AN INTUITIONISTIC EPISTEMIC LOGIC FOR ASYNCHRONOUS COMMUNICATION
非同期通信のための直観主義知識論理

by

Yoichi Hirai
平井洋一

A Master Thesis
修士論文

Submitted to
the Graduate School of the University of Tokyo
on February 10, 2010
in Partial Fulfillment of the Requirements
for the Degree of Master of Information Science and Technology
in Computer Science

Thesis Supervisor: Masami Hagiya　萩谷昌己
Professor of Computer Science

ABSTRACT

We apply formal constructive reasoning to asyncyhronous communication. After defining a general-purpose logic called intuitionistic epistemic logic (**IEC** in short), we solve a motivating example problem, characterising waitfree communication logically in response to the abstract simplicial topological characterisation of waitfree computation given by Herlihy, Shavit, Saks and Zaharoglou in the celebrated Gödel Prize winning papers.

Intuitionistic logic is originally a formalisation of a single mathematician whose knowledge increases over time. The logic **IEC** formalises multiple agents who communicate asynchronously and whose knowledge increases over time. The logic **IEC** has a simple language: it has epistemic modality but no temporal modality so that it is simpler than many previous logics for communication. We do not need temporal modality because we regard time as the partial order in the semantics of intuitionistic epistemic logic. Before defining the deduction system, we first extend the informal intuitionistic reading of logical connectives. Precisely, we extend Brouwer–Heyting–Kolmogorov interpretation of logical connectives by adding one clause reagarding the additional epistemic modality K_a. After stating the informal meaning for the modality, we define a deduction system and a Kripke semantics meeting this intuition. Soundness, strong completeness, finite model property, disjunction property and decidability are shown. We also investigate the relationship between **IEC** and classilcal modal logic with multple S4 modalities.

On top of the logic **IEC**, we give an axiom type that characterises sequential consistency for shared memory. The advantage of intuitionistic logic over classical logic is shown in an example where a set of axioms characterises sequential consistency on shared memory. The axioms for sequential consistency are meaningless in classical logic while meaningful in intuitionistic logic. The axioms are similar to the axiom type for prelinerilty. This similarity reflects the analogy between sequential consistency for shared memory scheduling and linearity for Kripke frames: both require antisymmetry on schedules or models.

Finally, under sequential consistency, we give soundness and completeness between a set of logical formulas called waitfree assertions and a set of models called waitfree schedule models.

論文要旨

構成主義的な形式的推論を，非同期通信に応用する．直観主義知識論理と呼ぶ汎用の論理を定義してから，価値を伝えるための例題として，waitfree な通信を論理的に特徴づける．この論理学的な特徴づけは，ゲーデル賞を取った，Herlihy と Shavit と Saks と Zaharoglou とによる，waitfree 計算の抽象単体幾何学的な特徴づけに応えるものである．

直観主義論理はそもそも知識を増大させつづける数学者を形式化した．直観主義知識論理は，非同期に通信をとりあって知識を増大させつづける複数の主体を形式化する．直観主義知識論理の言語は，知識様相はあっても時相様相はないので，既存の通信を扱う多くの論理よりも単純である．時相様相がないのは，直観主義論理の意味論に登場する半順序構造がそのまま時間を表すとみなすからだ．直観主義知識論理の推論体系を定義する前に，直観主義における論理結合子の直観的な読みを拡張する．具体的には，論理結合子の Brower–Heyting–Kolmogorov 解釈に，知識様相 K_α に関する一条を追加する．知識様相の直観的な読みを説明した後に，直観主義知識論理の推論体系と Kripke 意味論を定義する．健全性と強い完全性と有限モデル性と選言性と決定可能性とを示す．さらに，S4 に従う様相を複数もつ古典様相論理との関連を調査する．

直観主義知識論理上に，共有メモリの逐次整合性を特徴づける公理型を与える．この公理型が古典論理では意味を失うが直観主義論理では意味をもつところに，古典論理に対する直観主義論理の優位性がしめされる．この公理型は Kripke モデルの擬線型性を特徴づける公理型に類似している．この類似は，逐次整合性と擬線型性の類似を反映している: どちらも，スケジュールやモデルに反対称性を要求する．

最後に，逐次整合性のもとで，waitfree 主張と呼ばれる論理式たちと，waitfree スケジュールモデルと呼ばれるモデルたちに対して，健全性と完全性を与える．

Acknowledgements

The author thanks Masami Hagiya, who patiently waited for the author, Yoshihiko Kakutani, who reminded the author of the axiom 5, and Tatsuya Abe, who pointed out the fact that Shoenfield's textbook has conservativity immediately after completeness. The author wishes to express his gratitude to the anonymous refrees of the conference PPL2010 for their comments that considerably improved the presentation of Chapter 4.

Contents

List of Figures

Chapter 1

Introduction

In this thesis, we show that formal constructive reasoning is applicable to asynchronous communication. We define a new logical deduction system called intuitionistic epistemic logic. Although there are infinitely many possible deduction systems, we propose this system because we are surprised to see that such a simple and useful logic has never been proposed, or if ever, has not gained popularity.

There are at least two different ways of reasoning about knowledge. In one view of knowledge using Kripke semantics, which classical epistemic logic employs, knowledge is defined as proposition valid in all possible worlds that is possible to an agent. On the other hand, knowledge can be seen as something agents can send and receive. We unify these two notions of knowledge into the semantics of the logic we present. We define the semantics formally in the style of Kripke semantics. At the same time, an extension to BHK-interpretation reveals that asynchronous communication is implicit in the formal definition.

1.1 The Reason for Another Logic

Motivation: reasoning about concurrent systems We give a formal deduction system for reasoning about asynchronous communication. The motivation for doing it is the fact that creating a concurrently working system with asynchronous communication and especially testing and debugging it is notoriously difficult because of nondeterministic scheduling. When the cost of testing and debugging is high, it is reasonable to spend more cost on ensuring correctness of the system at earlier stages like designing phase or implementation phase, not testing and debugging. In order to ensure correctness at an earlier stage, it is crucially important to reason about the system correctly because at such an early stage, knowledge about the system can only

be obtained by reasoning, not by testing.

Method: giving a formal deduction system A formal deduction system mathematically defines available form of reasoning. In order to define reasoning mathematically, a formal deduction system uses languages defined mathematically. The main advantage of the reasoning on a formal deduction system over reasoning in a natural language is the former is independent of most implicit assumptions on which the latter is dependent so that the validity of the former formal reasoning can be checked more rigorously than the latter informal reasoning.

We seek to have a formal deduction system as simple and learnable as possible to reason about asynchronous communication. We choose to give an epistemic logic, i.e., a logic with an operator expressing an agent's knowledge because mentioning agents' knowledge appeals to human intuition. For example, as Halpern and Zuck [16] point out, Bochmann and Gecsei's paper [6] written in 1977 already uses the notion of knowledge when reasoning about protocols:

> Verification ... will correspond ... to finding out whether and in which circumstances the sender ... can "know" that all data ... have been delivered correctly[1].

Previous work presumes a global clock unnecessarily Existing formal epistemic logic for reasoning about communication implicitly or explicitly assume a global clock. Even if they are capable of reasoning about asynchronous communication, they first consider the synchronous case and then define the asynchrony in terms of ignorance of the global situation. This way, asynchronous communication can be dealt with successfully as done in Halpern's famous work [11, 14] However, the procedure of considering the global clock and then forgetting it makes formal reasoning unnecessarily complicated: we propose a formal deduction system whose semantics does not contain the notion of a global clock anywhere.

1.2 Intuitionistic Epistemic Logic

The main contribution of this thesis is giving definition of intuitionistic epistemic logic (**IEC** for short) and investigating it.

[1] The dots ... and a period by the author.

Abstraction of Herlihy and Shavit's topological model In order to reason about general asynchronous communication, we abstracted some important features from the mathematical model for wait-free computation proposed by Herlihy and Shavit [19]. The obtained model is abstract enough so that it can be described as a Kripke model of intuitionistic propositional logic equipped with additional functions on possible worlds.

Two views on knowledge

Original intuitionistic meaning of knowledge Agents in asynchronous systems can obtain knowledge about other agents only by receiving some constructions from them, not by waiting for a fixed length of time. This specific style of knowledge, where obtaining knowledge requires obtaining physical constructions, is the same as the style of knowledge of intuitionistic, constructive reasoners. That is the reason why we deliberately choose intuitionistic not classical meanings for the basic logical connectives, especially $\supset$ and $\vee$, although classical logic is more popularly used among computer scientists and mathematicians. The abstract Kripke model for asynchronous communication can be seen as a description of agents passing around constructions that ensure propositions.

We extend the language of intuitionistic propositional logic with a unary operator K_a, whose meaning can be expressed as: a proof of $K_a\varphi$ is a construction that witnesses agent a's acknowledgement of a proof of φ and also contains the acknowledged proof. This formulation of knowledge is original. This meaning is different from that of classical epistemic logic where the meaning of K_a can be expressed as: $K_a\varphi$ is valid if and only if φ is valid in all possible worlds that agent a thinks possible.

One advantage of our meaning of K_a over that of classical meaning is that it can express communication without the help of another modality. Namely, in our meaning, a proof of K_bK_aP is a construction that is passed from agent a to agent b. On the other hand, in classical meaning, the same formula expresses nothing about communication: K_bK_aP is valid when P is valid in all possible worlds that agent b in any possible world that agent a thinks possible thinks possible.

Intuitionistic logic can be seen as a logic describing an agent whose knowledge increases over time. The logic **IEC** can be seen as a logic describing multiple agents that asynchronously communicate with each other and increase their knowledge. Although **IEC** deals with communication, the logic has only epistemic modalities so that it has simpler syntax than many other logics for communication.

The problem with classical logic Classical logic asserts the Law of Excluded Middle, which states either a proposition or the negation of it is always valid. The Law of Excluded Middle asserts that either a message has reached the intended receiver or it has not reached the intended receiver. We point out that this reasoning assumes the existence of a current state of the world. The notion of the current state implicitly assumes global clock within the use of the adjective "current".

In classical epistemic logic, the description of knowledge relies on the notion of possible worlds. An agent can distinguish some pairs of possible worlds while he or she cannot distinguish the other pairs of possible worlds. When the actual state is one of the possible worlds, agent a knows something when it is valid in all possible worlds indistinguishable from the actual state. In this description of knowledge, all possible states are considered to exist at the same time. Knowledge change can only be modelled via a sequence of such models. The sequence forms a global clock, which is unnecessary to describe asynchronous communication.

For example, in dynamic epistemic logic [8, 40], communication is instantaneous and forms common knowledge. A message changes the model globally. Although no clock appears syntactically, the instantaneous change of models implicitly assumes every agent shares the same uniform progress of time and all events are lined up in a total order. Dynamic epistemic logic might successfully describe human intuition on communication, which is unfortunately incorrect for reasoning about asynchronous communication. In fact, as Halpern [15] pointed out, it is asynchronously impossible to form a new common knowledge.

Aside from dynamic epistemic logic, some logics [35] have numbering in syntax or in semantics that represents a global clock. Although it is possible to understand asynchronous communication using a hypothetical global clock and then forgetting it as in [15] a model without a global clock would be simpler and more preferable according to Occam's razor.

Reducing the number of design choices by identifying intuitionistic relation with temporal relation There were other choices: there have been proposed a huge number of epistemic logics for communication [3–5, 7, 15, 23, 27, 30, 31, 39] and a huge number of intuitionistic modal logics [1, 10, 29, 30, 32]. In both cases, when considered under Kripke semantics, the huge variety of logics comes from the diversity of relationships between two binary relations on the state space. In intuitionistic modal logic, the two relations are: (a) which state is prior to which state with regard to Kripke monotonicity and (b) the modality in which state refers to which state. In

logics for communication, the two relationships are: (a') which state is temporarily prior to which state and (b') from which state to which state a communication occurs.

The semantics of **IEC** uses a binary relation on the states and *functions* on the states instead of additional binary relations. For an agent to know something about another agent, it is necessary to receive something from the other agent. When an agent receives something from another agent, the receiver can identify the sender. We formalised this identification as a function on the states. This choice dramatically limits the room for design choice. Also, we identify relations (a) with (a') and (b) with (b') in order to make the language of **IEC** simpler.

Formalising available reasoning We give a deduction system and show soundness (Theorem 2.5.1), disjunction property (Theorem 2.6.20), strong completeness (Theorem 2.7.10), finite model property (Theorem 2.7.15) and decidability (Theorem 2.7.16).

1.3 Application to Wait-free Communication

Since the semantics for **IEC** is inspired by the topological characterisation of wait-free computation given by Herlihy and Shavit [19], we applied the logic **IEC** to wait-free computation in order to see what change is caused by the abstraction of simplicial complexes to Kripke models.

Sequential consistency The topological characterisation by Herlihy and Shavit [19] implicitly assumes sequential consistency [26] of shared memory. This motivated us to characterise sequential consistency with the axiom type $(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$ in the logic **IEC** for asynchronous computation. Technically, we defined a class of models called sequential models and proved soundness (Lemma 3.2.1) and completeness (Theorem 4.3.4) of the axiom type with respect to the sequential models.

Wait-free communication A waitfree protocol over shared memory [18] assigns a program to each process so that no process waits for another process. Some tasks can be solved by a well-chosen waitfree protocol while the others cannot.

For example, it is waitfreely impossible for both of two processes to attain the input value of the other process. On the other hand, it is waitfreely possible for either one of two processes to attain the input value of the other process. A waitfree protocol that solves this task is:

- process a tells the memory m that φ holds, and then m replies back to a,

- process b tells the memory m that ψ holds, and then m replies back to b.

After this protocol finishes, either φ has been communicated from a to b or ψ has been communicated from b to a.

In the logic **IEC**, this fact is represented by a judgement $K_a K_{\mathsf{m}} K_a \varphi, K_b K_{\mathsf{m}} K_b \psi \vdash_{\mathrm{SC}} K_a K_b \psi \vee K_b K_a \varphi$, which is deducible in **IEC** with sequential consistency axioms (Figure 3.1).

Herlihy and Shavit [19] characterised waitfree computation using simplicial topology. Using their characterisation, Gafni and Koutsoupias [12] showed that it is undecidable whether a task is waitfreely solvable or not. When tasks are restricted to communication defined by a class of logical formulas that we call waitfree assertions, we can characterise waitfreely available communication logically (Theorem 4.3.4) and it is decidable whether a task is waitfreely solvable or not (Theorem 4.4.2).

1.4 Structure of the Paper

The rest of the paper is mostly in the bottom-to-top order. In Chapter 2, we define and examine the syntax and semantics of intuitionistic epistemic logic. In Chapter 3, we characterise sequential consistency of shared memory in **IEC**. In Chapter 4, we characterise waitfree communication under sequential consistency. Chapter 5 compares our work with others. In Chapter 6, we summarise our achievements. In Chapter 7, we treat issues including informal speculation and future work.

1.5 Preliminaries and Notations

We assume inductive definitions using BNF and coinductive definition. $\mathcal{P}(X)$ denotes the powerset of X. For a symbol or a sequence of symbols p, p^+ denotes repetition of p more than zero times and p^* denotes repetition of p more than or equal to zero times.

Chapter 2

Intuitionistic Epistemic Logic

In this chapter, we give a logic called intuitionistic epistemic logic. The logic has epistemic modality K_a in addition to ordinary logical connectives $(\wedge, \vee, \supset, \bot)$ of propositional logic. We explain the meaning of the new modality K_a informally, by extending the Brouwer–Heyting–Kolmogorov interpretation (BHK-interpretation) of logical connectives, which dates back to 1930's (Heyting [21, 22] are cited by Troelstra et al. [38]).

2.1 Formulas

We fix a countably infinite set of propositional symbols $PVar$ and a finite set of agents A. Let $P, Q, \ldots$ run over the propositional symbols.

Definition 2.1.1. *We define a formula φ by the BNF:*

$$\varphi ::= \bot \mid P \mid (K_a\varphi) \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \supset \varphi)$$

where $a \in A$ stands for an agent.

We sometimes omit the parenthesis when no confusion occurs. We use $=$ for syntactic equality of formulas. The notation $(\neg\varphi)$ stands for $(\varphi \supset \bot)$. For a sequence of formula $\Gamma = (\varphi_i)$, the notation $K_a\Gamma$ stands for the sequence $(K_a\varphi_i)$.

2.2 Informal Explanation by BHK-Interpretation

Intuitionistic meanings for logical connectives can be presented as following sentences called BHK-interpretation[1]:

[1] Taken from Troelstra and van Dalen's textbook [38, Ch. 1]: author made notational modification of logical formulas and omission of quantifiers $\forall$ and $\exists$.

(H1) A proof of $\varphi \wedge \psi$ is given by presenting a proof of φ and a proof of ψ.

(H2) A proof of $\varphi \vee \psi$ is given by presenting either a proof of φ or a proof of ψ (plus the stipulation that we want to regard the proof presented as evidence for $\varphi \vee \psi$[2]).

(H3) A proof of $\varphi \supset \psi$ is a construction which permits us to transform any proof of φ into a proof of ψ.

