathsf{Frag}(A)$. Now

we define by induction, for $n = 0, \ldots, k$,

$$N_0 \;:=\; N,$$

$$N_{n+1} \;:=\; \begin{cases} N_n \cup \{A_n\} & \text{if } N_n \cup \{A_n\} \nvdash_{\mathbf{ICK}} B, \\ N_n & \text{if } N_n \cup \{A_n\} \vdash_{\mathbf{ICK}} B. \end{cases}$$

Clearly, we have $N \subseteq N_n \subseteq N_{n+1}$ and $N_{n+1} \nvdash_{\mathbf{ICK}} B$ for $n = 0, \ldots, k$. We set $P := N_{k+1}$ and show that P is A-prime. The reasoning is exactly the same as in the proof of the prime lemma for **IK**. □

As for prime sets of formulas, in this section we let P, Q, R (possibly with subscripts) range over A-prime sets of $\mathcal{L}_{CK}$ formulas. In addition, we set

$$P^c \;:=\; \mathsf{Frag}(A) \setminus P.$$

Definition 3.28 (Canonical model for **ICK**)**.** Depending on the given $\mathcal{L}_{CK}$ formula A we now define the structure

$$\mathfrak{M}(A) \;:=\; (\mathcal{W}^A, \subseteq, \mathcal{R}_1^A, \ldots, \mathcal{R}_\ell^A, \mathcal{V}^A)$$

where

(C.1) $\mathcal{W}^A \;:=\; \{P \subseteq \mathsf{Frag}(A) \mid P \text{ is } A\text{-prime}\}$.

(C.2) For any $i = 1, \ldots, \ell$, $\mathcal{R}_i^A$ is defined to be the binary relation on W^A defined as

$$P \,\mathcal{R}_i^A\, Q \quad :\Longleftrightarrow \quad \Box_i^{-1} P \subseteq Q$$

(C.3) $\mathcal{V}^A : \mathcal{W}^A \to \mathcal{P}(\mathsf{Prop})$ is the function given by

$$\mathcal{V}^A(Q) \;:=\; \{p \in \mathsf{Prop} \mid p \in Q\}.$$

We immediately observe that $\mathfrak{M}(A)$ is an EK-structure. The following lemma is the core of the completeness proof.

Lemma 3.29 (Truth lemma)**.** *We have for all formulas $B \in \mathsf{Frag}(A)$ and all $P \in \mathcal{W}^A$ that*

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

Proof. It is clear that we can assign a rank to each $\mathcal{L}_{CK}$ formula such that the rank of the logical constant $\bot$ and of every atomic proposition is 0, the rank of a subformula C_0 of a formula C is smaller than that of C, and the rank of a formula $\Box_i C$ is smaller than that of $\mathbb{C}(C)$. We establish the equivalence of the truth lemma by induction on the rank of B and distinguish the following cases.

(i) It trivially holds in case that B is an atomic proposition or the logical constant $\bot$.

(ii) If B is a disjunction or a conjunction it follows from the induction hypothesis and the properties of A-prime sets. The reasoning is the same as for **IK**.

(iii) B is the implication $C_1 \to C_2$. Again we proceed similarly to the situation for **IK**. We first assume that

$$C_1 \to C_2 \in P, \qquad P \subseteq Q, \qquad \text{and} \qquad Q \vDash C_1.$$

Then we have $C_1 \to C_2 \in Q$ and (by the induction hypothesis) $C_1 \in Q$. Since Q is deductively closed with respect to $\mathsf{Frag}(A)$ this yields $C_2 \in Q$ and thus again by the induction hypothesis that $Q \vDash C_2$. Since Q has been an arbitrary A-prime superset of P, we conclude $P \vDash C_1 \to C_2$.

Now assume $P \vDash C_1 \to C_2$ and $C_1 \to C_2 \notin P$. Since P is deductively closed with respect to $\mathsf{Frag}(A)$, we have $P \cup \{C_1\} \nvdash_{\mathbf{ICK}} C_2$. By the prime lemma there exists a Q such that

$$P \cup \{C_1\} \subseteq Q \qquad \text{and} \qquad Q \nvdash_{\mathbf{ICK}} C_2.$$

Together with the induction hypothesis we thus obtain

$$Q \vDash C_1 \qquad \text{and} \qquad Q \nvDash C_2.$$

Since $P \subseteq Q$, this contradicts $P \vDash C_1 \to C_2$.

(iv) B is a formula $\Box_i C$. For the direction from left to right assume

$$\Box_i C \in P \qquad \text{and} \qquad \Box_i^{-1} P \subseteq Q$$

for an arbitrary Q. This implies $C \in Q$, and in view of the induction hypothesis we thus have $Q \vDash C$. Therefore, $P \vDash \Box_i C$.

For the converse direction we assume $P \models \Box_i C$. We first claim that

$$\Box_i^{-1} P \vdash_{\mathbf{ICK}} C. \tag{3.1}$$

To establish this claim, assume for contradiction that $\Box_i^{-1} P \nvdash_{\mathbf{ICK}} C$. According to the prime lemma we thus have a Q such that $\Box_i^{-1} P \subseteq Q$ and $Q \nvdash_{\mathbf{ICK}} C$. In particular, $C \notin Q$. By the induction hypothesis, this yields $Q \not\models C$; a contradiction to $P \models \Box_i C$ and $\Box_i^{-1} P \subseteq Q$.

From (1) we conclude that there are $A_1, \ldots, A_n \in \Box_i^{-1} P$ with

$$\vdash_{\mathbf{ICK}} A_1 \wedge \cdots \wedge A_n \to C.$$

By using necessitation we get

$$\vdash_{\mathbf{ICK}} \Box_i (A_1 \wedge \cdots \wedge A_n \to C)$$

and with the K-axiom and propositional reasoning we obtain

$$\vdash_{\mathbf{ICK}} \Box_i A_1 \wedge \cdots \wedge \Box_i A_n \to \Box_i C$$

with $\Box_i A_1, \ldots, \Box_i A_n \in P$, implying that $P \vdash_{\mathbf{ICK}} \Box_i C$. Hence $\Box_i C \in P$ since P is deductively closed with respect to $\mathsf{Frag}(A)$.