(H4) Absurdity $\perp$ (contradiction) has no proof; a proof of $\neg\varphi$ is a construction which transforms any hypothetical proof of φ into a proof of a contradiction.

In this paper, we consider extending BHK-interpretation with another stipulation for epistemic modality:

(HK) A proof of $K_a\varphi$ is a construction that witnesses agent a's acknowledgement of a proof of φ and also contains the acknowledged proof.

We choose to regard knowledge as acknowledgement of proofs so that the modality K_a informally describes knowledge of agent a. The formalisation of knowledge is different from that in classical epistemic logic, where knowledge is described as a limitation on the ability to distinguish possible worlds.

2.3 Deduction System

The unary operators connect more strongly than the binary operators. We sometimes omit the parentheses when no confusion occurs. We use $=$ for syntactic equality of formulas. The notation $(\neg\varphi)$ stands for $(\varphi \supset \perp)$. For a sequence of formulas $\Gamma = (\varphi_i)_{i\in I}$ or a set of formulas Γ, the notation $K_a\Gamma$ stands for the sequence $(K_a\varphi_i)_{i\in I}$ or the set $\{K_a\varphi \mid \varphi \in \Gamma\}$ respectively.

We give a proof system of **IEC** in natural deduction. Most of the rules are common with intuitionistic propositional logic while some rules are added to define the meaning of the K_a modality.

Definition 2.3.1. *We define the proof system of* **IEC** *by Figure 2.1. The system is presented in the form of usual schemata. A proof diagram is a finite tree of deduction*

[2]In fact, the author considers this as not enough. A proof $\varphi \vee \varphi$ must contain the choice of the left φ or the right φ.

$$(\text{ax})\ \frac{}{\varphi \vdash \varphi} \qquad (\text{w})\ \frac{\Gamma \vdash \varphi}{\psi,\, \Gamma \vdash \varphi} \qquad (\text{c})\ \frac{\varphi,\, \varphi,\, \Gamma \vdash \varphi'}{\varphi,\, \Gamma \vdash \varphi'} \qquad (\text{e})\ \frac{\Gamma, \varphi, \psi,\, \Gamma' \vdash \varphi'}{\Gamma,\, \psi, \varphi,\, \Gamma' \vdash \varphi'}$$

$$(\wedge\text{-E}_0)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} \qquad (\wedge\text{-I})\ \frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \varphi \wedge \psi} \qquad (\wedge\text{-E}_1)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$(\vee\text{-I}_0)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \qquad (\vee\text{-I}_1)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi}$$

$$(\vee\text{-E})\ \frac{\Gamma \vdash \psi_0 \vee \psi_1 \qquad \Gamma,\, \psi_0 \vdash \varphi \qquad \Gamma,\, \psi_1 \vdash \varphi}{\Gamma \vdash \varphi}$$

$$(\supset\text{-I})\ \frac{\varphi,\, \Gamma \vdash \psi}{\Gamma \vdash \varphi \supset \psi} \qquad (\supset\text{-E})\ \frac{\Gamma \vdash \psi_0 \supset \psi_1 \qquad \Gamma \vdash \psi_0}{\Gamma \vdash \psi_1} \qquad (\bot\text{-E})\ \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi} \qquad (\text{T})\ \frac{\Gamma \vdash K_a\varphi}{\Gamma \vdash \varphi}$$

$$(\text{ispec})\ \frac{\Gamma \vdash K_a\varphi}{\Gamma \vdash K_aK_a\varphi} \qquad (\text{nec})\ \frac{\Gamma \vdash \varphi}{K_a\Gamma \vdash K_a\varphi} \qquad (\vee K)\ \frac{\Gamma \vdash K_a(\varphi \vee \psi)}{\Gamma \vdash K_a\varphi \vee K_a\psi}$$

Figure 2.1: Deduction rules of **IEC**. (ax) stands for axiom, (w) for weakening, (c) for contraction, (e) for exchange, (ispec) for introspection and (nec) for necessitation. ($\Diamond$-I) denotes the introduction rule for connective $\Diamond$. ($\Diamond$-E) denotes the elimination rule for connective $\Diamond$.

rules with one bottom node with the following property: when a node has a judgement above the line, there is a node immediately above it and the above node has the same judgement below the line.

Rationales for the rules on modalities While the rules (T), (ispec) and (nec) are admissible in classical epistemic logic, we have an additional rule ($\vee K$) which needs explanation. In this paragraph, we are going to give a rationale for the rule ($\vee K$) with the help of BHK-interpretation given in Section 2.2. A proof for the premise of the rule ($\vee K$) is a construction that witnesses agent a's acknowledgement of a proof of $\varphi \vee \psi$. Since a proof of $\varphi \vee \psi$ is either a proof of φ or a proof of psi, agent a's acknowledge of a proof of $\varphi \vee \psi$ implies either agent a's acknowledgement of a proof of φ or agent a's acknowledgement of a proof of ψ.

Also, we are informally assuming logical omniscience of the agents by rule (nec), that is, we assume agents have complete command on intuitionistic epistemic logic so that they acknowledge every formulas deducible from the set of formulas they acknowledge. We do not try to convince that every conceivable agent has logical omniscience. We only speculate that agents without logical omniscience are hard to

represent in a formal system.

Notational conventions For a set of formula Γ and a formula φ, $\Gamma \vdash \varphi$ denotes a relation where there is such a finite sequence Γ_0 that $\Gamma_0 \vdash \varphi$ is deducible and that Γ_0 contains only formulas in Γ.

2.4 Semantics

We define validity of a formula on a state in a model. A model is a Kripke model for propositional intuitionistic logic equipped with an additional mapping $f_a : W \to W$ for each agent $a \in A$ where W is the set of possible states. Informally[3], the function f_a represents the view of agent a. When the current state is $w \in W$, agent a sees that the current state is $f_a(w) \in W$, in other words, agent a knows everything valid in $f_a(w)$. As a special consequence, agent a knows that agent b sees that the current state is $f_b(f_a(w)) \in W$. This model is an abstraction of Herlihy and Shavit's model of waitfree computation [19]. See Section 7.1 for details.

Definition 2.4.1. *A model $\langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$ is a tuple with following properties:*

1. *$\langle W, \preceq\rangle$ is a partial order,*
2. *$f_a \colon W \to W$ is a function satisfying*
   (a) *(descendance) $f_a(w) \preceq w$,*
   (b) *(idempotency) $f_a(f_a(w)) = f_a(w)$, and*
   (c) *(monotonicity) $w \preceq v$ implies $f_a(w) \preceq f_a(v)$*

   for all $v, w \in W$,
3. *$\rho \colon PVar \to \mathcal{P}(W)$ is a function such that each $\rho(P)$ is upward-closed with respect to $\preceq$, i.e., $w' \succeq w \in \rho(P)$ implies $w' \in \rho(P)$.*

With the informal account in mind, the conditions on f_a have rationales: descendance condition says an agent a recognises only truth, idempotency says an agent a recognises that a recognises something whenever the agent a recognises that thing, and monotonicity says an agent a does not forget things recognised. Differently from classical epistemic logic, there is no distinction between global states and local states.

The valuation ρ for propositional variables in $PVar$ is extended into validity relation $\models$ for all formulas in **Fml**.

[3]This account is informal in that we do not attempt to define the terms "view" and "current state".

Definition 2.4.2. *We define the validity relation* $\models$ *of a model* $\langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$*, a state* $w \in W$ *of the model and a formula* φ*. Let us fix a model* $M = \langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$*. The definition of* $M, w \models \varphi$ *is inductive on the structure of* φ*.*

(Case $\varphi = \bot$**)** $M, w \models \bot$ *never holds.*

(Case $\varphi = P$**)** $M, w \models P$ *if and only if* $w \in \rho(P)$*.*

(Case $\varphi = K_a\psi$**)** $M, w \models K_a\psi$ *if and only if* $M, f_a(w) \models \psi$*.*

(Case $\varphi = \psi_0 \wedge \psi_1$**)** $M, w \models \psi_0 \wedge \psi_1$ *if and only if both* $M, w \models \psi_0$ *and* $M, w \models \psi_1$ *hold.*

(Case $\varphi = \psi_0 \vee \psi_1$**)** $M, w \models \psi_0 \vee \psi_1$ *if and only if either* $M, w \models \psi_0$ *or* $M, w \models \psi_1$ *holds.*

(Case $\varphi = \psi_0 \supset \psi_1$**)** $M, w \models \psi_0 \supset \psi_1$ *if and only if for any* $w' \in W$ *with* $w' \succeq w$*, the validity* $M, w' \models \psi_0$ *implies the validity* $M, w' \models \psi_1$*.*

Next, we show that the restriction on the valuation ρ is preserved by the extension to validity $\models$. Informally, this theorem presents the limitation of the logic **IEC**: it can only deal with propositions whose validity is preserved by progress with respect to the partial order $\preceq$ belonging to the model.

Theorem 2.4.3 (Kripke monotonicity)**.** $M, w \models \varphi$ *and* $w \preceq v$ *imply* $M, v \models \varphi$*.*

Proof. By structural induction on φ. We fix a model M and we abbreviate $M, w \models \varphi$ into $w \models \varphi$.

(Case $\varphi = \bot$**)** The assumption $w \models \bot$ never holds.

(Case $\varphi = P$**)** By the restriction on ρ in Definition 2.4.1.

(Case $\varphi = K_a\psi$**)** By monotonicity of f_a and induction hypothesis.

(Case $\varphi = \psi_0 \wedge \psi_1$**)** Assume $w \models \psi_0 \wedge \psi_1$. Both $w \models \psi_0$ and $w \models \psi_1$ hold. By induction hypothesis, $v \models \psi_0$ and $v \models \psi_1$ hold. Thus $v \models \psi_0 \wedge \psi_1$ holds.

(Case $\varphi = \psi_0 \vee \psi_1$**)** Similarly by induction hypothesis.

(Case $\varphi = \psi_0 \supset \psi_1$**)** By definition of $\models$.

□

Semantics of judgements We introduce some notations which look similar to the judgements appearing in the deduction system. Being aware of the different definitions of $\vdash$ and $\models$, we are going to compare the two relations $\vdash$ and $\models$ in the next sections.

Notation 2.4.4. *For a model M and a state w of the model, we write $M, w \models \Gamma$ when the validity $M, w \models \varphi$ holds for any formula φ in Γ.*

Notation 2.4.5. *$\Gamma \models \varphi$ stands for the relation of formula sequences Γ and a formula φ that holds if and only if for any model M and $w \in M$, $M, w \models \Gamma$ implies $M, w \models \varphi$.*

Definition 2.4.6. *$\Gamma \models \varphi$ stands for the relation of a set of a formulas Γ and a formula φ where $M, w \models \Gamma$ implies $M, w \models \varphi$ for any model M and a state $w \in M$.*

For a sequence of formulas Γ, we let $u(\Gamma)$ denote the set of formulas appearing in Γ. We abbreviate $u(\Gamma) \models \varphi$ into $\Gamma \models \varphi$. We will sometimes write Γ instead of $u(\Gamma)$ for the sake of brevity.

Definition 2.4.7. *A set of formulas Γ is consistent if and only if $\Gamma \not\models \bot$.*

2.5 Soundness

Soundness is the single most important feature of a formal deductive system because the main reason for using a formal deductive system is it ensures correct reasoning. We regard the defined semantics as a standard for correct reasoning and show that the deduction systems of **IEC** meets that standard. Soundness ensures a formula provable in **IEC** is valid in any state of any model. At the same time, we show a stronger notion: a formula provable under a set of assumptions is always valid whenever the assumptions are valid.

Theorem 2.5.1 (Soundness)**.** *$\Gamma \vdash \varphi$ implies $\Gamma \models \varphi$.*

Proof. We prove soundness with induction on the definition of $\vdash$. We fix a model M and we abbreviate $M, w \models \varphi$ into $w \models \varphi$.

(ax)(w)(c)(e) Trivial.

($\supset$-I) Assume $\Gamma, \varphi \models \psi$. Assume $w \models \Gamma$. Also assume that there is such a state w' in M that $w' \succeq w$ and $w' \models \varphi$ hold. By Lemma 2.4.3, $w' \models \Gamma$ holds. Since $\Gamma, \varphi \models \psi$, the relation $\Gamma, w' \models \psi$ holds.

($\supset$-E) Assume $\Gamma \models \varphi \supset \psi$ and $\Gamma \models \varphi$. By the second assumption, $w \models \varphi$ holds. The first assumption says $w \models \varphi \supset \psi$. Since $w \succeq w$, the relation $w \models \psi$ holds.

($\wedge$-I)($\vee$-I$_0$)($\vee$-I$_1$)($\vee$-E)($\wedge$-E$_0$)($\wedge$-E$_1$) Trivial.

(T) Assume $w \models \Gamma$. By induction hypothesis, the validity $w \models K_a\varphi$ holds. By definition of $\models$, $f_a(w) \models \varphi$ holds. Since $f_a(w) \preceq w$, Lemma 2.4.3 says $w \models \varphi$.

(inspec) Assume $w \models \Gamma$. By induction hypothesis, the validity $w \models \varphi$ holds. By definition of $\models$, $f_a(w) \models \varphi$ holds. Since f_a is idempotent, $f_a(f_a(w)) \models \varphi$. Applying the definition of $\models$ again in the opposite direction, we obtain $w \models K_a\varphi$.

(nec) Assume $\Gamma \models \varphi$ and $w \models K_a\Gamma$ hold. Since $w \models \Gamma$, the first assumption says $w \models \varphi$. By definition of $\models$, the relation $w \models K_a\varphi$ holds.

($\vee K_a$) Assume $\Gamma \models K_a(\varphi \vee \psi)$. For any state w of any model M, assume $w \models K_a(\varphi \vee \psi)$. By the definition of $\models$, $f_a(w) \models \varphi \vee \psi$. Applying the definition of $\models$ again, either $f_a(w) \models \varphi$ or $f_a(w) \models \psi$ holds. This implies either $w \models K_a\varphi$ or $w \models K_a\psi$ holds. We have $w \models K_a\varphi \vee K_a\psi$.

□

2.6 Disjunction Property

We modify Aczel's slash and prove disjunction property. We referred Troelstra and van Dalen's textbook [38, 3.5] for the proof of disjunction property of intuitionistic propositional logic.

The main originality of this section is the following definition of the function f_a. Informally, for a set Γ of formulas, $f_a(\Gamma)$ is agent a's view of the set Γ.

Definition 2.6.1. *For an agent $a \in A$, we define two functions $g_a, f_a \colon \mathcal{P}(\mathbf{Fml}) \to \mathcal{P}(\mathbf{Fml})$ as*

$$g_a(\Gamma) = \{\varphi \in \mathbf{Fml} \mid (K_a)^+\varphi \in \Gamma \text{ and } \varphi \text{ does not begin with } K_a\},$$
$$f_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma) \cup \{\varphi \in \mathbf{Fml} \mid \Gamma \vdash \bot\}.$$

where $(K_a)^+$ denotes a finite repetition of at least one (K_a).

2.6.1 Properties of the Auxiliary Functions

Since the definition for the auxiliary function f_a is not very straightforward, it is worthwhile checking some properties of it like monotonicity and idempotency. Actually, in the next section, a variant of this function f_a will be used for constructing a model so that its monotonicity and idempotency are necessary.

Proposition 2.6.2. $\Gamma \subseteq \Delta$ *implies* $g_a(\Gamma) \subseteq g_a(\Delta)$.

Proof. By the form of definition of g_a in Definition 2.6.1. □

Proposition 2.6.3. $g_a(\Delta \cup \Gamma) = g_a(\Delta) \cup g_a(\Gamma)$.

Proof. By the form of definition of g_a in Definition 2.6.1. □

Proposition 2.6.4. $f_a(\Delta \cup \Gamma)$ *is equal to* $f_a(\Delta) \cup f_a(\Gamma)$ *provided* $\Delta \cup \Gamma \nvdash \bot$.

Proof.

$$\begin{aligned} f_a(\Delta \cup \Gamma) &= g_a(\Delta \cup \Gamma) \cup K_a g_a(\Delta \cup \Gamma) && \text{(definition of } f_a\text{)} \\ &= g_a(\Delta) \cup g_a(\Gamma) \cup K_a g_a(\Delta) \cup K_a g_a(\Gamma) && \text{(Proposition 2.6.3)} \\ &= g_a(\Delta) \cup K_a g_a(\Delta) \cup g_a(\Gamma) \cup K_a g_a(\Gamma) && \text{(reordering)} \\ &= f_a(\Delta) \cup f_a(\Gamma) && \text{(definition of } f_a\text{)}. \end{aligned}$$

□

Proposition 2.6.5. $\Gamma \subseteq \Delta$ *implies* $f_a(\Gamma) \subseteq f_a(\Delta)$.

Proof. If $\Delta \vdash \bot$, $f_a(\Gamma) \subseteq \mathbf{Fml} = f_a(\Delta)$. Otherwise, there exists a set Γ' with $\Gamma \cup \Gamma' = \Delta$. Using Proposition 2.6.4 suffices. □

Proposition 2.6.6. *For any* $\varphi \in K_a f_a(\Gamma)$, $\Gamma \vdash \varphi$ *holds.*

Proof. $\varphi = K_a\psi$ where $\psi \in f_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma) \cup \{\varphi \in \mathbf{Fml} \mid \Gamma \vdash \bot\}$.