(v) B is a formula $\mathbb{C}(C)$. We first assume $\mathbb{C}(C) \in P$ and check by simple induction on n that for all natural numbers $n \geq 1$ and all $Q \in \mathit{Reach}_{\mathfrak{M}(A)}(P, n)$,

$$C \in Q \qquad \text{and} \qquad \mathbb{C}(C) \in Q. \tag{3.2}$$

Hence we have $C \in Q$ for all $Q \in \mathit{Reach}_{\mathfrak{M}(A)}(P)$ and by the induction hypothesis $Q \models C$ for these sets Q. Therefore, $P \models \mathbb{C}(C)$.

Now we assume $P \models \mathbb{C}(C)$. To show that then $\mathbb{C}(C) \in P$ is the most interesting part of this proof. We set

$$\mathcal{W} := \{Q \in \mathcal{W}^A \mid Q \models \mathbb{C}(C)\} \quad \text{and} \quad S := \bigvee \left(\left\{ \bigwedge Q \;\middle|\; Q \in \mathcal{W} \right\} \right).$$

We briefly pause to reflect on the formula S. Intuitively, a world Q of $\mathcal{W}$ is a situation where $\mathbb{C}(C)$ holds, and since such a Q is a finite set of formulas, we can form the conjunction $\bigwedge Q$. This is a formula which completely

describes this situation Q. Then, the disjunction S describes that we are in one of the worlds of $\mathcal{W}$, so in a situation where $\mathbb{C}(C)$ holds. In the following, we will show that our logic reflects that in the situation (described by) S, everybody knows C and everbody knows S, more precisely:

$$\vdash_{\mathbf{ICK}} S \to \mathbb{E}(C) \wedge \mathbb{E}(S).$$

Then we will use the induction rule to derive $\vdash_{\mathbf{ICK}} S \to \mathbb{C}(C)$ which leads to $\mathbb{C}(C) \in P$. We continue by proving a series of auxiliary assertions.

(I) For all $P \in \mathcal{W}$: $\vdash_{\mathbf{ICK}} \bigwedge P \to \Box_i C$.

Proof of (I). For $P \in \mathcal{W}$ we have $P \vDash \Box_i C$ and thus $\Box_i C \in P$ by the induction hypothesis. The assertion follows immediately.

(II) For all $P \in \mathcal{W}$ and $Q \in R_i[P]$: $Q \in \mathcal{W}$.

Proof of (II). For $P \in \mathcal{W}$ we have $P \vDash \Box_i \mathbb{C}(C)$ and thus $Q \vDash \mathbb{C}(C)$ for all $Q \in R_i[P]$. This is what we had to show.

(III) For all $P \in \mathcal{W}$: $\Box_i^{-1} P \vdash_{\mathbf{ICK}} S$.

Proof of (III). Let P be an element of $\mathcal{W}$ and assume that $\Box_i^{-1} P \nvdash_{\mathbf{ICK}} S$. By the prime lemma then there exists a Q such that $\Box_i^{-1} P \subseteq Q$ and $Q \nvdash_{\mathbf{ICK}} S$. Hence $Q \in R_i[P]$ and, in view of (II), $Q \in \mathcal{W}$. This is a contradiction to $Q \nvdash_{\mathbf{ICK}} S$.

(IV) For all $P \in \mathcal{W}$: $\vdash_{\mathbf{ICK}} \bigwedge P \to \Box_i S$.

Proof of (IV). Because of (III) we know that there are $A_1, \ldots, A_n \in \Box_i^{-1} P$ such that

$$\vdash_{\mathbf{ICK}} A_1 \wedge \cdots \wedge A_n \to S.$$

Thus we also have

$$\vdash_{\mathbf{ICK}} \Box_i A_1 \wedge \cdots \wedge \Box_i A_n \to \Box_i S$$

with $\Box_i A_1, \ldots, \Box_i A_n \in P$. Hence $P \vdash_{\mathbf{ICK}} \Box_i S$, and the assertion is an immediate consequence.

From (I) and (IV) we obtain

$$\vdash_{\mathbf{ICK}} \bigwedge P \to \mathbb{E}(C) \wedge \mathbb{E}(S)$$

for all $P \in \mathcal{W}$, hence

$$\vdash_{\mathbf{ICK}} S \to \mathbb{E}(C) \wedge \mathbb{E}(S). \tag{3.3}$$

By means of the induction rule we obtain from (3) that

$$\vdash_{\mathbf{ICK}} S \to \mathbb{C}(C).$$

By assumption we have $P \in \mathcal{W}$ and thus $P \vdash_{\mathbf{ICK}} S$. Hence $P \vdash_{\mathbf{ICK}} \mathbb{C}(C)$ and so $\mathbb{C}(C) \in P$ since P is deductively closed with respect to $\mathsf{Frag}(A)$. This finishes the proof of the truth lemma. □

With the truth lemma at our disposal, the proof of the completeness of **ICK** is now routine.

Theorem 3.30 (Completeness of **ICK**)**.** *Suppose that A is an EK-valid $\mathcal{L}_{CK}$ formula. Then $\vdash_{\mathbf{ICK}} A$.*

Proof. Assume that $\nvdash_{\mathbf{ICK}} A$. Then there exists an A-prime P such that $P \nvdash_{\mathbf{ICK}} A$. Hence $A \notin P$, and thus the truth lemma implies $P \not\models A$. However, then A is not valid in the canonical model $\mathfrak{M}(A)$, contradicting our assumption. □

Now we turn to the completeness of **ICKT**. In principle, we proceed as before: We start off from an $\mathcal{L}_{CK}$ formula A, introduce the set $\mathsf{Frag}(A)$ and build a canonical model. The only difference is that we work with A-**T**-prime sets instead of A-prime sets. Here a set P of $\mathcal{L}_{CK}$ formulas is called A-**T**-prime iff it has the properties (P.1), (P.3), (P.4) of A-prime sets plus for all B the property

(P.2') $B \in \mathsf{Frag}(A)$ and $P \vdash_{\mathbf{ICKT}} B \implies B \in P$.

Then we construct the canonical model as before, but with A-prime sets replaced by A-**T**-prime sets; we call it

$$\mathfrak{N}(A) := (S^A, \subseteq, S_1^A, \ldots, S_\ell^A, U^A).$$

All we have to show in addition to what we did before is that $\mathfrak{N}(A)$ is reflexive. Hence take an i with $1 \leq i \leq \ell$, an A-**T**-prime set P, and an arbitrary element B of $\Box_i^{-1}P$. Then $\Box_i B \in P$. Since

$$\vdash_{\mathbf{ICKT}} \Box_i B \to B$$

this implies $B \in P$. Hence $\Box_i^{-1} P \subseteq P$ and thus $P \in S_i^A[P]$. The truth lemma for $\mathfrak{N}(A)$ goes through as above, and the completeness of **ICKT** with respect to reflexive EK-structures is an immediate consequence.

Theorem 3.31 (Completeness of **ICKT**). *Suppose that the $\mathcal{L}_{CK}$ formula A is valid in all reflexive EK-structures. Then $\vdash_{\mathbf{ICKT}} A$.*

3.4. Disjunction property

Typically, intuitionistic formalisms possess the disjunction property:

$$\vdash A \vee B \quad \Longrightarrow \quad \vdash A \text{ or } \vdash B$$

It is an immediate consequence of the previous soundness and completeness results that the disjunction property also holds for **ICK** and **ICKT**.

Theorem 3.32 (Disjunction property). *For all $\mathcal{L}_{CK}$ formulas A and B we have:*

(a) If $A \vee B$ is EK-valid, then A is EK-valid or B is EK-valid.

(b) If $A \vee B$ is valid in all reflexive EK-structures, then A is valid in all reflexive EK-structures or B is valid in all reflexive EK-structures.

(c) If **ICK$^\bullet$** *is the system* **ICK** *or the system* **ICKT**, *then*

$$\vdash_{\mathbf{ICK}^\bullet} A \vee B \quad \Longrightarrow \quad \vdash_{\mathbf{ICK}^\bullet} A \text{ or } \vdash_{\mathbf{ICK}^\bullet} B.$$

Proof. In view of the soundness and completeness of **ICK$^\bullet$**, the third assertion is an immediate consequence of the first and the second. The proof of the second is exactly as the proof of the first, and to prove the first, we assume that neither A nor B are EK-valid. Then there exist EK-structures

$$\mathfrak{M}_1 = (W_1, \leq_1, R_1^{(1)}, \ldots, R_\ell^{(1)}, V_1) \quad \text{and} \quad \mathfrak{M}_2 = (W_2, \leq_2, R_1^{(2)}, \ldots, R_\ell^{(2)}, V_2)$$

together with $w_1 \in W_1$ and $w_2 \in W_2$ such that

$$(\mathfrak{M}_1, w_1) \nvDash A \quad \text{and} \quad (\mathfrak{M}_2, w_2) \nvDash B$$

Now consider the structure $\mathfrak{M} := (W, \leq, R_1, \ldots, R_\ell, V)$ whose universe is the set

$$W := \{(0,0)\} \cup \{(1,x) \mid x \in W_1\} \cup \{(2,x) \mid x \in W_2\}$$

and the preorder $\leq$ on W is defined by

$$(x_1, y_1) \leq (x_2, y_2) \;:\Leftrightarrow\; \begin{cases} x_1 = 0 \text{ or} \\ (x_1 = x_2 = 1 \text{ and } y_1 \leq_1 y_2) \text{ or} \\ (x_1 = x_2 = 2 \text{ and } y_1 \leq_2 y_2). \end{cases}$$

Furthermore, for every $i = 1, \ldots, \ell$, $R_i \subseteq W \times W$ is given by

$$R_i[(x,y)] \;:=\; \begin{cases} W & \text{if } x = 0, \\ \{(1,z) \mid z \in R_i^{(1)}[y]\} & \text{if } x = 1, \\ \{(2,z) \mid z \in R_i^{(2)}[y]\} & \text{if } x = 2. \end{cases}$$

Finally, $V : W \to \mathcal{P}(\mathsf{Prop})$ is defined by

$$V(x,y) \;:=\; \begin{cases} \varnothing & \text{if } x = 0, \\ V_1(y) & \text{if } x = 1, \\ V_2(y) & \text{if } x = 2. \end{cases}$$

Obviously, $\mathfrak{M}$ is an EK-structure. It is also easy to check that for all $\mathcal{L}_{CK}$ formulas C, all $x \in W_1$, and all $y \in W_2$,

$$\begin{aligned} (\mathfrak{M}, (1,x)) \vDash C \quad &\Longleftrightarrow \quad (\mathfrak{M}_1, x) \vDash C \\ (\mathfrak{M}, (2,y)) \vDash C \quad &\Longleftrightarrow \quad (\mathfrak{M}_2, y) \vDash C. \end{aligned}$$

Because of (*) this implies that

$$(\mathfrak{M}, (1, w_1)) \nvDash A \quad \text{and} \quad (\mathfrak{M}, (2, w_2)) \nvDash B$$

The monotonicity of $\mathfrak{M}$ with respect to $\leq$, cf. Lemma 3.6, and the fact that

$(0,0) \leq (1,w_1)$ and $(0,0) \leq (2,w_2)$ thus yield

$$(\mathfrak{M},(0,0)) \nvDash A \quad \text{and} \quad (\mathfrak{M},(0,0)) \nvDash B.$$

implying that

$$(\mathfrak{M},(0,0)) \nvDash A \vee B.$$

From this we conclude that $A \vee B$ is not EK-valid. □

It is also fairly easy to extend the results of this article to semantics and deductive systems that reflect positive introspection, like **IS4**; details are left to the reader. Negative introspection, on the other hand, is a different matter. Typically, intuitionistic **S5** is formulated by making use of the box and the diamond operator; see, e.g., Fischer Servi [Fis84] and Simpson [Sim94] and in intuitionistic modal logic $\Diamond A$ is not equivalent to $\neg\Box\neg A$. It is planned for the future to look at negative introspection from an intuitionistic perspective and to analyze the emerging issues from a technical and conceptual perspective.