(Case $\psi \in g_a(\Gamma)$) By definition of g_a, $(K_a)^+\psi \in \Gamma$. By rule (T), $\Gamma \vdash K_a\psi$. This is what we sought: $\Gamma \vdash \varphi$.

(Case $\psi \in K_a g_a(\Gamma)$) $\psi = K_a\psi'$ where $\psi' \in g_a(\Gamma)$. By the same argument, $\Gamma \vdash K_a\psi'$. By rule (inspec), $\Gamma \vdash K_aK_a\psi'$. This is what we sought: $\Gamma \vdash \varphi$.

(Case $\Gamma \vdash \bot$) By rule ($\bot$-E), $\Gamma \vdash \varphi$ holds.

□

Proposition 2.6.7. *For any* $\varphi \in f_a(\Gamma)$, $\Gamma \vdash \varphi$ *holds.*

Proof. $K_a\varphi \in K_a f_a(\Gamma)$. By Proposition 2.6.6, $\Gamma \vdash K_a\varphi$ holds. By rule (T), deducibility $\Gamma \vdash \varphi$ holds. □

Proposition 2.6.8. $f_a(f_a(\Gamma)) = f_a(\Gamma)$.

Proof. If $\Gamma \nvdash \bot$, by Proposition 2.6.7, $f_a(\Gamma) \nvdash \bot$ also holds.

$$\begin{aligned} f_a(f_a(\Gamma)) &= f_a(g_a(\Gamma) \cup K_a g_a(\Gamma)) && \text{(definition of } f_a\text{)} \\ &= f_a(g_a(\Gamma)) \cup f_a(K_a g_a(\Gamma)) && \text{(Proposition 2.6.4)} \\ &= \emptyset \cup f_a(\Gamma) && \text{(definitions of } f_a \text{ and } g_a\text{)} \\ &= f_a(\Gamma). \end{aligned}$$

Otherwise, if $\Gamma \vdash \bot$, $f_a(\Gamma) = \mathbf{Fml} = f_a(f_a(\Gamma))$. □

2.6.2 The Slash Relation

We use f_a defined above to extend Aczel's slash relation to the language of **IEC**. We add a clause for K_a modalities where we use the function f_a.

Definition 2.6.9. *We define the slash relation* $|$ *as follows:*

$$\begin{aligned} \Gamma \mid \bot &\iff \Gamma \vdash \bot, \\ \Gamma \mid P &\iff \Gamma \vdash P, \\ \Gamma \mid K_a\varphi &\iff f_a(\Gamma) \mid \varphi \\ \Gamma \mid \varphi \wedge \psi &\iff \Gamma \mid \varphi \textit{ and } \Gamma \mid \psi, \\ \Gamma \mid \varphi \vee \psi &\iff \Gamma \mid \varphi \textit{ or } \Gamma \mid \psi, \\ \Gamma \mid \varphi \supset \psi &\iff \Delta \mid \varphi \textit{ implies } \Delta \mid \psi \textit{ for any } \Delta \supseteq \Gamma \textit{ and also } \Gamma \vdash \varphi \supset \psi. \end{aligned}$$

Lemma 2.6.10. $\Gamma \mid \varphi \Rightarrow \Gamma \vdash \varphi$.

Proof. By induction on φ.

(Case $\varphi = \bot$)(Case $\varphi = P$) By definition of $|$.

(Case $\varphi = K_a\psi$) The assumption $\Gamma \mid K_a\psi$ is equivalent to $f_a(\Gamma) \mid \psi$. By induction hypothesis, $f_a(\Gamma) \vdash \psi$. By rule (nec), $K_a f_a(\Gamma) \vdash K_a\psi$. By Proposition 2.6.6, the deducibility $\Gamma \vdash K_a\psi$ holds.

(Case $\varphi = \psi_0 \wedge \psi_1$) $\Gamma \mid \psi_0 \wedge \psi_1$. By definition of $|$, Both $\Gamma \mid \psi_0$ and $\Gamma \mid \psi_1$ hold. By induction hypothesis, both $\Gamma \vdash K_x\psi_0$ and $\Gamma \vdash K_x\psi_1$ hold. By logic, $\Gamma \vdash K_x(\psi_0 \wedge \psi_1)$ holds.

(Case $\varphi = \psi_0 \vee \psi_1$) Similar to the case above.

(Case $\varphi = \psi_0 \supset \psi_1$) By definition of $|$.

□

Lemma 2.6.11. $\Gamma \mid \varphi$ *and* $\Gamma \subseteq \Delta$ *imply* $\Delta \mid \varphi$.

Proof. By induction on φ.

(Case $\varphi = \bot$) (Case $\varphi = P$) (Case $\varphi = \psi_0 \supset \psi_1$) By definition of the slash relation $\mid$.

(Case $\varphi = \psi_0 \wedge \psi_1$) (Case $\varphi = \psi_0 \vee \psi_1$) Directly from induction hypotheses.

(Case $\varphi = K_a\psi$) By Proposition 2.6.5, $f_a(\Gamma) \subseteq f_a(\Delta)$ holds. By induction hypothesis, $f_a(\Gamma) \mid \psi$ implies $f_a(\Delta) \mid \psi$, which is equivalent to $\Delta \mid \varphi$ holds.

□

Lemma 2.6.12. *For any set* Γ *of formulas with* $\Gamma \mid \psi$ *for all* $\psi \in \Gamma$, $\varphi \in g_a(\Gamma)$ *implies* $f_a(\Gamma) \mid \varphi$.

Proof. By definition of g_a, $(K_a)^{(n)}\varphi \in \Gamma$ for some $n \geq 1$, where $(K_a)^{(n)}$ denotes an n-time repetition of K_a's. By assumption, $\Gamma \mid (K_a)^{(n)}\varphi$. By definition of $\mid$, $f_a^{(n)}(\Gamma) \mid \varphi$. Since f_a is idempotent (Proposition 2.6.8), $f_a(\Gamma) \mid \varphi$. □

This definition of hereditary f-closed formulas is original.

Definition 2.6.13. *A hereditary* f*-closed set* Γ *is coinductively defined as:* Γ *is a hereditary* f*-closed set if and only if* $f_a(\Gamma)$ *is hereditary* f*-closed and* $f_a(\Gamma) \subseteq \Gamma$ *for all* $a \in A$.

Equivalently, we can define the negation inductively as:

- if $f_a(\Gamma) \not\subseteq \Gamma$, Γ is not a hereditary f-closed set.
- if Γ is not a hereditary f-closed set, $f_a(\Gamma)$ is not a hereditary f-closed set.

For example, the set $\Gamma = \{K_bK_aK_aP\}$ is not hereditary f-closed because $f_b(\Gamma)$ is not hereditary f-closed. $f_b(\Gamma)$ is not hereditary f-closed because $K_aP \in f_a(f_b(\Gamma))$ while $K_aP \notin f_b(\Gamma)$.

Since $f_a(\emptyset) = \emptyset$ for any $a \in A$, $\emptyset$ is a hereditary f-closed set.

Lemma 2.6.14. *For any hereditary* f*-closed set* Γ *and a formula* φ, $\Gamma \vdash \bot$ *implies* $\Gamma \mid \varphi$.

Proof. By induction on φ.

(Case $\varphi = \bot$) (Case $\varphi = P$) $\Gamma \vdash \varphi$ implies $\Gamma \mid \varphi$ because φ is atomic.

(Case $\varphi = K_a\psi$) Since $f_a(\Gamma)$ is also hereditary f-closed and $\bot \inf_a(\Gamma)$, by induction hypothesis, $f_a(\Gamma) \mid \psi$. This is equivalent to $\Gamma \mid K_a\psi$.

(Case $\varphi = \psi_0 \wedge \psi_1$) (Case $\varphi = \psi_0 \vee \psi_1$) Directly from induction hypothesis.

(Case $\varphi = \psi_0 \supset \psi_1$) By rule ($\bot$-E), $\Gamma \vdash \psi_0 \supset \psi_1$. For all $\Delta \supset \Gamma$, by induction hypothesis, $\Delta \mid \psi_1$ holds. These two facts show $\Delta \mid \psi_0 \supset \psi_1$.

□

Lemma 2.6.15. *For any hereditary f-closed set Γ of formulas, if $\Gamma \mid \psi$ for all $\psi \in \Gamma$, $f_a(\Gamma) \mid \varphi$ for all $\varphi \in f_a(\Gamma)$.*

Proof. By induction on the structure of φ. However, most cases are uniformly treated in the last clause.

(Case $\varphi = K_x\psi$) Assume $K_x\psi \in f_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma) \cup \{\theta \in \mathbf{Fml} \mid \Gamma \vdash \bot\}$.

- **(Case $K_x\psi \in g_a(\Gamma)$)** By Lemma 2.6.12, $f_a(\Gamma) \mid K_x\psi$.
- **(Case $K_x\psi \in K_a g_a(\Gamma)$)** Note $x = a$. By Lemma 2.6.12, $f_a(\Gamma) \mid \psi$ holds. Since f_a is idempotent, $f_a(f_a(\Gamma)) \mid \psi$ holds. By definition of $\mid$, $f_a(\Gamma) \mid K_a\psi$.
- **(Case $\Gamma \vdash \bot$)** $f_a(\Gamma) \vdash \bot$ also holds. By Lemma 2.6.14, $f_a(\Gamma) \mid \varphi$ holds.

(Other cases) Assume $\varphi \in f_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma) \cup \{\theta \in \mathbf{Fml} \mid \Gamma \vdash \bot\}$. If $\Gamma \vdash \bot$, by Lemma 2.6.14 and definition of f_a, $f_a(\Gamma) \mid \varphi$. Otherwise, since the formula φ does not begin with K_a, $\varphi \in g_a(\Gamma)$. By Lemma 2.6.12, $f_a(\Gamma) \mid \varphi$.

□

Lemma 2.6.16. $\Gamma \mid K_a\varphi \Rightarrow \Gamma \mid \varphi$ *if* Γ *is f_a-closed.*

Proof. Immediate from Lemma 2.6.11. □

Lemma 2.6.17. $\Gamma \mid \psi$ *and* $\Gamma \cup \{\psi\} \mid \varphi$ *imply* $\Gamma \mid \varphi$.

Proof. By induction on φ.

(Case $\varphi = \bot$) (Case $\varphi = P$) Since $\Gamma \mid \psi$, by Lemma 2.6.10, the deducibility $\Gamma \vdash \psi$ holds. Likewise since $\Gamma \cup \{\psi\} \mid \varphi$, the deducibility $\Gamma \cup \{\psi\} \vdash \varphi$ holds. These combined imply $\Gamma \vdash \varphi$. By definition of the slash relation $\mid$, the relation $\Gamma \mid \varphi$ holds because φ is atomic.

(Case $\varphi = \psi_0 \vee \psi_1$) **(Case $\varphi = \psi_0 \wedge \psi_1$)** Directly from induction hypotheses.

(Case $\varphi = K_a\theta$) Since $\Gamma \cup \{\psi\} | K_a\theta$, by definition of the slash relation $|$, $f_a(\Gamma \cup \{\psi\}) | \theta$ holds. If $\Gamma \cup \{\psi\} \vdash \bot$, by the assumption, $\Gamma \vdash \bot$. Thus, by Lemma 2.6.14, $\Gamma \vdash \varphi$ holds. Otherwise, since $f_a(\Gamma \cup \{\psi\}) = f_a(\Gamma) \cup f_a(\{\psi\})$, we have $f_a(\Gamma) \cup f_a(\{\psi\}) | \theta$. If $\psi = K_a\psi'$, $\Gamma \,|\, \psi$ is equivalent to $f_a(\Gamma) \,|\, \psi'$. By induction hypothesis, $f_a(\Gamma) \,|\, \theta$. This is equivalent to $f_a(\Gamma) \,|\, K_a\theta$. This is what we sought: $f_a(\Gamma) \,|\, \varphi$. Otherwise, if ψ does not begin with K_a, $f_a(\{\psi\}) = \emptyset$. Thus, $f_a(\Gamma) \,|\, \theta$. This means $\Gamma \,|\, K_a\theta$.

(Case $\varphi = \psi_0 \supset \psi_1$) Since $\Gamma \cup \{\psi\} \,|\, \psi_0 \supset \psi_1$, by Lemma 2.6.10, $\Gamma \cup \{\psi\} \vdash \psi_0 \supset \psi_1$ holds. In addition to this, $\Delta \cup \{\psi\} \,|\, \psi_0$ implies $\Delta \cup \{\psi\} \,|\, \psi_1$ for any $\Delta \supseteq \Gamma$. We claim that $\Delta \,|\, \psi_0$ implies $\Delta \,|\, \psi_1$ for any $\Delta \supseteq \Gamma$. To show that, we assume $\Delta \,|\, \psi_0$. By Lemma 2.6.11, $\Delta \cup \{\psi\} \,|\, \psi_0$ holds. By assumption, $\Delta \cup \{\psi\} \,|\, \psi_1$ holds. By induction hypothesis, $\Delta \,|\, \psi_1$ holds. We have shown that $\Delta \,|\, \psi_0$ implies $\Delta \,|\, \psi_1$. In addition to this, by $\Gamma \vdash \psi$ and $\Gamma \cup \{\psi\} \vdash \psi_0 \supset \psi_1$, the deducibility $\Gamma \vdash \psi_0 \supset \psi_1$ holds. The slash relation $\Gamma \,|\, \psi_0 \supset \psi_1$ has been proved.

□

Lemma 2.6.18. *If Γ and Δ are provably equivalent and satisfy $f_a(\Gamma) = f_a(\Delta)$ for all $a \in A$, $\Gamma \,|\, \varphi$ is equivalent to $\Delta \,|\, \varphi$.*

Proof. By the form of the definition of the slash relation $|$. □

2.6.3 Disjunction Property

The standard proof for disjunction property is extended to the logic **IEC**.

Theorem 2.6.19. *For any hereditary f-closed set Γ of formulas, if $\Gamma \,|\, \varphi$ holds for any $\varphi \in \Gamma$, $\Gamma \vdash \varphi$ implies $\Gamma \,|\, \varphi$.*

Proof. By induction on definition of $\Gamma \vdash \varphi$.

(ax) **(w)** **(c)** **(e)** Trivial.

($\wedge$-E$_i$) **($\wedge$-I)** **($\vee$-I$_i$)** By definition of the slash relation $|$.

($\vee$-E) $$\frac{\Gamma \vdash \psi_0 \vee \psi_1 \qquad \Gamma, \psi_0 \vdash \varphi \qquad \Gamma, \psi_1 \vdash \varphi}{\Gamma \vdash \varphi}$$

By an induction hypothesis, $\Gamma \,|\, \psi_0 \vee \psi_1$ holds. By definition of the slash relation, either $\Gamma \,|\, \psi_0$ or $\Gamma \,|\, \psi_1$ holds.

(Case $\Gamma \mid \psi_0$) By another induction hypothesis, $\Gamma \cup \{\psi_0\} | \varphi$ holds. By Lemma 2.6.17, $\Gamma \mid \varphi$ holds.

(Case $\Gamma \mid \psi_1$) Similar.

($\supset$-I) $\dfrac{\varphi, \Gamma \vdash \psi}{\Gamma \vdash \varphi \supset \psi}$

By induction hypothesis, $\varphi \cup \Gamma \mid \psi$ holds. Thus for any $\Delta \supseteq \Gamma$, $\varphi \cup \Delta \mid \psi$ holds. $\Delta \mid \varphi$ implies $\Delta \mid \psi$ by Lemma 2.6.17. This fact and the deducibility $\Gamma \vdash \varphi \supset \psi$ imply $\Gamma \mid \varphi \supset \psi$.

($\supset$-E) $\dfrac{\Gamma \vdash \psi_0 \supset \psi_1 \qquad \Gamma \vdash \psi_0}{\Gamma \vdash \psi_1}$

By induction hypothesis, $\Gamma \mid \psi_0 \supset \psi_1$ holds. By definition of the slash relation, $\Gamma \mid \psi_0$ implies $\Gamma \mid \psi_1$. Actually, $\Gamma \mid \psi_0$ holds by an induction hypothesis. Thus, $\Gamma \mid \psi_1$ holds.

($\bot$-E) By Lemma 2.6.14.

(T) $\dfrac{}{K_a\varphi \vdash \varphi}$

Assume $K_a\varphi \in \Gamma$. By assumption of the theorem, $\Gamma \mid K_a\varphi$. Since Γ is f_a-closed, by Lemma 2.6.16, $\Gamma \mid \varphi$.

(nec) $\dfrac{\Delta \vdash \varphi}{K_a\Delta \vdash K_a\varphi}$

We can assume $K_a\Delta \subseteq \Gamma$ and that $\varphi \in \Gamma$ implies $\Gamma \mid \varphi$. Also, by induction hypothesis, any Γ' with $\Delta \subseteq \Gamma'$ and $\psi \in \Gamma' \Rightarrow \Gamma' \mid \psi$, $\Gamma' \mid \varphi$ holds. Since Δ is a finite sequence, there exists a natural number n with $\Delta \subseteq f_a(\Gamma) \cup K_a f_a(\Gamma) \cup \cdots \cup (K_a)^{(n)} f_a(\Gamma)$. By induction hypothesis, $f_a(\Gamma) \cup K_a f_a(\Gamma) \cup \cdots \cup (K_a)^{(n)} f_a(\Gamma) \mid \varphi$ holds. By Lemma 2.6.18, this is equivalent to $f_a(\Gamma) \mid \varphi$. By definition of $|$, $\Gamma \mid K_a\varphi$ holds.

($\vee K$) $\dfrac{}{K_a(\varphi \vee \psi) \vdash (K_a\varphi) \vee K_a\psi}$

The proof can be pictorially shown as follows:

$$
\begin{aligned}
K_a(\varphi \vee \psi) &\Longrightarrow \Gamma \mid K_a(\varphi \vee \psi) && \text{(assumption)} \\
&\Longleftrightarrow f_a(\Gamma) \mid \varphi \vee \psi && \text{(definition of the slash relation } \mid) \\
&\Longleftrightarrow f_a(\Gamma) \mid \varphi \text{ or } f_a(\Gamma) \mid \psi && \text{(definition of the slash relation } \mid) \\
&\Longleftrightarrow \Gamma \mid K_a\varphi \text{ or } \Gamma \mid K_a\psi && \text{(definition of the slash relation } \mid) \\
&\Longleftrightarrow \Gamma \mid K_a\varphi \vee K_a\psi && \text{(definition of the slash relation } \mid).
\end{aligned}
$$

□

Using the apparatus prepared above, we can finally show disjunction property, which is the standard for constructive logic.

Theorem 2.6.20 (Disjunction property)**.** *If* $\vdash \varphi \vee \psi$ *holds, either* $\vdash \varphi$ *or* $\vdash \psi$ *holds.*

Proof. Taking $\Gamma = \emptyset$ in Theorem 2.6.19, $\vdash \varphi \vee \psi$ implies $\emptyset \mid \varphi$ or $\emptyset \mid \psi$. By Lemma 2.6.10, either $\vdash \varphi$ or $\vdash \psi$ holds. □

2.7 Strong Completeness and Finite Model Property

In this section, we show strong completeness and finite model property. Since both proofs contain model construction, most parts of both proofs can be written in the same lemmas. This utilisation of similarity of finite model property and strong completeness is originally the idea of Sato [35].

Definition 2.7.1. *We modify* f_a *introduced in the last section (Definition 2.6.1) and define* f'_a *as:*

$$f'_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma).$$

For some pages, we argue about a set of formula Ω. Later, when we show strong completeness, we take Ω to be the whole set of well formed formulas. Also, when we show finite model property, we take Ω to be the set of the subformulas of a certain formula. This model construction is inspired by Sato's paper [35] and Troelstra and van Dalen's textbook [38]. However, the notion of f'-subformula-closed sets is new and original.

Definition 2.7.2. *For a set of formulas* Ω*, a set of formulas* $\Gamma \subseteq \Omega$ *is* Ω*-saturated if and only if*

1. Γ *is* Ω*-deductively closed, i.e.,* $\Gamma \vdash \varphi \in \Omega \Rightarrow \varphi \in \Gamma$*,*

2. $\Gamma \vdash \varphi \vee \psi \Rightarrow \Gamma \vdash \varphi$ *or* $\Gamma \vdash \psi$ *if* $\varphi, \psi \in \Omega$,

3. $\Gamma \nvdash \bot$.

Definition 2.7.3. *A hereditary f'-subformula-closed set Γ is coinductively defined as: Γ is a hereditary f'-subformula-closed set if and only if $f'_a(\Gamma)$ is hereditary f'-closed, Γ is closed for taking subformulas and $f'_a(\Gamma) \subseteq \Gamma$.*

Definition 2.7.4. *We define $s_a(\varphi)$ inductively on φ:*

$$s_a(\varphi) = \begin{cases} s_a(K_a\psi) & \text{(if } \varphi = K_aK_a\psi\text{)}, \\ \varphi & \text{(otherwise)}. \end{cases}$$

The function s_a replaces every K_aK_a with K_a repeatedly so that there are no K_aK_a occurrences left.

Lemma 2.7.5. *For a hereditary f'-subformula-closed set Ω, if Γ is an Ω-saturated set, $f_a(\Gamma)$ is an $f'_a(\Omega)$-saturated set.*

Proof. We first make sure that $f_a(\Gamma)$ is a subset of $f'_a(\Omega)$. By definition of f_a, $f_a(\Gamma) = g_a(\Gamma) \cup K_ag_a(\Gamma) \cup \{\bot \in \mathbf{Fml} \mid \Gamma \vdash \bot\}$. Since Γ is an Ω-saturated set, $\Gamma \nvdash \bot$ so that $f_a(\Gamma) = g_a(\Gamma) \cup K_ag_a(\Gamma)$. On the other hand, $f'_a(\Omega) = g_a(\Omega) \cup K_ag_a(\Omega)$. Since $g_a(\Gamma) \subseteq g_a(\Omega)$ by Proposition 2.6.2, $f_a(\Gamma) \subseteq f'_a(\Omega)$ holds.

We check each condition of Definition 2.7.2 to make sure that $f_a(\Gamma)$ is actually an $f'_a(\Omega)$-saturated set.

1. Assume $f_a(\Gamma) \vdash \varphi$ and $\varphi \in f'_a(\Omega)$. $\varphi \in g_a(\Omega) \cup K_ag_a(\Omega)$ holds.

   (Case $\varphi \in g_a(\Omega)$) Note that φ does not begin with K_a. By definition of g_a, $(K_a)^+\varphi \in \Omega$. Since Ω is subformula-closed, $K_a\varphi \in \Omega$ holds. By $\Gamma \vdash K_a\varphi$, since Γ is Ω-saturated, $K_a\varphi \in \Gamma$. Thus, $\varphi \in f_a(\Gamma)$.

   (Case $\varphi \in K_ag_a(\Omega)$) $\varphi = K_a\varphi'$ and $\varphi' \in g_a(\Omega)$ hold. Note that φ' does not begin with K_a. By definition of g_a, $(K_a)^+\varphi' \in \Omega$. This implies $K_a\varphi' \in \Omega$. Since $\Gamma \vdash K_aK_a\varphi'$, $\Gamma \vdash K_a\varphi'$ holds. Thus, since Γ is Ω-saturated, $K_a\varphi' \in \Gamma$ holds. This means $\varphi = K_a\varphi' \in f_a(\Gamma)$.

2. Assume $f_a(\Gamma) \vdash \varphi \vee \psi$ and $\varphi, \psi \in f'_a(\Omega)$. By rule (nec), $K_af_a(\Gamma) \vdash K_a(\varphi \vee \psi)$ holds. By Proposition 2.6.6, the formulas in $K_af_a(\Gamma)$ are deducible from Γ. Thus, $\Gamma \vdash K_a(\varphi \vee \psi)$ holds. By rule $(\vee K)$ and the fact that Γ is saturated, either $K_as_a(\varphi) \in \Gamma$ or $K_as_a(\psi) \in \Gamma$ holds. We can assume $K_as_a(\varphi) \in \Gamma$ without loss of generality. This implies $f_a(\Gamma) \vdash \varphi$ and then $\varphi \in f_a(\Gamma)$.

3. Seeking contradiction, assume $f_a(\Gamma) \vdash \bot$. Since $\Gamma \vdash K_a\bot$, the deducibility $\Gamma \vdash \bot$ holds, which contradicts the fact that Γ is an Ω-saturated set.

□

Lemma 2.7.6 (Saturation lemma)**.** *For sets of formulas Γ and Ω with $\Gamma \nvdash \varphi$, $\Gamma \subseteq \Omega$ and $\varphi \in \Omega$, there exists an Ω-saturated set Γ^ω with $\Gamma^\omega \nvdash \varphi$ and $\Gamma \subseteq \Gamma^\omega$.*

Proof. Since both $PVar$ and A are countable, we can enumerate all formulas of Ω in a sequence $(\varphi_i)_{i\in\mathbb{N}^+}$. We define Γ^i inductively:

(Case $i = 0$) $\Gamma^0 = \Gamma$,

$$\textbf{(Case } i > 0\textbf{)} \quad \Gamma^i = \begin{cases} \{\varphi_i\} \cup \Gamma^{i-1} & (\text{if } \{\varphi_i\} \cup \Gamma^{i-1} \nvdash \varphi), \\ \Gamma^i = \Gamma^{i-1} \cup \{\varphi_i \supset \varphi\} & (\text{otherwise if } \varphi_i \supset \varphi \in \Omega), \\ \Gamma^i = \Gamma^{i-1} & (\text{otherwise}). \end{cases}$$

Using these Γ^i, we define $\Gamma^\omega = \bigcup_{i\in\omega} \Gamma^i$.

Claim: $\Gamma^\omega \nvdash \varphi$. Seeking contradiction, assume a deducibility $\Gamma^\omega \vdash \varphi$. Since only finite number of formulas in Γ are used to prove φ, there exists a minimal i with $\Gamma^i \vdash \varphi$. Since $\Gamma \nvdash \varphi$, i is not 0. Since $\Gamma^i \neq \Gamma^{i-1}$, either $\Gamma^i = \{\varphi_i\} \cup \Gamma^{i-1}$ or $\Gamma^i = \{\varphi_i \supset \varphi\} \cup \Gamma^{i-1}$ holds. The first case is explicitly forbidden. In the second case, $\Gamma^{i-1}, \varphi_i \supset \varphi \vdash \varphi$ holds. That means $\Gamma^{i-1} \vdash (\varphi_i \supset \varphi) \supset \varphi$. Also, since we could not take the first case, $\Gamma^{i-1}, \varphi_i \vdash \varphi$ holds. That means $\Gamma^{i-1} \vdash \varphi_i \supset \varphi$. By these combined, $\Gamma^{i-1} \vdash \varphi$ holds, which contradicts to the minimality of i. The claim is now proved. □

Claim: Γ^ω is an Ω-saturated set.

Proof of Claim. We check each condition listed in Definition 2.7.2:

1. Assume $\Gamma^\omega \vdash \psi \in \Omega$. There is $i \in \mathbb{N}^+$ with $\varphi_i = \psi$. We know that $\Gamma^{i-1} \cup \{\varphi_i\} \nvdash \varphi$. It means $\psi \in \Gamma^\omega$.

2. Assume $\psi_0 \vee \psi_1 \in \Gamma^\omega$ and $\psi_0, \psi_1 \in \Omega$. Seeking contradiction, assume $\psi_0 \notin \Gamma^\omega$ and $\psi_1 \notin \Gamma^\omega$. By construction, both $\Gamma^\omega \vdash \psi_0 \supset \varphi$ and $\Gamma^\omega \vdash \psi_1 \supset \varphi$ hold. Since Γ^ω is deductively closed, by ($\vee$-E) rule, we have $\Gamma^\omega \vdash \varphi$, which contradicts to the previous fact.

3. Since $\Gamma^\omega \nvdash \varphi$, by rule ($\bot$-E), $\Gamma^\omega \nvdash \bot$.

Since $\Gamma^0 = \Gamma$, Γ^ω contains Γ. The lemma is now proved. □

Definition 2.7.7 (Canonical model candidate)**.** *For a sset of formulas Ω, we define $M^{\mathrm{C}}(\Omega)$ as a tuple $\langle W^{\mathrm{C}}, \preceq^{\mathrm{C}}, (f_a^{\mathrm{C}})_{a\in A}, \rho^{\mathrm{C}}\rangle$ where:*

- *W^{C} is the set of pairs of the form (Ω', Γ) where Γ is an Ω'-saturated set and Ω' is a hereditary f'-subformula-closed subset of Ω.*
- *$(\Omega', \Gamma) \preceq^{\mathrm{C}} (\Omega'', \Delta)$ if and only if $\Omega' \subseteq \Omega''$ and $\Gamma \subseteq \Delta$,*
- *$f_a^{\mathrm{C}}((\Omega', \Gamma)) = (f'_a(\Omega), f_a(\Gamma))$*
- *$\rho^{\mathrm{C}}(P) = \{(\Omega', \Gamma) \in W^{\mathrm{C}} \mid P \in \Gamma\}$.*

Lemma 2.7.8 (Canonical model)**.** *The tuple M^{C} is a model.*

Proof. First of all, f_a^{C} is actually a function $W^{\mathrm{C}} \to W^{\mathrm{C}}$ by Lemma 2.7.5. We check each condition in Definition 2.4.1 to make sure the tuple is actually a model:

1. $\preceq^{\mathrm{C}}$ is a partial order because set theoretic inclusion $\subseteq$ is a partial order.
2. (a) $f_a^{\mathrm{C}}((\Omega', \Gamma)) = (f'_a(\Omega'), f_a(\Gamma))$. Since Ω' is hereditary f'-subset-closed, $f'_a(\Omega') \subseteq \Omega'$ holds. Now, showing $\Gamma \subseteq f_a(\Gamma)$ is enough. Take an arbitrary $\varphi \in f_a(\Gamma)$. Since $\Gamma \nvdash \bot$, either $\varphi \in g_a(\Gamma)$ or $\varphi \in K_a g_a(\Gamma)$ holds. In either case, $(K_a)^*\varphi \in \Gamma$ holds. That means $\Gamma \vdash \varphi$. Since $\varphi \in \Omega'$, $\varphi \in \Gamma$ holds. Thus we have shown $\Gamma \subseteq f_a(\Gamma)$. This completes the proof of $f_a^{\mathrm{C}}((\Omega', \Gamma)) \preceq^{\mathrm{C}} (\Omega', \Gamma)$.
   (b) By Lemma 2.6.8, $f_a(f_a(\Gamma)) = f_a(\Gamma)$ holds. Similar argument gives $f'_a(f'_a(\Omega')) = f'_a(\Omega')$. These combined imply that f_a^{C} is idempotent.
   (c) Both f_a and f'_a are monotonic with respect to set theoretic inclusion. This implies that f_a^{C} is monotonic with respect to $\preceq^{\mathrm{C}}$.
3. Immediate.

□

Lemma 2.7.9. *For a state $(\Omega', \Gamma) \in W^{\mathrm{C}}$ in the canonical model M^{C} and $\varphi \in \Omega'$, φ is an element of Γ if and only if M^{C},$(\Omega', \Gamma) \models \varphi$ holds.*

Proof. By induction on φ.

(Case $\varphi = \bot$) Neither side ever holds because Γ is Ω'-saturated.

(Case $\varphi = P$) By definition of ρ^{C} and $\models$, the equivalency $\varphi \in \Gamma \Leftrightarrow (\Omega', \Gamma) \in \rho(P) \Leftrightarrow M^{\mathrm{C}}, (\Omega, \Gamma) \models P$ holds.

(Case $\varphi = \psi_0 \wedge \psi_1$)(Case $\varphi = \psi_0 \vee \psi_1$) Directly from the induction hypothesis.

(Case $\varphi = K_a\psi$) ($\Rightarrow$) Assume $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma) \models K_a\psi$. By definition of $\models$ and induction hypothesis, $\psi \in f_a(\Gamma) = g_a(\Gamma) \cup K_a g_a(\Gamma)$. If $\psi \in g_a(\Gamma)$, $(K_a)^+\psi \in \Gamma$ holds. This means $\Gamma \vdash K_a\psi$. Otherwise, if $\psi \in K_a g_a(\Gamma)$, $\psi = K_a\psi'$ where $\psi' \in g_a(\Gamma)$. This means $\Gamma \vdash K_a\psi'$ and consequently $\Gamma \vdash K_a\psi$. In either case $\Gamma \vdash K_a\psi$ holds. Also by the assumption of the lemma, $K_a\psi \in \Omega'$. These imply $K_a\psi \in \Gamma$ because Γ is an Ω'-saturated set.

($\Leftarrow$) Assume $K_a \in \Gamma$. There exists ψ' that does not begin with K_a such that $\psi = (K_a)^*\psi'$. By definition of f_a, $\psi' \in f_a(\Gamma)$. By induction hypothesis, $(f'_a(\Omega'), f_a(\Gamma)) \models \psi'$. This is equivalent to $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma) \models K_a\psi'$. Since f_a^{c} is idempotent, $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma) \models K_a\psi$.

(Case $\varphi = \psi_0 \supset \psi_1$) ($\Rightarrow$) Assume $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma) \models \psi_0 \supset \psi_1$. Seeking contradiction, assume $\psi_0 \supset \psi_1 \notin \Gamma$. Since Γ is deductively closed, $\Gamma \cup \{\psi_0\} \nvdash \psi_1$. By Lemma 2.7.6, there exists an Ω'-saturated set Γ' with $\Gamma' \supseteq \Gamma \cup \{\psi_0\}$ and $\Gamma' \nvdash \psi_1$. By induction hypothesis, $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma') \models \psi_0$ but not $M^{\mathrm{c}}(\Omega), (\Omega', \Gamma') \models \psi_1$. Since $(\Omega', \Gamma') \succeq (\Omega', \Gamma)$, this contradicts to $M^{\mathrm{c}}(\Omega), \Gamma \models \psi_0 \supset \psi_1$.