Part II.

Intuitionistic Justification Logic

3.5. Introduction

Justification logics extend propositional logics with formulas of the form $t : A$, meaning that t is a justification, a piece of evidence, or a proof of A, or that A is known for the reason t. Intuitionistic justification logic consists of the usual machinery of justification logic, but based on intuitionistic propositional logic instead of classical propositional logic. It was introduced by Artemov in [Art98].

As reported in Gettier [Get63], Plato (see also [Cha13]) already seemed to have considered three criteria for knowledge : belief, truth and justification. To know something, so is the idea, one has to believe it, it has to be true, and in addition one needs to have a justification for it. The rationale for the justification condition goes roughly as follows: If someone comes to believe A and just by pure luck, A is actually true, then he does not have knowledge of A, but only true belief. There is something lacking, namely him having a justification for believing A.

Some formal counterparts of the concepts of belief and truth have their role in epistemic logic based on modal logic: The $\Box$-modality can be seen as expressing belief, and the truth axiom $\Box A \to A$ expresses the factivity of these beliefs. Whereas some formal counterparts of the concepts of belief and truth play a role in epistemic logic based on modal logic, there is no explicit formal counterpart of th concept of justification in these frameworks.

Epistemic logic based on modal logic treats knowledge via universal quantification: An agent knows a proposition iff it is true in all worlds accessible to the agent. Justification logic adds an aspect of existential quantification to epistemic logics: An agent knows a proposition if he has a justification for it, in other words if there exists a justification available to him.

The first justification logic was called the Logic of Proofs, and a special case of justification is when we consider all justifications to be mathematical proofs in a specific proof system.

There is a very close connection between some justification logics and some modal logics. The so-called forgetful projection maps formulas of justification logic to formulas of modal logic by replacing all justification terms with $\Box$ and therefore embeds the justification logic into the modal logic. On the other hand, there are techniques of realization which replaces all boxes by appropriate justification terms, and therefore embedding a

justification logic into a modal logic. This is more involved, and there exist several approaches to realization, from semantic arguments to algorithmic ones. Given realization, we can view justification logic as as a kind of more explicit modal logic.

Justification logics have found many applications. Artemov has used them to give a provability interpretation of **S4** [Art95, Art01], modeling epistemic paradoxes like Gettier cases, the Red Barn Example of Goldman and Kripke, and Russel's example of induced factivity [Art08a]. Artemov and Kuznets used justification logic to address the problem of logical omniscience [AK06a], and it has found applications to protocol-verification [Stu11a] and data privacy [Stu11b].

In this thesis, we will only treat single-agent systems of justification logic, and $t : A$ can then be read as "the agent has the justification t for A". There are also multi-agent versions of justification logics, where we instead have formulas of the form $t :_i A$, meaning that the agent i has justification t for A. Also, there are approaches for connecting some justification logics with distributed [Gha10] and with common knowledge [Art06, BKS11]. Moreover, there are dynamic epistemic justification logics [KS13] and probabilistic justification logics [KMOS15] available.

The original part of this chapter is the completeness proof with respect to basic modular models, which is based on [MS16].

3.6. A sequent system for IS4

We shortly come back to intuitionistic modal logic. For connecting our justification logic with the single-agent version of **IS4** via realization, we will need a cut-free sequent system of the single-agent versions of **IS4**, which we call **GIS4**.

Definition 3.33 (The proof system **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 **GIS4** derives sequents of the language $\mathcal{L}_K$ (where $\ell = 1$) 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 **GIS4**, in symbols $\vdash_{\mathbf{GIS4}} A$, if the sequent $\supset A$ is provable.

In the following, we will use Γ, Δ (possibly with subscripts) exclusively for finite multisets of formulas.

Theorem 3.34. GIS4 *is sound and complete with respect to single-agent reflexive transitive EK-structures.*

Proof. Soundness and completeness follow from [Ono77, Theorem 3.2 on p. 696] and the observation that Ono's I-models of type 0 are the same as our single-agent reflexive transitive EK-structures. □

Using soundness 1.12 and completeness 1.22 of **IS4** the equivalence of **IS4** and **GIS4** follows immediately.

Corollary 3.35. *The Hilbert system* **IS4** *and the sequent system* **GIS4** *are equivalent, i.e. for each $\mathcal{L}_K$-formula A we have*

$$\vdash_{\mathbf{IS4}} A \iff \vdash_{\mathbf{GIS4}} A$$

Definition 3.36 (Justification terms)**.** We assume a countable set of justification constants and a countable set of justification variables. The set of *justification terms* (or just *terms*) Tm is inductively defined by:

(a) each justification constant and each justification variable is a justification term;

(b) 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 3.37 (Formulas)**.** We start with the same set Prop of atomic propositions as in $\mathcal{L}_K$. The set of formulas $\mathcal{L}_\mathsf{J}$ is inductively defined by:

(a) every atomic proposition is a formula;

(b) the constant symbol $\bot$ is a formula;

(c) If A and B are formulas, then $(A \wedge B)$, $(A \vee B)$ and $(A \to B)$ are formulas;

(d) if A is a formula and t a term, then $t : A$ is a formula.

Definition 3.38. The system **iJT4** has the following axioms:

(a) all axioms for intuitionistic propositional logic

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

(c) $t : A \to t + s : A$ and $s : A \to t + s : A$

(d) $t : A \to A$

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

A *constant specification* CS is any subset

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

A constant specification CS is called:

- *axiomatically appropriate* if for each axiom A of **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 **iJT4**.

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

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

Remark 3.39. 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 3.40. Let Tot be the total constant specification, i.e.

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

Artemov's [Art02] intuitionistic logic of proofs $\mathcal{ILP}$ is then the same as our $\mathbf{iJT4}_{\mathsf{Tot}}$.

As for our intuitionistic modal logics, we have the deduction theorem for intuitionistic justification logic.