($\Leftarrow$) For an Ω'-saturated set Γ, assume $\psi_0 \supset \psi_1 \in \Gamma$. Take a state (Ω'', Δ) with $(\Omega', \Gamma) \preceq^{\mathrm{c}} (\Omega'', \Delta)$ and $M^{\mathrm{c}}(\Omega), (\Omega'', \Delta) \models \psi_0$. Showing $M^{\mathrm{c}}(\Omega), (\Omega'', \Delta) \models \psi_1$ is enough. By induction hypothesis, $\psi_0 \in \Delta$. Since $\psi_0 \supset \psi_1 \in \Gamma \subseteq \Delta$ and Δ is an Ω''-saturated set, $\psi_1 \in \Delta$. By induction hypothesis, $M^{\mathrm{c}}(\Omega), (\Omega'', \Delta) \models \psi_1$ holds.

Now we have shown the lemma. □

2.7.1 Strong Completeness

Theorem 2.7.10 (Strong completeness)**.** $\Gamma \models \varphi$ *implies* $\Gamma \vdash \varphi$.

Proof. We show the contraposition: assuming $\Gamma \nvdash \varphi$, we show $\Gamma \not\models \varphi$. By Lemma 2.7.6, there is a saturated set of formula Γ' with $\Gamma' \nvdash \varphi$ and $\Gamma' \supseteq \Gamma$. By Lemma 2.7.9, $M^{\mathrm{c}}(\mathbf{Fml}), (\mathbf{Fml}, \Gamma') \models \Gamma$ but not $M^{\mathrm{c}}(\mathbf{Fml}), (\mathbf{Fml}, \Gamma') \models \varphi$. This denies $\Gamma \models \varphi$. □

Corollary 2.7.11 (Compactness)**.** *If any finite subset* Γ_0 *of* Γ *is consistent,* Γ *is consistent.*

Proof. For any finite subset Γ_0, $\Gamma_0 \vdash \bot$ does not hold. Thus, $\Gamma \vdash \bot$ does not hold. By strong completeness (Theorem 2.7.10), Γ is consistent. □

2.7.2 Finite Model Property

Definition 2.7.12. *We define the length of a formula φ inductively on φ:*

$$\begin{aligned} \mathrm{len}(\bot) = \mathrm{len}(P) &= 1, \\ \mathrm{len}(K_a\varphi) &= \mathrm{len}(\varphi) + 1, \\ \mathrm{len}(\varphi \wedge \psi) = \mathrm{len}(\varphi \vee \psi) = \mathrm{len}(\varphi \supset \psi) &= \mathrm{len}(\varphi) + \mathrm{len}(\psi) + 1. \end{aligned}$$

Notation 2.7.13. *We denote a set of formulas which only contain the propositional variables in $V \subseteq PVar$ as $\mathbf{Fml}_V$.*

Lemma 2.7.14. *For a set of propositional variables $V \subseteq \mathbf{Fml}$, the length-limited set of formulas $\Gamma_n = \{\varphi \in \mathbf{Fml}_V \mid \mathrm{len}(\varphi) \leq n\}$ is hereditary f'-subformula-closed.*

Proof. By induction on n, we show a stronger proposition: both Γ_n and $\Gamma_n \cup K_a\Gamma_n$ are hereditary f'-subformula-closed for any $a \in A$.

(Case $n = 0$) Since $\Gamma_0 = \emptyset$, $\Gamma_0 \cup K_a\Gamma_0 = \emptyset$. Both are hereditary f'-subformula-closed.

(Case $n = n_0 + 1$) By definition of Γ_n and the definition of subformula, Γ_n is subformula-closed set. For any $a \in A$, since $g_a(\Gamma_n) = \Gamma_{n_0}$, $f'_a(\Gamma) = \Gamma_{n_0} \cup K_a\Gamma_{n_0} \subseteq \Gamma_n$ holds. Thus, by induction hypothesis, $f'_a(\Gamma)$ is a hereditary f'-subformula-closed set. These facts imply Γ_n is a hereditary f'-subformula-closed set.

We also show $\Gamma_n \cup K_b\Gamma_n$ is a hereditary f'-subformula-closed set. Since $\Gamma_n \cup K_b\Gamma_n$ is subformula-closed, we only have to check that $f'_c(\Gamma_n \cup K_b\Gamma_n)$ is f'-subformula-closed.

(Case $c \neq b$) $f'_c(\Gamma_n \cup K_b\Gamma_n) = f'_c(\Gamma_n)$, which is shown to be a hereditary f'-subformula-closed set.

(Case $c = b$) $f'_c(\Gamma_n \cup K_b\Gamma_n) = f'_c(f'_c(\Gamma_n)) = f'_c(\Gamma_n)$, which is shown to be a hereditary f'-subformula-closed set.

□

Theorem 2.7.15 (Finite model property)**.** *If φ is not a theorem of **IEC**, there is a finite model M with $M \not\models \varphi$.*

Proof. Since a formula φ is finitary, it contains only a finite number of propositional variables. Let V be the set of propositional variables occurring in φ. The

set $\Omega = \{\psi \in \mathbf{Fml}_V \mid \mathrm{len}(\psi) \leq \mathrm{len}(\varphi)\}$ is finite and hereditary f'-subformula-closed by Lemma 2.7.14. By Lemma 2.7.6, there exist an Ω-saturated set Γ with $\varphi \notin \Gamma$. By Lemma 2.7.9, $M^{\mathrm{c}}(\Omega), (\Omega, \Gamma) \not\models \varphi$. Since Ω is finite, the model $M^{\mathrm{c}}(\Omega)$ is finite. In fact, the number of the states of $M^{\mathrm{c}}(\Omega)$ is at most $4^{|\Omega|}$. □

Theorem 2.7.16. *It is decidable whether a formula φ is a theorem of **IEC** or not.*

Proof. Since **IEC** is finitely axiomatisable and has finite model property, by Harrop's Theorem [17], the set of theorems of **IEC** is recursively decidable. □

2.8 Adding Double Negation Elimination

A simple way to obtain a classical modal logic from **IEC** adding a deduction rule called double negation elimination (in short DN).

$$(\mathrm{DN})\ \frac{\Gamma \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \neg\neg\varphi}{\Gamma \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \varphi}\ .$$

However, adding this rule makes the modalities meaningless because both $\varphi \supset K_a\varphi$ and $K_a\varphi \supset \varphi$ would become theorems as shown in Figure 2.2. We speculate that even with double negation elimination, missing substructural rules such as weakeining regains the meaning of the modality K_a.

Theorem 2.8.1. ***IEC*** $+ (\mathrm{DN}) \vdash K_a\varphi \supset \varphi$.

Proof. See Figure 2.2. □

2.9 Conservativity over the Fragment without Disjunction

We give a validity preserving translation from the classical modal logic multiple S4 modalities to **IEC**. The translation is into the disjunction-less fragment of **IEC**. We use conservativity to show the validity preservation of the translation. Since the disjunction-less fragment of **IEC** does not have $(\vee K)$ rule, using conservativity for this fragment simplifies the task.

We consider a fragment $\mathbf{IEC_f}$ where $\vee$ is missing. The aim of this section is to prove the conservativity.

We prove conservativity through completeness of $\mathbf{IEC_f}$ and soundness of **IEC** for the same semantics.

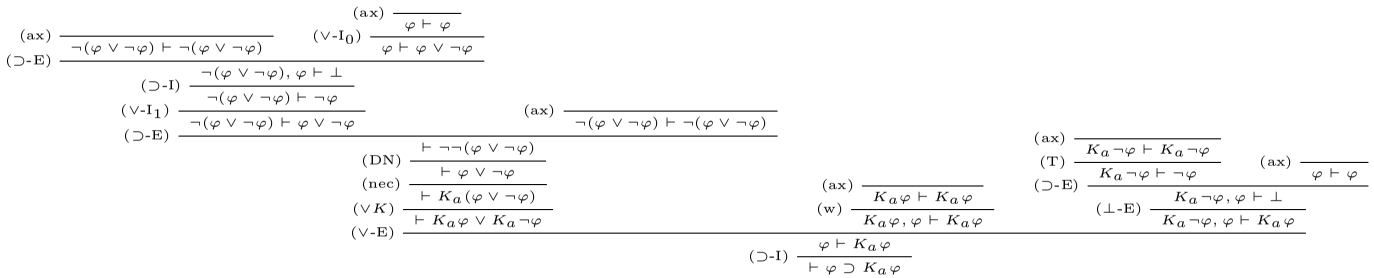

Figure 2.2: Adding a classical principle called double negation elimination destroys the meaning of modalities. Note that weakening is used in the proof.

Theorem 2.9.1 (Completeness of $\vee$-less fragment)**.** *For a $\vee$-less formula φ and a set of $\vee$-less formulas Γ, the relation $\Gamma \models \varphi$ implies the deducibility $\Gamma \vdash_{\mathbf{f}} \varphi$.*

Proof deferred.

Theorem 2.9.2 (Conservativity)**.** *For a $\vee$-less formula φ and a set of $\vee$-less formulas Γ, $\Gamma \vdash \varphi \Rightarrow \Gamma \vdash_{\mathbf{f}} \varphi$.*

Proof of Theorem 2.9.2. By soundness for **IEC** (Theorem **??**), $\Gamma \vdash \varphi$ implies $\Gamma \models \varphi$. By strong completeness for $\mathbf{IEC_f}$ (Theorem 2.9.1), $\Gamma \models \varphi$ implies $\Gamma \vdash_{\mathbf{f}} \varphi$. The theorem is proved by combining these two implication. □

Definition 2.9.3. *A set of formulas Γ is $\vee$less-saturated if and only if*

1. *Γ is deductively closed, i.e., $\Gamma \vdash_{\mathbf{f}} \varphi \Rightarrow \varphi \in \Gamma$, and*
2. *$\Gamma \nvdash_{\mathbf{f}} \bot$.*

Lemma 2.9.4 ($\vee$less-saturation lemma)**.** *For a set of formulas Γ with $\Gamma \nvdash_{\mathbf{f}} \varphi$, there exists a $\vee$less-saturated set Γ^ω of formulas with $\Gamma^\omega \nvdash_{\mathbf{f}} \varphi$ and $\Gamma \subseteq \Gamma^\omega$.*

Proof. We can enumerate all formulas in a sequence $(\varphi_i)_{i \in \mathbb{N}^+}$. We define Γ^i inductively:

(Case $i = 0$) $\Gamma^0 = \Gamma$,

(Case $i > 0$) $$\Gamma^i = \begin{cases} \{\varphi_i\} \cup \Gamma^{i-1} & \text{if } \{\varphi_i\} \cup \Gamma^{i-1} \nvdash_{\mathbf{f}} \varphi \\ \Gamma^{i-1} \cup \{\varphi_i \supset \varphi\} & \text{otherwise.} \end{cases}$$

Claim: $\Gamma^\omega \nvdash_{\mathbf{f}} \varphi$.

Proof of Claim. Seeking contradiction, assume $\Gamma^\omega \vdash_{\mathbf{f}} \varphi$. Since only finite number of formulas in Γ are used to prove φ, there exists a minimal i with $\Gamma^i \vdash_{\mathbf{f}} \varphi$. Since $\Gamma \nvdash_{\mathbf{f}} \varphi$, $i \neq 0$. Either $\Gamma^i = \{\varphi_i\} \cup \Gamma^{i-1}$ or $\Gamma^i = \{\varphi_i \supset \varphi\} \cup \Gamma^{i-1}$. The first case is explicitly forbidden. In the second case, $\Gamma^{i-1} \cup \{\varphi_i \supset \varphi\} \vdash_{\mathbf{f}} \varphi$ holds. That means $\Gamma^{i-1} \vdash_{\mathbf{f}} (\varphi_i \supset \varphi) \supset \varphi$. Also, since we could not take the first case, $\Gamma^{i-1} \cup \{\varphi_i\} \vdash_{\mathbf{f}} \varphi$ holds. That means $\Gamma^{i-1} \vdash_{\mathbf{f}} \varphi_i \supset \varphi$. These combined, $\Gamma^{i-1} \vdash_{\mathbf{f}} \varphi$ holds, which contradicts to the minimality of i. □

Claim: $\Gamma^\omega = \bigcup_{i \in \omega} \Gamma^i$ is a saturated set.

Proof of the claim. 1. Assume $\Gamma^\omega \vdash \psi$. There is $i \in \mathbb{N}^+$ with $\varphi_i = \psi$. By the previous claim, we know that $\Gamma^{i-1} \cup \{\varphi_i\} \nvdash \varphi$. It means $\psi \in \Gamma^\omega$.

2. Since $\Gamma^\omega \nvdash \varphi$, $\Gamma^\omega \nvdash \bot$.

The lemma is now proved. □

□

Definition 2.9.5 (Canonical model candidate for disjunction-less fragment)**.** $M^n = \langle W^n, \preceq^n, (f_a^n)_{a\in A}, \rho^n\rangle$ *where:*

- W^n *is the set of* $\vee$*-less saturated sets of formulas,*
- $\Gamma \preceq^n \Delta$ *if and only if* $\Gamma \subseteq \Delta$*,*
- $f_a^n(\Gamma) = \{\varphi \mid K_a\varphi \in \Gamma\}$*,*
- $\rho^n(P) = \{\Gamma \mid P \in \Gamma\}$*.*

Lemma 2.9.6 (Canonical model for $\vee$-less fragment)**.** *The tuple* $M^n = \langle W^c, \preceq^c, (f_a^c)_{a\in A}, \rho^c\rangle$ *is a model.*

Proof. First, let us check f_a^{n} is actually a function $W^{\mathrm{n}} \to W^{\mathrm{n}}$. Assume $\Gamma \in W^{\mathrm{n}}$. Claim: $f_a(\Gamma)$ is a $\vee$less-saturated set of formulas. To prove the claim, we check each condition on the definition of saturated sets.

1. Assume $f_a^{\mathrm{n}}(\Gamma) \vdash \varphi$. Since there is (nec) rule, $K_a(f_a(\Gamma)) \vdash_{\mathbf{f}} K_a\varphi$. Since $K_a(f_a^{\mathrm{n}}(\Gamma)) \subseteq \Gamma$, the relation $\Gamma \vdash_{\mathbf{f}} K_a\varphi$ holds. Since Γ is deductively closed, $K_a\varphi \in \Gamma$. By definition of f_a^{n}, $\varphi \in f_a^{\mathrm{n}}(\Gamma)$.
2. Seeking contradiction, assume $f_a^{\mathrm{n}}(\Gamma) \vdash_{\mathbf{f}} \bot$. Since $f_a^{\mathrm{n}}(\Gamma)$ is deductively closed, $\bot \in f_a^{\mathrm{n}}(\Gamma)$. By definition of f_a^{n}, $K_a\bot \in \Gamma$. Because of the rule (T), $\Gamma \vdash_{\mathbf{f}} \bot$. This contradicts to the assumption of Γ being a $\vee$less-saturated set.

Now, let us check each condition in Definition 2.4.1 in order to see that the tuple is actually a model.

1. $\preceq^{\mathrm{n}}$ is a partial order because set theoretic inclusion $\subseteq$ is a partial order.
2. (a) $f_a^{\mathrm{n}}(\Gamma) \preceq \Gamma$ of the rule (T).
   (b) $f_a^{\mathrm{n}}(f_a^{\mathrm{n}}(\Gamma)) \subseteq f_a^{\mathrm{n}}(\Gamma)$ is now obvious from the previous line. Let us show the opposite. Assume $\varphi \in f_a^{\mathrm{n}}(\Gamma)$. By definition of f_a^{n}, $K_a\varphi \in \Gamma$. By the rule (introspection), $\Gamma \vdash_{\mathbf{f}} K_aK_a\varphi$. Since Γ is deductively closed, $K_aK_a\varphi \in \Gamma$. Thus $\varphi \in f_a^{\mathrm{n}}(f_a^{\mathrm{n}}(\Gamma))$.
   (c) Assume $\Gamma \preceq \Delta$. Every $K_a\varphi \in \Delta$ is also in Γ. Thus $f_a^{\mathrm{n}}(\Gamma) \preceq f_a^{\mathrm{n}}(\Delta)$.

3. Assume $\Gamma' \succeq \Gamma \in \rho^{\mathrm{n}}(P)$. $P \in \Gamma$. So $P \in \Gamma'$. Thus $\Gamma' \in \rho^{\mathrm{n}}(P)$.

□

Lemma 2.9.7. *For a $\vee$less-saturated set of formula Γ and the canonical model M^n, an equivalency $\varphi \in \Gamma \Leftrightarrow M^n, \Gamma \models \varphi$ holds.*

Proof. By induction on φ.

(Case $\varphi = \bot$) Neither side ever holds.

(Case $\varphi = P$) By definition of ρ^{n}, $\varphi \in \Gamma \Longleftrightarrow \Gamma \in \rho(P) \Longleftrightarrow M^{\mathrm{n}}, \Gamma \models P$.

(Case $\varphi = \psi_0 \wedge \psi_1$) **(Case $\varphi = \psi_0 \vee \psi_1$)** Directly from the induction hypothesis.

(Case $\varphi = K_a\psi$) ($\Rightarrow$) Assume $M^{\mathrm{n}}, \Gamma \models K_a\psi$. By definition of $\models$, $M^{\mathrm{n}}, f_a^{\mathrm{n}}(\Gamma) \models \psi$. By induction hypothesis, $\psi \in f_a^{\mathrm{n}}(\Gamma)$. By definition of f_a^{n}, $K_a\psi \in \Gamma$.
($\Leftarrow$) Assume $K_a\psi \in \Gamma$. By definition of f_a^{n}, $\psi \in f_a^{\mathrm{n}}(\Gamma)$. By induction hypothesis, $f_a^{\mathrm{n}}(\Gamma) \models \psi$. By definition of $\models$, $\Gamma \models K_a\psi$.

(Case $\varphi = \psi_0 \supset \psi_1$) ($\Rightarrow$) Assume $M^{\mathrm{n}}, \Gamma \models \psi_0 \supset \psi_1$. Seeking contradiction, assume $\psi_0 \supset \psi_1 \notin \Gamma$. Since Γ is deductively closed, $\Gamma, \psi_0 \nvdash_{\mathbf{f}} \psi_1$. By Lemma 2.9.4, there exists a $\vee$-less saturated set Γ' with $\Gamma' \supseteq \Gamma \cup \{\psi_0\}$ and $\Gamma' \nvdash_{\mathbf{f}} \psi_1$. By induction hypothesis, $M^{\mathrm{n}}, \Gamma' \models \psi_0$ but not $M^{\mathrm{n}}, \Gamma' \models \psi_1$. Since $\Gamma' \succeq \Gamma$, this contradicts to $M^{\mathrm{n}}, \Gamma \models \psi_0 \supset \psi_1$.
($\Leftarrow$) Assume $\psi_0 \supset \psi_1 \in \Delta$, $\Delta' \succeq \Delta$ and $M^{\mathrm{n}}, \Delta' \models \psi_0$. Showing $M^{\mathrm{n}}, \Delta' \models \psi_1$ is enough. By induction hypothesis, $\psi_0 \in \Delta'$. Since Δ' is deductively closed and $\psi_0 \supset \psi_1 \in \Delta'$, $\psi_1 \in \Delta'$. By induction hypothesis, $M^{\mathrm{n}}, \Delta' \models \psi_1$.

Now we have shown the lemma.

□

We can prove strong completeness for $\mathbf{IEC_f}$ (Theorem 2.9.1) at last.

Proof of Theorem 2.9.1. We show the contraposition: assuming $\Gamma \nvdash_{\mathbf{f}} \varphi$, we show $\Gamma \not\models \varphi$. By Lemma 2.9.4, there is a $\vee$less-saturated set of formula Γ' with $\Gamma' \nvdash_{\mathbf{f}} \varphi$ and $\Gamma' \supseteq \Gamma$. By Lemma 2.9.7, $M^{\mathrm{n}}, \Gamma' \models \Gamma$ but not $M^{\mathrm{n}}, \Gamma' \models \varphi$. This denies $\Gamma \models \varphi$. □

2.10 Formula Translation from Classical S4

Although simply adding the double negation eliminiation makes **IEC** degenerate into classical propositional logic, there is a connection between classical modal logic **S4** and **IEC**. In this section, we show a connection between classical multi modal **S4** logc and **IEC**by extending Gödel translation of classical propositional logic into intuitionistic propositional logic.

$\mathbf{S4} * \cdots * \mathbf{S4}$ has the same formulas as **IEC**. $\mathbf{S4} * \cdots * \mathbf{S4}$ has all rules of **IEC** except $(\vee K)$ and a new rule (DN):

$$\text{(DN)}\ \frac{\Gamma \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \neg\neg\varphi}{\Gamma \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \varphi}\ .$$

We use Gödel translation to translate classical epistemic formula into $\mathbf{IEC_f}$ formula.

Definition 2.10.1. *We define the extended Gödel translation* $\langle\cdot\rangle : \mathbf{Fml} \to \mathbf{Fml}$ *inductively on the definition of* **Fml***:*

$$\begin{aligned}
\langle\bot\rangle &= \bot, \\
\langle P\rangle &= \neg\neg P, \\
\langle K_a\varphi\rangle &= \neg\neg K_a \langle\varphi\rangle, \\
\langle\varphi \wedge \psi\rangle &= \langle\varphi\rangle \wedge \langle\psi\rangle, \\
\langle\varphi \vee \psi\rangle &= \neg(\neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle), \\
\langle\varphi \supset \psi\rangle &= \langle\varphi\rangle \supset \langle\psi\rangle.
\end{aligned}$$

Lemma 2.10.2. $\vdash_{\boldsymbol{S4}*\cdots*\boldsymbol{S4}} \varphi \leftrightarrow \langle\varphi\rangle$.

Proof. Induction on φ. This is easily shown using (DN) rules. □

Lemma 2.10.3. $\vdash_{\mathbf{f}} (\neg\neg\langle\varphi\rangle) \supset \langle\varphi\rangle$.

Proof. Induction on φ.

(Case $\varphi = \bot$) $\langle\varphi\rangle = \bot$.

$$\dfrac{\dfrac{\dfrac{}{\neg\neg\bot \vdash_{\mathbf{f}} \neg\neg\bot}\,\text{(ax)} \qquad \dfrac{\dfrac{}{\bot \vdash \bot}\,\text{(ax)}}{\vdash \neg\bot}\,(\supset\text{-I})}{\neg\neg\bot \vdash \bot}\,(\supset\text{-E})}{\vdash_{\mathbf{f}} (\neg\neg\bot) \supset \bot}\,(\supset\text{-I})$$

(Case $\varphi = P$) $\langle\varphi\rangle = \neg\neg P$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg\neg\neg P \vdash_{\mathbf{f}} \neg\neg\neg\neg P}\,(\text{ax})}{\dfrac{\dfrac{}{\neg P \vdash_{\mathbf{f}} \neg P}\,(\text{ax}) \quad \dfrac{}{\neg\neg P \vdash_{\mathbf{f}} \neg\neg P}\,(\text{ax})}{\neg P, \neg\neg P \vdash_{\mathbf{f}} \bot}\,(\supset\text{-I})}{\neg P \vdash_{\mathbf{f}} \neg\neg\neg P}\,(\supset\text{-E})}{\neg\neg\neg\neg P, \neg P \vdash_{\mathbf{f}} \bot}\,(\supset\text{-I})}{\neg\neg\neg\neg P \vdash_{\mathbf{f}} \neg\neg P}\,(\supset\text{-I})}{\vdash_{\mathbf{f}} \neg\neg\neg\neg P \supset \neg\neg P}\,(\supset\text{-I})$$

(Case $\varphi = \psi_0 \wedge \psi_1$) Figure 2.3 Part A.

(Case $\varphi = \psi_0 \vee \psi_1$) $\langle\varphi\rangle = \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)$. Figure 2.3 Part B.

(Case $\varphi = \psi_0 \supset \psi_1$) Figure 2.3 Part C.

(Case $\varphi = K_x\psi$) $\langle\varphi\rangle = \neg\neg K_x\langle\psi\rangle$. Similar to $\vee$ case.

□

Theorem 2.10.4 (Translation)**.** $\Gamma \vdash_{\boldsymbol{S4}*\cdots*\boldsymbol{S4}} \varphi \Leftrightarrow \langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$.

Proof. ($\Leftarrow$) Since $\vdash_{\mathbf{S4}*\cdots*\mathbf{S4}}$ has all deduction rules of $\vdash_{\mathbf{f}}$, $\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$ implies $\langle\Gamma\rangle \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \langle\varphi\rangle$. By Lemma 2.10.2, this implies $\Gamma \vdash_{\mathbf{S4}*\cdots*\mathbf{S4}} \varphi$.
($\Rightarrow$) Induction on the definition of $\vdash_{\mathbf{S4}*\cdots*\mathbf{S4}}$.

(DN) Assume $\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\neg\neg\varphi\rangle$. By Lemma 2.10.3, $\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$ holds.

($\vee$-I$_0$) Assuming $\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$, showing $\langle\Gamma\rangle \vdash_{\mathbf{f}} \neg(\neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle)$ is enough.

$$\dfrac{\dfrac{\dfrac{\text{I.H.}}{\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle} \quad \dfrac{\dfrac{}{\neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle \vdash_{\mathbf{f}} \neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle}\,(\text{ax})}{\neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle \vdash_{\mathbf{f}} \neg\langle\varphi\rangle}\,(\wedge\text{-E}_0)}{\langle\Gamma\rangle, \neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle \vdash_{\mathbf{f}} \bot}\,(\supset\text{-E})}{\langle\Gamma\rangle \vdash_{\mathbf{f}} \neg(\neg\langle\varphi\rangle \wedge \neg\langle\psi\rangle)}\,(\supset\text{-I})$$

($\vee$-I$_1$) Similar to ($\vee$-I$_0$).

($\vee$-E) Assume $\langle\Gamma\rangle \vdash_{\mathbf{f}} \langle\psi_0 \vee \psi_1\rangle$, $\langle\Gamma\rangle, \langle\psi_0\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$ and $\langle\Gamma\rangle, \langle\psi_1\rangle \vdash_{\mathbf{f}} \langle\varphi\rangle$. The first assumption is equivalent to $\langle\Gamma\rangle \vdash_{\mathbf{f}} \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)$. See Figure 2.10.

($\wedge$-I)($\wedge$-E$_0$)($\wedge$-E$_1$)($\supset$-I)($\supset$-E)($\bot$-E)(T)(introspection)(nec) Trivial.

□

Part A

$$
(\wedge\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
\dfrac{\text{I.H.}}{\vdash_{\mathbf{f}} \neg\neg\langle\psi_0\rangle \supset \langle\psi_0\rangle}
\qquad
(\supset\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
(\supset\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
(\text{ax})\,\dfrac{}{\neg\langle\psi_0\rangle \vdash_{\mathbf{f}} \neg\langle\psi_0\rangle}
\quad
(\wedge\text{-E}_0)\,\dfrac{(\text{ax})\,\dfrac{}{\langle\psi_0\rangle \wedge \langle\psi_1\rangle \vdash_{\mathbf{f}} \langle\psi_0\rangle \wedge \langle\psi_1\rangle}}{\langle\psi_0\rangle \wedge \langle\psi_1\rangle \vdash_{\mathbf{f}} \langle\psi_0\rangle}
}{\neg\langle\psi_0\rangle , \langle\psi_0\rangle \wedge \langle\psi_1\rangle \vdash_{\mathbf{f}} \bot}
}{\neg\langle\psi_0\rangle \vdash_{\mathbf{f}} \neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle)}
\quad
(\text{ax})\,\dfrac{}{\neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \vdash_{\mathbf{f}} \neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle)}
}{\neg\langle\psi_0\rangle , \neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \vdash_{\mathbf{f}} \bot}
}{\neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle \vdash_{\mathbf{f}} \neg\neg\langle\psi_0\rangle)}
}{\neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \vdash_{\mathbf{f}} \langle\psi_0\rangle}
\qquad
\dfrac{\vdots\ \text{(same as left)}}{\neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \vdash_{\mathbf{f}} \langle\psi_1\rangle}
}{
(\supset\text{-I})\,\dfrac{\neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \vdash_{\mathbf{f}} \langle\psi_0\rangle \wedge \langle\psi_1\rangle}{\vdash_{\mathbf{f}} \neg\neg(\langle\psi_0\rangle \wedge \langle\psi_1\rangle) \supset (\langle\psi_0\rangle \wedge \langle\psi_1\rangle)}
}
$$

Part B

$$
(\supset\text{-E})\,\dfrac{
(\text{ax})\,\dfrac{}{\neg\neg\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)}
\qquad
(\supset\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
(\text{ax})\,\dfrac{}{\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle) \vdash_{\mathbf{f}} \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)}
\quad
(\text{ax})\,\dfrac{}{\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle \vdash_{\mathbf{f}} \neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle}
}{\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle , \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle) \vdash_{\mathbf{f}} \bot}
}{\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle \vdash \neg\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)}
}{
(\supset\text{-I})\,\dfrac{
(\supset\text{-I})\,\dfrac{\neg\neg\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle), \neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle \vdash_{\mathbf{f}} \bot}{\neg\neg\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle) \vdash_{\mathbf{f}} \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)}
}{\vdash_{\mathbf{f}} \neg\neg\neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle) \supset \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)}
}
$$

Part C

$$
(\supset\text{-E})\,\dfrac{
\dfrac{\text{I.H.}}{\vdash_{\mathbf{f}} \neg\neg\langle\psi_1\rangle \supset \langle\psi_1\rangle}
\qquad
(\supset\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
(\text{ax})\,\dfrac{}{\neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle) \vdash_{\mathbf{f}} \neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle)}
\quad
(\supset\text{-I})\,\dfrac{
(\supset\text{-E})\,\dfrac{
(\text{ax})\,\dfrac{}{\neg\langle\psi_1\rangle \vdash_{\mathbf{f}} \neg\langle\psi_1\rangle}
\quad
(\supset\text{-E})\,\dfrac{(\text{ax})\,\dfrac{}{\langle\psi_0\rangle \supset \langle\psi_1\rangle \vdash_{\mathbf{f}} \langle\psi_0\rangle \supset \langle\psi_1\rangle} \quad (\text{ax})\,\dfrac{}{\langle\psi_0\rangle \vdash_{\mathbf{f}} \langle\psi_0\rangle}}{\langle\psi_0\rangle , \langle\psi_0\rangle \supset \langle\psi_1\rangle \vdash_{\mathbf{f}} \langle\psi_1\rangle}
}{\langle\psi_0\rangle , \neg\langle\psi_1\rangle , \langle\psi_0\rangle \supset \langle\psi_1\rangle \vdash_{\mathbf{f}} \bot}
}{\langle\psi_0\rangle , \neg\langle\psi_1\rangle \vdash_{\mathbf{f}} \neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle)}
}{\neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle), \langle\psi_0\rangle , \neg\langle\psi_1\rangle \vdash_{\mathbf{f}} \bot}
}{\neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle), \langle\psi_0\rangle \vdash_{\mathbf{f}} \neg\neg\langle\psi_1\rangle}
}{
(\supset\text{-I})\,\dfrac{
(\supset\text{-I})\,\dfrac{\neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle), \langle\psi_0\rangle \vdash_{\mathbf{f}} \langle\psi_1\rangle}{\neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle) \vdash_{\mathbf{f}} \langle\psi_0\rangle \supset \langle\psi_1\rangle}
}{\vdash_{\mathbf{f}} \neg\neg(\langle\psi_0\rangle \supset \langle\psi_1\rangle) \supset \langle\psi_0\rangle \supset \langle\psi_1\rangle}
}
$$

Figure 2.3: Parts of Proofs for Lemma 2.10.3. I.H. stands for induction hypothesis.

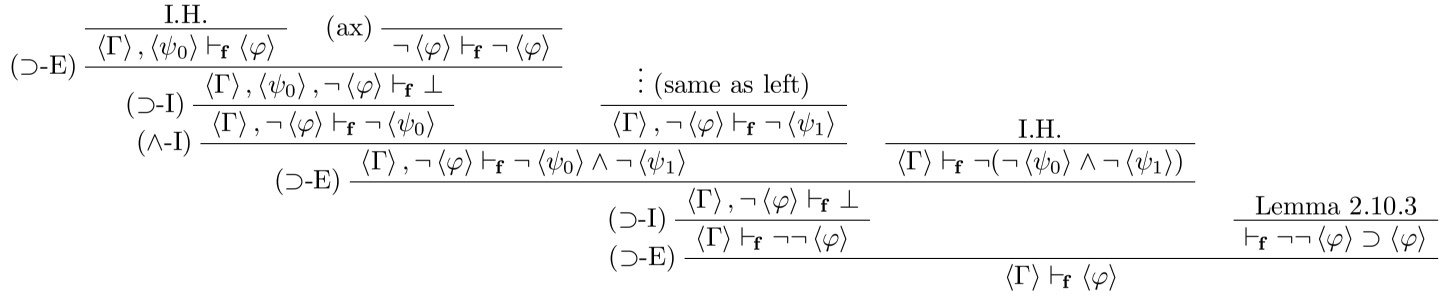

Figure 2.4: (∨-E) case in the proof of Theorem 2.10.4.

2.11 Model Translation

In Section 2.10, we considered a translation from a formula interpreted in $\mathbf{S4} * \cdots * \mathbf{S4}$ into a formula interpreted in **IEC**. It is natural to ask for an adjoint model translation that translates a model of **IEC** into a model of $\mathbf{S4} * \cdots * \mathbf{S4}$.