Theorem 3.41 (Deduction Theorem)**.** *For every set of formulas M and all formulas A, B we have that*

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

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

Lemma 3.42 (Lifting Lemma)**.** *Let CS be an axiomatically appropriate constant specification. For arbitrary formulas $A, B_1, \ldots, B_m, C_1, \ldots, C_n$ and arbitrary justification terms $r_1, \ldots, r_m, s_1, \ldots, s_n$, if*

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

then there is a justification term t such that

$$r_1 : B_1, \ldots, r_m : B_m, s_1 : C_1, \ldots, s_n : C_n \vdash_{\mathbf{iJT4_{CS}}} t : A.$$

Definition 3.43 (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 3.44 (Substitution Property)**.** *Let* CS *be a schematic constant specification. We have for any* $\mathcal{L}_{\mathsf{J}}$*-formula* A *and any substitution* σ

$$B_1, \ldots, B_n \vdash_{\mathbf{iJT4_{CS}}} A \quad \textit{implies} \quad B_1\sigma, \ldots, B_n\sigma \vdash_{\mathbf{iJT4_{CS}}} A\sigma.$$

We find that $\mathbf{iJT4_{CS}}$ is a conservative extension of intuitionistic propositional logic. Hence $\mathbf{iJT4_{CS}}$ is consistent.

Lemma 3.45 (Conservativity)**.** $\mathbf{iJT4_{CS}}$ *is a conservative extension of intuitionistic propositional logic* Int*, i.e., for any formula* A *of intuitionistic propositional logic,*

$$\vdash_{\mathbf{iJT4_{CS}}} A \quad \textit{iff} \quad \vdash_{\mathbf{Int}} A.$$

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

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

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

Lemma 3.46 (Consistency of $\mathbf{iJT4_{CS}}$)**.** *For any constant specification* CS*, the logic* $\mathbf{iJT4_{CS}}$ *is consistent.*

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

3.7. 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 $\mathbf{iJT4_{CS}}$. Accordingly we use $\vdash$ to mean $\vdash_{\mathbf{iJT4_{CS}}}$.

For two sets of formulas M, N and a term s we write

$$M \cdot N := \{A \mid B \to A \in M \text{ and } B \in N \text{ for some formula } B\}$$
$$s : M := \{s : A \mid A \in M\}$$

Definition 3.47 (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:

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

(M.2) $w \leq v \quad \Longrightarrow \quad t_w^* \subseteq t_v^*$.

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 3.48 (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 3.49 (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 3.50 (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 3.51 (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 3.52 (Soundness of $\mathbf{iJT4_{CS}}$ with respect to basic modular models)**.** *For every formula A:*

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

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

As for intuitionistic modal logic, we need a lemma about provability from disjunctions and then a version of the prime lemma for intuitionistic justification logics. The proofs of these statements are very similar to those for modal logic: We only use properties of prime sets and propositional reasoning.

Lemma 3.53 (Disjunction Lemma)**.** *Let N be an arbitrary set of formulas and let A, B and C be formulas. If*

$$N \cup \{A\} \vdash C \textit{ and } N \cup \{B\} \vdash C, \textit{ then } N \cup \{A \vee B\} \vdash C.$$

Theorem 3.54 (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 P with $N \subseteq P$ and $P \nvdash B$.*

Lemma 3.55. *Let P be a prime set and t be a justification term. Then*

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

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

Definition 3.56 (Canonical basic modular model)**.** The canonical basic modular model is the structure

$$\mathfrak{B} := (\mathcal{W}, \subseteq, \bigstar)$$

where

(i) $\mathcal{W} := \{P \mid P \text{ is prime}\}$

(ii) $\bigstar(p, P) = 1$ iff $p \in P$

(iii) $\bigstar(t, P) := t^{-1}P$

Lemma 3.57. *$\mathfrak{B}$ is a basic evaluation.*

Proof. $W \neq \varnothing$: By the consistency of $\mathbf{iJT4_{CS}}$ we have that $\varnothing \nvdash \bot$, it follows by the Prime Lemma 3.54 that there exists a prime set, so $\mathcal{W} \neq \varnothing$.

Next, we check the conditions on the sets of formulas $t_P^\bigstar$.

(1) $s_P^\bigstar \cdot t_P^\bigstar \subseteq (s \cdot t)_P^\bigstar$. Let $A \in s_P^\bigstar \cdot t_P^\bigstar$. Then there is a formula $B \in t_P^\bigstar$ such that $B \to A \in s_P^\bigstar$. So $s : B \to A \in P$ and $t : B \in P$. Since P 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 P is deductively closed, it follows by (MP) that $s \cdot t : A \in P$, so $A \in (s \cdot t)^{-1}P = (s \cdot t)_P^\bigstar$.

(2) $s_P^\bigstar \cup t_P^\bigstar \subseteq (s+t)_P^\bigstar$. Let $A \in s_P^\bigstar \cup t_P^\bigstar$. Case 1: $A \in s_P^\bigstar = s^{-1}P$. Then $s : A \in P$. Since P is deductively closed, it contains the axiom

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

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

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

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

Now we check the monotonicity conditions.

(M.1) Assume that $p_P^\bigstar = 1$ and $P \subseteq Q$. By the definition of $\bigstar$ we have that $p \in P$, so $p \in Q$ hence $p_Q^\bigstar = 1$.

(M.2) Now assume that $P \subseteq Q$. Then $t^{-1}P \subseteq t^{-1}Q$, which is $t_P^\bigstar \subseteq t_Q^\bigstar$. □

Lemma 3.58 (Truth Lemma)**.** *For any formula A and any prime set P :*

$$A \in P \iff (\mathfrak{B}, P) \vDash A.$$

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

(a) $A = p$ or $A = \bot$. By definition.

(b) $A = B \wedge C$. Assume that $B \wedge C \in P$. Since P is deductively closed, we have $B \in P$ and $C \in P$, so it follows by the induction hypothesis that $(\mathfrak{B}, P) \vDash B$ and $(\mathfrak{B}, P) \vDash C$, hence $(\mathfrak{B}, P) \vDash B \wedge C$.

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

(c) $A = B \vee C$. Assume that $B \vee C \in P$. Since P has the disjunction property, it follows that $B \in P$ or $C \in P$, so by the induction hypothesis, $(\mathfrak{B}, P) \vDash B$ or $(\mathfrak{B}, P) \vDash C$, so $(\mathfrak{B}, P) \vDash B \vee C$.

For the other direction assume that $(\mathfrak{B}, P) \vDash B \vee C$. Then

$$(\mathfrak{B}, P) \vDash B \text{ or } (\mathfrak{B}, P) \vDash C,$$

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

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

For the other direction assume that $(\mathfrak{B}, P) \vDash B \to C$. We have to show that $B \to C \in P$. Assume for a contradiction that $B \to C \notin P$. Since P is deductively closed, it follows that $P \nvdash B \to C$. It follows by the Deduction Theorem 3.41 that $P \cup \{B\} \nvdash C$. By the Prime Lemma 3.54, there is a prime set Q such that $P \cup \{B\} \subseteq Q$ and $Q \nvdash C$, so in particular, $C \notin Q$. By the induction hypothesis it follows that $(\mathfrak{B}, Q) \vDash B$ and $(\mathfrak{B}, Q) \nvDash C$, contradicting our assumption that $(\mathfrak{B}, P) \vDash B \to C$.

(e) $A = t : B$. We have

$$t : B \in P \iff B \in t^{-1}P = \bigstar(t, P) \iff (\mathfrak{B}, P) \vDash t : B.$$

□

Lemma 3.59. $\mathfrak{B}$ *is a basic modular model.*

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

$$A \in \bigstar(t, P) = t^{-1}P.$$

By Lemma 3.55 we know that $t^{-1}P \subseteq P$, so we have $A \in P$. By the Truth Lemma for the canonical basic modular model, we can conclude that $(\mathfrak{B}, P) \vDash A$. So factivity is shown. □

Theorem 3.60 (Completeness of $\mathbf{iJT4_{CS}}$ 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 3.54, there exists a prime set P such that $P \nvdash A$. In particular, $A \notin P$. By the Truth Lemma 3.58, it follows that

$$(\mathfrak{B}, P) \nvDash A.$$

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

3.8. 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., [Art12, KS12].

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 3.61 (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 3.62 (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 $\Box_w := \{A \in \mathcal{L}_\jmath \mid (\mathfrak{M}, v) \vDash A \text{ for all } v \in R[w]\}$.

Lemma 3.63 (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 3.64 (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 3.65 (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 $\mathfrak{M} = (W, \leq R, *)$ 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 [Art12].

Lemma 3.66 (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 3.67 (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 3.63. □

Lemma 3.68 (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 $A \in t^*_v$. □

Theorem 3.69 (Soundness and completeness: modular models)**.** *For any constant specification* CS *and any formula* A *we have*

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

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 3.67, we know that $\mathfrak{B} := (W, \leq, *)$ is a basic modular model. By soundness of $\mathbf{iJT4}_{\mathsf{CS}}$ 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 3.63).

Completeness. For the opposite direction, suppose $\nvdash A$. By completeness of $\mathbf{iJT4}_{\mathsf{CS}}$ 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 3.63), we have that $(\mathfrak{M}, w) \nvDash A$, and it only remains to show that $\mathfrak{M}$ is a modular $\mathbf{iJT4}_{\mathsf{CS}}$-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 $A \in \Box_w$. □

Definition 3.70 (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 3.71. $M/\sharp := \{A \in \mathcal{L}_\mathsf{J} \mid t : A \in M \quad \text{for some } t \in \mathsf{Tm}\}$.

Lemma 3.72.

$$M \subseteq N \quad \Longrightarrow \quad M/\sharp \subseteq N/\sharp$$

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

Lemma 3.73 (Soundness and completeness: fully explanatory modular models)**.** *Let* CS *be an axiomatically appropriate constant specification. Then* $\mathbf{iJT4}_\mathsf{CS}$ *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 modular model as

$$\mathfrak{C} := (\mathcal{W}, \subseteq, \mathcal{R}, \bigstar)$$

where

(i) $\mathcal{W} := \{P \mid P \text{ is prime}\}$

(ii) $\bigstar(p, P) = 1$ iff $p \in P$

(iii) $\bigstar(t, P) := t^{-1}P$

(iv) $P \mathcal{R} Q$ iff $P/\sharp \subseteq Q$

To show that $\mathfrak{C}$ is a modular $\mathbf{iJT4}_\mathsf{CS}$-model, it remains to establish that the set $\mathcal{W}$ is non-empty, that $\mathcal{R}$ is reflexive and transitive, that $\subseteq$ is compatible with $\mathcal{R}$ and that the condition JYB is satisfied. We start with showing $\mathcal{W} \neq \varnothing$. We have already shown that the empty set is $\mathbf{iJT4}_\mathsf{CS}$-consistent, so by the Prime Lemma 3.54, there exists a prime set extending $\varnothing$, which is an element of $\mathcal{W}$.

To show that $\subseteq$ is compatible with $\mathcal{R}$, assume that $P \subseteq Q$. We need to show that $\mathcal{R}[Q] \subseteq \mathcal{R}[P]$, so we pick $R \in \mathcal{R}[Q]$ and show that $R \in \mathcal{R}[P]$.

$R \in \mathcal{R}[Q]$ means that $Q/\sharp \subseteq R$. By the lemma above, we have that $P/\sharp \subseteq Q/\sharp$, and therefore $P/\sharp \subseteq R$, i.e., $R \in \mathcal{R}[P]$.

To show JYB, assume $A \in t_P^{\bigstar}$ for some formula A , some $t \in \mathsf{Tm}$, and some $P \in \mathcal{W}$. We need to show that $A \in \Box_P$, i.e., that $(\mathfrak{C}, Q) \vDash A$ whenever $\mathcal{R}(P, Q)$. Consider any such $Q \in \mathcal{W}$. We have $t : A \in P$ by the definition of $t_P^{\bigstar}$ and $A \in Q$ by the definition of $\mathcal{R}$. By the truth lemma for basic evaluations, it follows that $(\mathfrak{B}, Q) \vDash A$ where $\mathfrak{B} = (\mathcal{W}, \subseteq, \bigstar)$. By the locality of truth in quasimodels, we have $(\mathfrak{C}, Q) \vDash A$.