From a given finite model of **IEC** $M = \langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$, we construct a model for $\mathbf{S4} * \cdots * \mathbf{S4}$ $M' = \langle W', (R_a)_{a\in A}, \rho'\rangle$. We also give a function $t\colon W \to W'$ so that the following equivalency holds

$$\langle W, \preceq, (f_a)_{a\in A}, \rho\rangle, w \models \langle\varphi\rangle \Longleftrightarrow \langle W', (R_a)_{a\in A}, \rho'\rangle, t(w) \models_c \varphi.$$

where $\models_c$ stands for the validity relation for $\mathbf{S4} * \cdots * \mathbf{S4}$ defined in Definition 2.11.2.

Definition 2.11.1. *A model for multiple S4 modal logic is a tuple* $\langle W, (R_a)_{a\in A}, \rho\rangle$ *where*

- W *is a set.*
- R_a *is a preorder on* W*.*
- $\rho\colon PVar \to \mathcal{P}(W)$*.*

Definition 2.11.2. *For a formula, a model for multiple S4 modal logic* $\langle W, (R_a)_{a\in A}, \rho\rangle$ *and a state* $w \in W$*, we define the validit relation* $M = \langle W, (R_a)_{a\in A}, \rho\rangle, w \models_c \varphi$ *inductively on the form of* φ *as follows:*

(Case $\varphi = \bot$**)** $M, w \models_c \bot$ *never holds.*

(Case $\varphi = P$**)** $M, w \models_c P$ *if and only if* $w \in \rho(P)$*.*

(Case $\varphi = K_a\psi$**)** $M, w \models_c K_a\psi$ *if and only if* $M, v \models_c \psi$ *for any* $v \in W$ *with* wR_av*.*

(Case $\varphi = \psi_0 \wedge \psi_1$**)** $M, w \models_c \psi_0\wedge\psi_1$ *if and only if both* $M, w \models_c \psi_0$ *and* $M, w \models_c \psi_1$ *hold.*

(Case $\varphi = \psi_0 \vee \psi_1$**)** $M, w \models_c \psi_0 \vee \psi_1$ *if and only if either* $M, w \models_c \psi_0$ *or* $M, w \models_c \psi_1$ *holds.*

(Case $\varphi = \psi_0 \supset \psi_1$**)** $M, w \models_c \psi_0 \supset \psi_1$ *if and only if the validity* $M, w \models_c \psi_0$ *implies the validity* $M, w \models_c \psi_1$*.*

Now, we define the translation of models.

Notation 2.11.3. $\uparrow X$ *denotes the upward-closure of a set* X*.*

Definition 2.11.4. *For a finite model of* **IEC** $M = \langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$*, we define a model for* $\boldsymbol{S4} * \cdots * \boldsymbol{S4}$ *called* $[M] = \langle [W], (R_a)_{a\in A}, [\rho]\rangle$*.*

- $[W]$ *is the set of maximal elements of* W*.*
- xR_ay *if and only if* $f_a(x) \preceq y$*.*
- $[\rho](P) = \rho(P) \cap [W]$*.*

Lemma 2.11.5. *The tuple defined above is actually a model for* $\boldsymbol{S4} * \cdots * \boldsymbol{S4}$*.*

Proof. We just prove that R_a is a preorder.

- R_a is reflexive. xR_ax is equivalent to $f_a(x) \preceq x$. This holds because f_a is a desceinding function by Definition 2.4.1.
- R_a is transitive. Assume xR_ay and yR_az. This is equivalent to $f_a(x) \preceq y$ and $f_a(y) \preceq z$. Since f_a is monotonic, $f_a(y) \succeq f_a(f_a(x))$. Since f_a is idempotent, $f_a(y) \succeq f_a(x)$. Combining two of the above, we have $z \succeq f_a(x)$. This means xR_az.

□

Now we can show the main result of this section. The translation of formulas from $\mathbf{S4} * \cdots * \mathbf{S4}$ to **IEC** is beautifully combined with the translation of models from **IEC** to $\mathbf{S4} * \cdots * \mathbf{S4}$.

Theorem 2.11.6. *For a finite model* M *of* **IEC***, the following equivalency holds:*

$$M, w \models \langle\varphi\rangle \Longleftrightarrow [M], v \models_c \varphi \text{ for all } v \in [W] \text{ with } v \succeq w.$$

Proof. By induction on the form of φ. We let $M = \langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$ and $[M] = \langle [W], (R_a)_{a\in A}, [\rho]\rangle$. We abbreviate $M, w \models \varphi$ into $w \models \varphi$ and $[M], w \models_c \varphi$ into $w \models_c \varphi$.

(Case $\varphi = \bot$) Neither side ever holds.

(Case $\varphi = P$) Note $\langle\varphi\rangle = \neg\neg P$.

$$\begin{aligned} w \models \neg\neg P \Leftrightarrow\ & \text{for any } x \succeq w, \text{ there exists } x \preceq v \in W \text{ exists } v \in \rho(P) \\ \Leftrightarrow\ & v \models_c P. \text{ for all } v \in [W] \text{ with } v \succeq w. \end{aligned}$$

(Case $\varphi = K_a\psi$) Note $\langle\varphi\rangle = \neg\neg K_a\psi$[4].

$$
\begin{aligned}
w \models \neg\neg K_a \langle\psi\rangle \Leftrightarrow\ & \text{for any } v \succeq w, \text{ there exists } x \succeq v \text{ and } f_a(x) \models \langle\psi\rangle \\
\Leftrightarrow\ & \text{for any } v \in [W] \text{ with } v \succeq w, f_a(v) \models \langle\psi\rangle \\
\Leftrightarrow\ & \text{for any } v \in [W] \text{ with } v \succeq w, \text{ for any } x \succeq f_a(v), x \models_c \psi \quad \text{(I.H.)} \\
\Leftrightarrow\ & \text{for any } v \in [W] \text{ with } v \succeq w, v \models_c K_a\psi.
\end{aligned}
$$

(Case $\varphi = \psi_0 \wedge \psi_1$) Note $\langle\varphi\rangle = \langle\psi\rangle_0 \wedge \langle\psi\rangle_1$. Directly from the induction hypothesis.

(Case $\varphi = \psi_0 \vee \psi_1$) Note $\langle\varphi\rangle = \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle)$.

$$
\begin{aligned}
& w \models \neg(\neg\langle\psi_0\rangle \wedge \neg\langle\psi_1\rangle) \\
\Leftrightarrow\ & \text{for any } v \succeq w, \text{ there exists } x \succ v \text{ and either } x \models \langle\psi_0\rangle \text{ or } x \models \langle\psi_1\rangle \text{ holds.} \\
\Leftrightarrow\ & \text{for any } v \in [W] \text{ with } v \succeq w, \text{ either } v \models \langle\psi_0\rangle \text{ or } x \models \langle\psi_1\rangle \text{ holds.} \\
\Leftrightarrow\ & \text{for any } v \in [W] \text{ with } v \succeq w, v \models_c \psi_0 \vee \psi_1 \text{ holds.}
\end{aligned}
$$

(Case $\varphi = \psi_0 \supset \psi_1$) ($\Rightarrow$) Assume $w \models \langle\psi_0\rangle \supset \langle\psi_1\rangle$. For any $v \succeq w$, $v \models \langle\psi_0\rangle$ implies $v \models \langle\psi_1\rangle$. Especially, for any $v \in [W]$ with $v \succeq w$, $v \models \langle\psi_0\rangle$ implies $v \models \langle\psi_1\rangle$. By induction hypothesis, For any $v \in [W]$ with $v \succeq w$, $v \models_c \psi_0$ implies $v \models_c \psi_1$. By definition of $\models_c$, $v \models_c \psi_0 \supset \psi_1$ holds for such v.
($\Leftarrow$) Assume $[M], v \models_c \psi_0 \supset \psi_1$ for all $v \in [W]$ with $v \succeq w$. For an arbitrary chosen $x \succeq w$, assume $x \models \langle\psi_0\rangle$. By induction hypothesis, for all $v \in [W]$ with $v \succeq x$, $v \models_c \psi_1$ holds. By assumption $v \models_c \psi_1$ holds. By induction hypothesis, $x \models \langle\psi_1\rangle$ holds. That means $w \models \langle\psi_0\rangle \supset \langle\psi_1\rangle$.

□

Extending this result to infinite models is future work. It would require coinductive methods. That would be a prerequisite to fully understand the relationship between **IEC** and $\mathbf{S4} * \cdots * \mathbf{S4}$. Viewing this relationship as an adjoint relation might be interesting especially after we consider reduction of proofs in both logics. It would be also interesting to Compare the proofs of Theorem 2.10.4 and Theorem 2.11.6 and then find duality among them.

[4] I.H. stands for induction hypothesis.

2.12 Comparison with Creative Subject Argument

Dummet [9, Section 6.3] gives an axiom candidate

$$\forall n(\vdash_n (\varphi \vee \psi)) \supset (\vdash_n \varphi) \wedge (\vdash_n \psi)$$

for creative subjects. When we interpret $\vdash_n$ as a modality, this axiom candidate is very similar to the rule $(\vee K)$. This axiom candidate is validated by a position with "we have proved a statement just in case we have effected a construction which would, by itself, be a proof of that statement, whether or not we have noticed that it is so."

Since the creative subject argument involves a clock n of natural number, it assumes total order of time so that it can be regarded as a special case of the model of **IEC**. Also, the creative subject argument only involves a single agent so that it can be regarded as a special case of the model of **IEC**.

2.13 Future Work

When we consider reduction of proofs, we speculate that we can find an upper bound of the computational complexity of the decision of whether a formula is theorem or not.

The proofs of strong completeness and finite model property given here are not constructive in that double negation elimination is used in the meta level. We speculate that the whole argument can be rewritten constructively, using methods similar to those used by Veldman [41], who gave an intuitionistic proof of completeness of intuitionistic predicate logic.

It remains open whether the classical epistemic logic can be interpreted in **IEC** in the spirit of Prawitz's reductive proof theory [33].

Chapter 3

Axiom Type for Sequential Consistency

A schedule determines temporal partial order of events such as message sending and receiving. A correct program must behave correctly under every schedule. Shared memory consistency is a restriction on schedules. When a stronger memory consistency is posed, it is easier for programs to behave correctly. This is analogous to the fact that when a stronger condition is posed upon models, more formulas become valid.

In this section, we characterise sequential consistency with a set of axioms. Sequential consistency defined by Lamport [26] is essentially a condition requiring the states of memory lined up in a total order. We define a deduction system $\vdash_{SC}$ by adding an axiom type to **IEC** and characterise sequential consistency.

Henceforth, we assume $A = \{\mathsf{m}\} \cup P \quad (\mathsf{m} \notin P)$, where P is the set of processes and m represents the shared memory.

3.1 Definitions

Sequential consistency requires the memory states to line up in a total order. A straightforward way to model sequential consistency might be choosing the set of memory states in the model and then asserting the memory states are lined up in a total order. Actually, we can identify a memory state as a state w with $f_{\mathsf{m}}(w) = w$ because this equation asserts that the memory's state seen from the state w is the state w itself. This straightforward modelling of sequential consistency turns out to be in appropriate logically because there is no formula which holds exactly in the models defined in that naive way. Even when there are memory states v and w without temporal relation between them, if the whole model is consists of a part containing v and another disjoint, unrelated part containing w, no formula on no state can recognise the break of sequential consistency. Considering this pitfall, we can model sequential

consistency as a class of models defined below.

Definition 3.1.1. *A sequential model is a model where for any states w, w' and x, $x \preceq w$, $x \preceq w'$, $f_{\mathsf{m}}(w) = w$ and $f_{\mathsf{m}}(w') = w'$ imply $w \preceq w'$ or $w' \preceq w$.*

Definition 3.1.2. *We let SC be the set of formula of the form $(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$.*

We add a rule (SC) to the previous calculus $\vdash$: $\dfrac{}{\vdash \varphi}\ (SC)$ *$(\varphi \in SC)$*

We define $\Gamma \vdash_{SC} \varphi$ in the same way as $\Gamma \vdash \varphi$.

Note that all axioms in the set SC are classical tautologies so that adding these axioms to classical logic is meaningless. This is the merit of using intuitionistic logic rather than classical logic.

3.2 Soundness

Lemma 3.2.1. *$\vdash_{SC} \varphi \Rightarrow M \models \varphi$ for any sequential model M.*

Proof. We extend the induction of Lemma 2.5.1 with a clause for the rule (SC).

(SC) Seeking contradiction, assume $M, w \not\models (K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$. The definition for $\models$ says that there exist states $w_0, w_1 \succeq w$ with $M, w_0 \models K_{\mathsf{m}}\varphi$, $M, w_1 \models K_{\mathsf{m}}\psi$, $M, w_1 \not\models K_{\mathsf{m}}\psi$ and $M, w_0 \not\models K_{\mathsf{m}}\varphi$. These and Kripke monotonicity (Lemma 2.4.3) contradicts to the assumption that M is a sequential model.

Other cases are the same as Lemma 2.5.1. □

3.3 Strong Completeness

Definition 3.3.1. *A set of formulas Γ is SC-saturated if and only if all of these conditions are satisfied:*

1. *Γ is SC-deductively closed, i.e., $\Gamma \vdash_{\mathrm{SC}} \varphi \Rightarrow \varphi \in \Gamma$,*
2. *$\varphi \vee \psi \in \Gamma \Rightarrow \varphi \in \Gamma$ or $\psi \in \Gamma$,*
3. *$\Gamma \nvdash_{\mathrm{SC}} \bot$.*

Lemma 3.3.2 (Saturation lemma)**.** *For a set of formulas Γ with $\Gamma \nvdash_{\mathrm{SC}} \varphi$, there exists a saturated set of formulas Γ^ω with $\Gamma^\omega \nvdash_{\mathrm{SC}} \varphi$ and $\Gamma \subset \Gamma^\omega$.*

This lemma can be proved in the same way as Lemma 2.7.6 where each $\vdash$ is replaced by $\vdash_{\mathrm{SC}}$.

Definition 3.3.3 (Canonical model candidate for sequential consistency)**.** *We define a tuple*
$M^{sc} = \langle W^{\mathrm{SC}}, \preceq^{\mathrm{SC}}, (f_a^{\mathrm{SC}})_{a\in A}, \rho^{\mathrm{SC}}\rangle$ *in the same way as Definition 2.7.7 of* M^c *except that* W^{sc} *is the set of SC-saturated sets of formulas.*

Lemma 3.3.4 (Canonical model for sequential consistency)**.** *The tuple* M^{sc} *is a sequential model.*

Proof. First, we can show, in the same way as before, that checking f_a^{SC} is actually a function $W^{\mathrm{SC}} \to W^{\mathrm{SC}}$. Also, checking each condition in Definition 2.4.1 is similar so that we see M^{SC} is actually a model. Finally, to see that the model M^{SC} is sequential, let Γ, Δ and Θ be states of M^{SC} and assume $\Theta \preceq^{\mathrm{SC}} \Delta$, $\Theta \preceq^{\mathrm{SC}} \Delta$, $f_{\mathsf{m}}^{\mathrm{SC}}(\Gamma) = \Gamma$ and $f_{\mathsf{m}}^{\mathrm{SC}}(\Delta) = \Delta$. We claim that either $\Delta \preceq^{\mathrm{SC}} \Gamma$ or $\Gamma \preceq^{\mathrm{SC}} \Delta$ holds. Seeking contradiction, deny the claim. Since the relation $\preceq^{\mathrm{SC}}$ is actually the set theoretic inclusion, there exist formulas φ and ψ with $\varphi \in \Gamma$, $\varphi \notin \Delta$, $\psi \in \Delta$ and $\psi \notin \Gamma$. Since $f_{\mathsf{m}}^{\mathrm{SC}}(\Gamma) = \Gamma$, $K_a\psi \notin \Gamma$ and $K_a\varphi \in \Gamma$ hold. Similarly, $K_a\varphi \notin \Delta$ and $K_a\psi \in \Delta$ hold. Since Θ is SC-saturated, $(K_a\varphi \supset K_a\psi) \vee (K_a\varphi \supset K_a\psi)$ is in Θ. The definition of saturation says either $K_a\varphi \supset K_a\psi \in \Theta$ or $K_a\psi \supset K_a\varphi \in \Theta$. Consequently, either $K_a\varphi \supset K_a\psi \in \Gamma$ or $K_a\psi \supset K_a\varphi \in \Delta$ holds. Each case leads to contradiction by deductive closedness of Γ and Δ. □

Lemma 3.3.5. *For an SC-saturated set of formulas* Γ *and the canonical model for sequential consistency* M^{sc}*, an equivalency* $\varphi \in \Gamma \iff M^{sc}, \Gamma \vdash_{\mathrm{SC}} \varphi$ *holds.*

This lemma can be proved in the same way as Lemma 2.7.9.