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

To show that $\mathcal{R}$ is transitive, consider arbitrary $P, Q, R \in \mathcal{W}$ such that $\mathcal{R}(P, Q)$ and $\mathcal{R}(Q, R)$. Assume that $A \in P/\sharp$, i.e., that $t : A \in P$ for some $t \in \mathsf{Tm}$. Since P is prime, it is deductively closed, and since $t : A \to !t : t : A$ is an axiom of $\mathbf{iJT4_{CS}}$, we conclude $!t : t : A \in P$. Hence $t : A \in P/\sharp \subseteq Q$ and $A \in Q/\sharp \subseteq R$. Therefore, $P/\sharp \subseteq R$, which means $\mathcal{R}(P, Q)$.

Finally, we show that $\mathfrak{C}$ is fully explanatory. Assume that $A \in \Box_P$ for some formula A and prime set P. Then

$$P/\sharp \vdash A \tag{3.4}$$

Indeed, assume for a contradiction that $P/\sharp \nvdash A$. By the Prime Lemma, there exists a prime set Q such that $P/\sharp \subseteq Q$ and $Q \nvdash A$. By the definition of $\mathcal{R}$, we have $\mathcal{R}(P, Q)$, and from $Q \nvdash A$ we get that $A \notin Q$. By the Truth Lemma for basic evaluations, it follows that $(\mathfrak{B}, Q) \nvDash A$. By the locality of truth in quasimodels, we have $(\mathfrak{C}, Q) \nvDash A$, contradicting our assumption that $A \in \Box_P$. By (3.4), it follows that there are finitely many formulas $B_1, \ldots, B_n \in P/\sharp$, such that

$$B_1, \ldots, B_n \vdash A.$$

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

By the Lifting Lemma 3.42, given the axiomatic appropriateness of

CS, there exists a term t such that

$$s_1 : B_1, \ldots, s_n : B_n \vdash t : A$$

By the Deduction Theorem

$$\vdash s_1 : B_1 \to (s_2 : B_2 \to \cdots \to (s_n : B_n \to t : A) \cdots).$$

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

$$A \in t^{-1}P = t_P^{\bigstar}.$$

So $\mathfrak{C}$ is fully explanatory. □

3.9. 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 [Art02, 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 3.74 (Forgetful projection)**.** *Let* CS *be an arbitrary constant specification. For each* $\mathcal{L}_{\mathsf{J}}$*-formula* A*,*

$$\vdash_{\mathbf{iJT4}_{\mathsf{CS}}} A \quad \textit{implies} \quad \vdash_{\mathbf{IS4}} A^\circ.$$

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

It is easy to see that for each axiom A of $\mathbf{iJT4}_{\mathsf{CS}}$, we have $\vdash_{\mathbf{IS4}} A^\circ$.

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

$$\vdash_{\mathbf{IS4}} B^\circ \quad \text{and} \quad \vdash_{\mathbf{IS4}} B^\circ \to A^\circ$$

and thus $\vdash_{\mathbf{IS4}} A^\circ$ 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 $\mathbf{iJT4_{CS}}$. Therefore, as shown above, $\vdash_{\mathbf{IS4}} B^\circ$. An application of necessitation yields $\vdash_{\mathbf{IS4}} \Box B^\circ$, which is $\vdash_{\mathbf{IS4}} A^\circ$. □

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 3.75 (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*

$$\vdash_{\mathbf{GIS4}} A \quad \textit{implies} \quad \vdash_{\mathbf{iJT4_{CS}}} r(A).$$

Proof. It turns out that Artemov's original realization proof for LP [Art01] 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 **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 **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 **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*.

(a) 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.

(b) 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.

(c) 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 $\mathbf{iJT4_{CS}}$ where derivability of $\Gamma \supset A$ means $\Gamma \vdash_{\mathbf{iJT4_{CS}}} A$. We distinguish the following cases.

a) The axioms $\Gamma \supset A$ with $A \in \Gamma$ or $\bot \in \Gamma$ are derivable in $\mathbf{iJT4_{CS}}$.

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 $\mathbf{iJT4_{CS}}$ 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 $\mathbf{iJT4_{CS}}$. Using the Lifting Lemma, we construct a term t such that

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

Thus

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

Substitute t for u_i everywhere in $\mathcal{D}'$. By Lemma 3.44, 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 $\mathbf{iJT4}_{\mathsf{CS}}$. The realization r built by this construction is normal. □

3.10. 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 **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.

Bibliography

[AK06a] S. Artemov and R. Kuznets. Logical omniscience via proof complexity. Technical Report TR–2006005, CUNY Ph.D. Program in Computer Science, May 2006. Later version published as [AK06b].

[AK06b] S. Artemov and R. Kuznets. Logical omniscience via proof complexity. In Zoltán Ésik, editor, *Computer Science Logic, 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 25–29, 2006, Proceedings*, volume 4207 of *Lecture Notes in Computer Science*, pages 135–149. Springer, 2006.

[AP14] S. Artemov and T. Protopopescu. Intuitionistic Epistemic Logic. eprint arXiv:1406.1582v2 [math.LO], 2014.

[Art95] S. Artemov. Operational modal logic. Technical Report MSI 95–29, Cornell University, December 1995.

[Art98] S. Artemov. Logic of Proofs: a unified semantics for modality and λ-terms. Technical Report CFIS 98–06, Cornell University, March 1998.

[Art01] S. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, March 2001.

[Art02] S. 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.

[Art06] S. Artemov. Justified common knowledge. *Theoretical Computer Science*, 357(1–3):4–22, July 2006.

[Art08a] S. Artemov. The logic of justification. Technical Report TR–2008010, CUNY Ph.D. Program in Computer Science, September 2008. Later version published as [Art08b].

[Art08b] S. Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, December 2008.

[Art12] S. Artemov. The ontology of justifications in the logical setting. *Studia Logica*, 100(1–2):17–30, April 2012. Published online February 2012.

[BKS11] S. Bucheli, R. Kuznets, and T. Studer. Justifications for common knowledge. *Journal of Applied Non-Classical Logics*, 21(1):35–60, January–March 2011.

[Cha13] T. Chappell. Plato on knowledge in the *Theaetetus*. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Winter 2013 edition, 2013.

[FHMV95] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[FHV92] R. Fagin, J.Y. Halpern, and M.Y. Vardi. What can machines know? On the properties of knowledge in distributed systems. *Journal of the Association for Computing Machinery*, 39(2):328–376, 1992.

[Fis84] G. Fischer Servi. Axiomatizations for some intuitionistic modal logics. *Rendiconti del Seminario Matematico Università e Politecnico di Torino*, 42(3):179–194, 1984.

[Get63] E. L. Gettier. Is justified true belief knowledge? *Analysis*, 23(6):121–123, 1963.

[Gha10] M. Ghari. Justification counterpart of distributed knowledge systems. In Marija Slavkovik, editor, *Proceedings of the* 15^{th} *Student Session of 13th European Summer School for Logic, Language and Information*, pages 25–36, Copenhagen, Denmark, August 9–20, 2010. FoLLI. Later version with errata published as [Gha12]; journal version published as [Gha13].

[Gha12] M. Ghari. Distributed knowledge with justifications. In Daniel Lassiter and Marija Slavkovik, editors, *New Directions in Logic, Language and Computation, ESSLLI 2010 and ESSLLI 2011 Student Sessions, Selected Papers*, volume 7415 of *Lecture Notes in Computer Science*, pages 91–108. Springer, 2012. Journal version published as [Gha13].

[Gha13] M. Ghari. Distributed knowledge justification logics. *Theory of Computing Systems*, Online First, August 2013. Published online August 2013.

[Hin62] J. Hintikka. *Knowledge and Belief: An Introduction to the Logic of the Two Notions*. Cornell University Press, 1962.

[Hir10] Y. Hirai. An intuitionistic epistemic logic for sequential consistency on shared memory. In E.M. Clarke and A. Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning*, volume 6355 of *Lecture Notes in Computer Science*, pages 272–289. North-Holland, 2010.

[JM16a] G. Jäger and M. Marti. A canonical model construction for intuitionistic distributed knowledge. In L. Beklemishev, S. Demri, and A. Máté, editors, *Advances in Modal Logic 2016*, pages 420–434. College Publications, 2016.

[JM16b] G. Jäger and M. Marti. Intuitionistic common knowledge or belief. *Journal of Applied Logic*, 18, 2016.

[KMOS15] I. Kokkinis, P. Maksimović, Z. Ognjanović, and T. Studer. First steps towards probabilistic justification logic. *Logic Journal of IGPL*, 23(4):662–687, 2015.

[KS12] R. Kuznets and T. 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.

[KS13] R. Kuznets and T. 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.

[MS14] S. Marin and L. Straßburger. Label-Free Modular Systems for Classical and Intuitionistic Modal Logics. In R. Goré, B. Kooi, and A. Kurucz, editors, *Advances in Modal Logic*, volume 10 of *AiML*, pages 387–406. College Publications, 2014.

[MS16] M. Marti and T. Studer. Intuitionistic modal logic made explicit. *IfCoLog Journal of Logics and their Applications*, 3:877–901, 2016.

[MSnt] M. Marti and T. Studer. The proof theory of common knowledge. In H. van Ditmarsch and G. Sandu, editors, *Jaakko Hintikka on knowledge and game theoretical semantics*, Outstanding Contributions to Logic. Springer, in print.

[MvdH04] J.-J. Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*, volume 41 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2004.

[Ono77] H. Ono. On some intuitionistic modal logics. *Publications of the Research Institute for Mathematical Sciences*, 13(3):687–722, 1977.

[Pro12] C. Proietti. Intuitionistic epistemic logic, Kripke models and Fitch's paradox. *Journal of Philosophical Logic*, 41(5):877–900, 2012.

[PS86] G.D. Plotkin and C.P. Stirling. A framework for intuitionistic modal logic. In J.Y. Halpern, editor, *Theoretical Aspects of Reasoning About Knowledge*, pages 399–406. Morgan Kaufmann Publishers„ 1986.

[Sim94] A. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic (revised version)*. PhD thesis, University of Edinburgh, 1994.

[Stu11a] T. Studer. An application of justification logic to protocol verification. In *Proceedings, 2011 Seventh International Conference on Computational Intelligence and Security, CIS 2011*, pages 779–783. IEEE, 2011.

[Stu11b] T. Studer. Justification logic, inference tracking, and data privacy. *Logic and Logical Philosophy*, 20(4):297–306, 2011.

[VG13] P. Vanderschraaf and G.Sillari. Common Knowledge. Stanford Encyclopedia of Philosophy, 2013.

[WÅ11] Y.N. Wáng and T. Ågotnes. Public announcement logic with distributed knowledge. In H. van Ditmarsch, J. Lang, and S. Ju, editors, *LORI 2011*, volume 6953 of *Lecture Notes in Artificial Intelligence*, pages 328–341. Springer, 2011.

[Wil92] T. Williamson. On intuitionistic modal epistemic logic. *Journal of Philosophy*, 21(1):63–89, 1992.

Erklärung

gemäss Art. 28 Abs. 2 RSL 05

Name/Vorname:	Marti Michel
Matrikelnummer:	06-213-029
Studiengang:	Informatik Bachelor ☐ Master ☐ Dissertation ☒
Titel der Arbeit:	Contributions to Intuitionistic Epistemic Logic
Leiter der Arbeit:	Prof. Dr. Gerhard Jäger

Ich erkläre hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls der Senat gemäss Artikel 36 Absatz 1 Buchstabe r des Gesetzes vom 5. September 1996 über die Universität zum Entzug des auf Grund dieser Arbeit verliehenen Titels berechtigt ist.

....

Ort/Datum Unterschrift

Lebenslauf

1985	Geboren am 8. Dezember in Jegenstorf
1993–2002	Grundschule Kerzers
2003–2006	Kantonale Matura, Kollegium St. Michael, Freiburg
2006–2012	Bachelorstudium Philosophie an den Universitäten Bern und Freiburg
2012–2013	Masterstudium Mathematik an der Universität Bern
2013–2017	Doktorand bei Prof. Dr. Gerhard Jäger an der Universität Bern, Institut für Informatik, Forschungsgruppe Logic and Theory Group