Theorem 3.3.6 (Strong completeness for sequential consistency)**.** $\Gamma \vdash_{\mathrm{SC}} \varphi$ *holds if* $M \models \Gamma$ *implies* $M \models \varphi$ *for every sequential model* M*.*

Proof. We show the contraposition: assuming $\Gamma \nvdash_{\mathrm{SC}} \varphi$, we show that there exists a sequential model M that satisfies $M \models \Gamma$ but not $M \models \varphi$. By Lemma 3.3.2, there is an SC-saturated set of formula Γ' with $\Gamma' \nvdash \varphi$ and $\Gamma' \supset \Gamma$. By Lemma 3.3.5, $M^{\mathrm{SC}}, \Gamma' \models \Gamma$ but not $M^{\mathrm{SC}}, \Gamma' \models \varphi$. These two facts deny $\Gamma \models \varphi$. □

Example Theorem In Introduction, we gave an example of deducible judgements of $\vdash_{\mathrm{SC}}$:
$K_aK_{\mathsf{m}}K_a\varphi, K_bK\mathsf{m}K_b\psi \vdash_{\mathrm{SC}} K_aK_b\psi \vee K_bK_a\varphi$. We give a proof for this judgement in Figure 3.1.

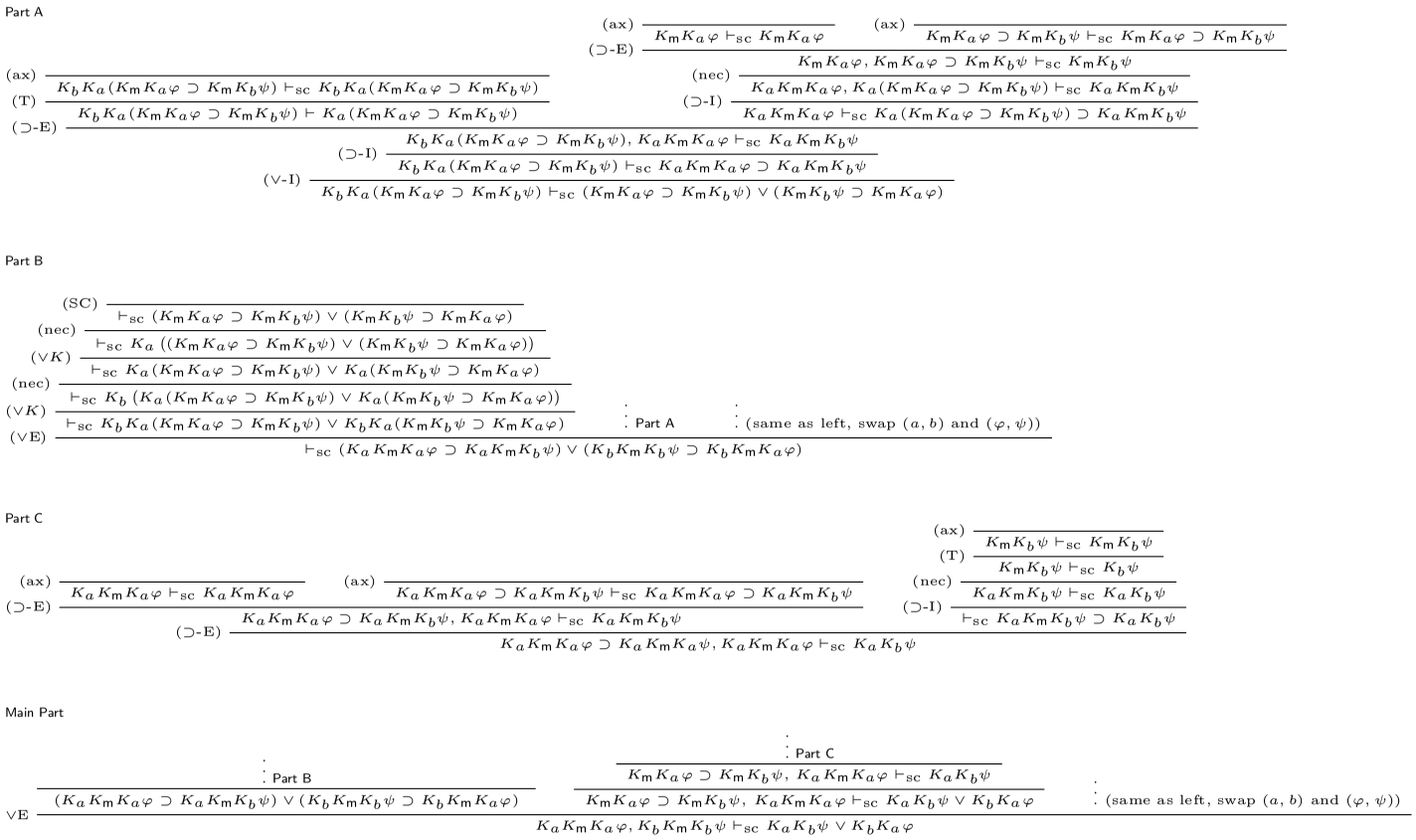

Figure 3.1: A proof diagram for an example theorem in $\vdash_{\mathrm{sc}}$.

Chapter 4

Waitfree Computation

4.1 Problem Domain

A distributed program assigns a program to each process. When we execute a distributed program, processes obtain execution steps in the order determined by the scheduler.

A distributed program is waitfree when there exists such a fixed number k that under any schedule, any process finishes before using k steps. The informal meaning of this condition is forbidding a process to wait for another process. Assuming a process p waits for another process q to do something, under an unfriendly schedule, the condition for waitfreedom is broken. Actually, under a schedule giving the first k steps exclusively to the process p the process q cannot do anything in those first k steps while the process p waits for the process q to do that something, thus breaking the wait-free condition.

Some tasks can be solved by a waitfree distributed program while others cannot. In this chapter, we consider the problem of distinguishing the waitfreely solvables task and the waitfreely unsolvable ones. Although this problem is undecidable in general [12], we find an approximation problem that is decidable.

4.2 Logical Representation of the Problem

While sequential consistency is a restriction on schedules, wait-freedom is a restriction on distributed programs. The behaviour of distributed programs depend on the schedule[1]. The a correct distributed program can be described as a distributed program

[1] A motivation for introducing formal reasoning into the area of distributed computation is in this fact, which makes testing harder.

which gives correct behaviour under any schedule. This form of definition is similar to that of validity of logical a formula: a valid logical formula is a formula which is satisfied by any model. We consider the schedule v.s. distributed program relation is similar to the formula v.s. model relation. In Chapter 3, in this chapter, we express wait-freedom as a class of formulas.

A distributed program specifies from which process, to which process, and in what order signals are transmitted. We consider the signal transimission in a logical formula. In short, a modality over a modality like K_pK_qP describes communication. We regard processes as agents. A propositional variable I_p informally denotes the fact that the process p has started. A logical formula $K_qK_pI_p$ informally states "the process p was aware of the fact that the process p had started, and then told the fact to the process q." Similarly, another formula $K_pK_qK_pI_p$ informally states "the process p was aware of the fact that the process p had started, and then told the fact to the process q. The process q in turn told back to the process p that the process q had received the fact from p." The latter communication pattern can be obtained by programs described in the following lines:

1. When process p starts, it sends a signal to the process q, then waits for a reply from q and then terminates.

2. When process q starts, it waits for a signal from the process p, replies back to p, and then terminates.

Unfortunately, since this distributed program is not waitfree, we cannot include the formula $K_pK_qK_pI_p$ in the class of formulas representing waitfreedom. We will define the class of formulas and call them waitfree protocol descriptions.

Actually, although a process running a waitfree program is forbidden to wait for another process, it is allowed to wait for the shared memory[2]. For example, after a process makes a read request to the shared memory, it is allowed to wait for a value from the shared memory. Also, after a process makes a write request to the shared memory, it is allowed to wait for an acknowledgement from the shared memory. That is why we introduced a special agent $\mathsf{m} \in A$ representing the shared memory. We call other agents in A processes so that $A = \{\mathsf{m}\} \cup P \quad (\mathsf{m} \notin P)$ holds.

After these observations, we can obtain the class of formulas representing a waitfree distributed program. When we are interested in a fixed waitfree distributed program, for any process, there is a constant k and the process can interact with the memory

[2]Otherwise, any communication whatsoever would be impossible.

for up to k times. Moreover, since a process is only allowed to interact with the shared memory not with the process. Thus, a waitfree distributed program can only make sure the property described as $K_p K_{\mathsf{m}} K_p \cdots K_{\mathsf{m}} K_p P$ where K_{m} and K_p appear alternatively. We call such a logical formula a waitfree program description.

Finally, as well the class of schedules and the class of wait-free programs, we describe specifications for wait-free programs in a logical formula. We forcifully decide that we only specify the posession of knowledge at finish of the program so that we only consider positive logical formulas as waitfree specifications.

We define a class of formulas called waitfree assertions combining the waitfree protocol description and the waitfree specifications. Waitfree assertions have a special finite model property: if a waitfree assertion is consistent[3], there is a finite model of a special shape where the assertion is valid. The special shape mimics the scheduling of shared memory defined by Saks and Zaharoglou [34].

Definition 4.2.1. *Assume there is a vector of atomic formulas $(I_p)_{p\in P}$. A waitfree protocol description φ is a formula of the form*

$$\varphi = \bigwedge_{p\in P} K_p K_{\mathsf{m}} K_p \cdots K_p I_p$$

where K_p and K_{m} appear alternatively in "$\cdots$". A waitfree task specification ψ is defined with the BNF:

$$\psi ::= K_p\psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid I_p$$

where p stands for a process in P. A waitfree assertion is a formula $\varphi \supset \psi$ where φ is a waitfree protocol description and ψ is a waitfree task specification.

4.3 Representation of Schedules as Models

Definition 4.3.1. *A partial schedule $(\sigma_i)_{i\in I}$ is a finite sequence of subsets of P.*

Definition 4.3.2. *For a process $p \in P$ and a partial schedule σ, $count_p(\sigma)$ is the cardinality $|\{i \in I \mid p \in \sigma_i\}|$.*

For a waitfree protocol description $\varphi = \bigwedge_{p\in P} K_p K_{\mathsf{m}} \cdots K_p I_p$, $count_p(\varphi)$ is the number of K_{m} occurrences in $K_p K_{\mathsf{m}} \cdots K_p I_p$.

A partial schedule σ is compatible to a waitfree protocol description φ if $count_p(\varphi) = count_p(\sigma)$ for any process $p \in P$.

We introduce a special thing o called an external observer with $o \notin A$.

[3] A formula φ is consistent if and only if $\bot$ cannot be proved even if φ is added as an axiom.

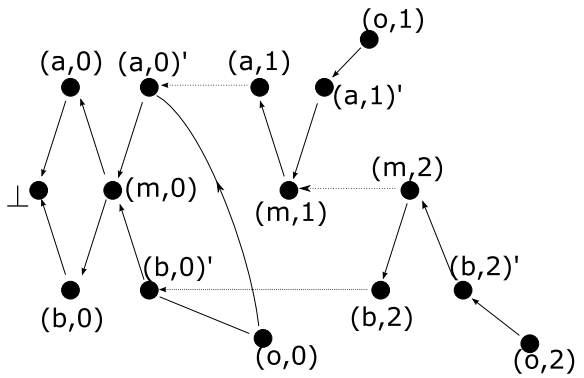

Figure 4.1: A model $R(\cdot, \sigma)$ induced by the partial schedule $\sigma = (\{a, b\}, \{a\}, \{b\})$. A solid arrow pointing to (x, n) shows an f_x mapping. Dotted arrows show $\preceq$ relations. We omit implied arrows and the valuation.

Definition 4.3.3. *For a waitfree protocol description φ and a compatible partial schedule $(\sigma_i)_{i \in I}$, we define a waitfree schedule model $R(\varphi, \sigma) = \langle W, \preceq, (f_x)_{x \in A}, \rho \rangle$ as:*

- $W = \{(p, i) \in P \times \mathbb{N} \mid p \in \sigma_i\} \cup \{(p, i)' \in P \times \mathbb{N} \mid p \in \sigma_i\} \cup \{(\mathsf{m}, i) \mid i \in I\} \cup \{(o, i) \mid i \in I\} \cup \{\bot\}$,
- $(a, i) \preceq (m, i) \preceq (a, i)'$,
- $(x, j) \preceq (o, i)$ *if and only if* $j \leq i$,
- $\bot \preceq w$ *for all* $w \in W$,
- $(x, j)' \preceq (o, i)$ *if and only if* $j \leq i$,
- $f_a(w) = \begin{cases} \text{the least } (a, j) \text{ with } (a, j) \preceq w \text{ (if there exists such } (a, j)) \\ \text{(the definition of } \preceq \text{ assures there is the least such } (a, j)), \\ \bot \text{ (if such } (a, j) \text{ does not exist).} \end{cases}$
- $\rho(I_a) = \{w \in W \mid (a, 0) \preceq w\}$.

An example of a model induced by a partial schedule is shown in Figure 4.1.

We can state the logical characterisation of waitfree communication.

Theorem 4.3.4 (Completeness for waitfree communication)**.** *Assume $\varphi \supset \psi$ is a waitfree assertion. The relation $\vdash_{SC} \varphi \supset \psi$ holds if the relation $R(\varphi, \sigma), (o, n) \models \psi$ holds for any compatible partial schedule σ where the state (o, n) is the last state of the waitfree model $R(\varphi, \sigma)$.*

To prove completeness, we only use special models called singleton models induced by a permutation of processes.

Definition 4.3.5. *For a set of processes P, we define $\mathsf{S}(P)$ to be the set of the permutations of P.*

Definition 4.3.6. *For $\pi \in \mathsf{S}(P)$ and $0 \leq k \leq |P|$, we define $SC(\pi, k)$ to be the set $\{K_{\mathsf{m}} K_a I_a \supset K_{\mathsf{m}} K_b I_b \mid b \leq a \text{ in } \pi_0, \ldots \pi_k\}$.*

Lemma 4.3.7. $\vdash_{\mathrm{sc}} \bigvee_{\pi \in \mathsf{S}(A)} SC(\pi, |P|)$ *holds.*

Proof. It suffices to use rule (SC) many times. □

Definition 4.3.8. *For a permutation π of P and a waitfree protocol description φ, we define a partial schedule $\sigma(\varphi, \pi)$ as*

$$\sigma(\varphi, \pi) = \overbrace{\pi_0, \cdots, \pi_0}^{count_{\pi_0}(\varphi)}, \overbrace{\pi_1, \cdots, \pi_1}^{count_{\pi_1}(\varphi)}, \cdots\cdots\cdots, \overbrace{\pi_n, \cdots, \pi_n}^{count_{\pi_n}(\varphi)}.$$

Definition 4.3.9. *A singleton model is a model of the form $R(\varphi, \sigma(\varphi, \pi))$. We abbreviate this to $R(\varphi, \pi)$.*

For a singleton model and an index $k \in I$, w_k denotes the minimum external observer state above all π_j states for $j < k$.

Definition 4.3.10. *For a waitfree protocol description $\varphi = \bigwedge_{a \in A} \overbrace{K_a K_{\mathsf{m}} K_a \cdots K_a}^{n_a} I_a$, we define the restriction*

$\varphi \restriction_{p,k} = \bigwedge_{a \in A \restriction_{p,k}} \overbrace{K_a K_{\mathsf{m}} K_a \cdots K_a}^{n_a} I_a$, *where $A \restriction_{p,k} = \{a \mid p_j = a \text{ for some } j < k\}$.*

Lemma 4.3.11. $R(\varphi, \pi), (o, k) \models \psi \Longrightarrow SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset \psi$.

Proof of Lemma 4.3.11. By induction on k.

(Case $k = 0$) We show a stronger proposition: $(o, 0) \models \psi \quad \Longrightarrow \quad f_{p_0}(o, 0) \models \psi, \vdash \varphi \restriction_{p,0} \supset \psi$ and $\vdash \varphi \restriction_{p,0} \supset K_a \psi$. by inner induction on ψ.

(When ψ is an atomic formula P) $P = I_{\pi_0}$ holds. Since $\varphi \restriction_{\pi,0} = K_{\pi_0} K_{\mathsf{m}} K_{\pi_0} \cdots K_{\mathsf{m}} K_{\pi_0} I_{\pi_0}$, $\vdash \varphi \restriction_{\pi,0} \supset K_{\pi_0} P$ holds. So, $SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset K_{\pi_0} P$ holds. Consequently, $SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset P$ also holds.

(When $\psi = \psi_0 \wedge \psi_1$ or $\psi_0 \vee \psi_1$) Induction goes smoothly.

(When $\psi = K_a \psi'$) Assume $(o, 0) \models K_a \psi'$. Claim: $a = \pi_0$ holds. Seeking contradiction, assume $a \neq \pi_0$. That means $f_a(o, 0) = \bot$. However, waitfree

task specification is satisfied at the state $\bot$. Contradiction. We have proved $a = \pi_0$. Using this, we can show that $f_a(o, 0) \models \psi'$ holds. By idempotency of f_a, $f_a(f_a((o, 0))) \models \psi'$ holds. This means $f_a((o, 0)) \models K_a\psi'$. Since $(o, 0) \models \psi'$, by inner induction hypothesis, $\vdash \varphi \restriction_{\pi,0}\supset K_a\psi'_a$. By proof theoretic consideration, $\vdash \varphi \restriction_{\pi,0}\supset K_aK_a\psi'$ holds.

(Case $k = k' + 1$) Like the base case, we show a stronger proposition $(o, k) \models \psi \Leftrightarrow f_{\pi_k}((o, k)) \models \psi \Rightarrow SC(\pi, k) \vdash \varphi \restriction_{\pi,k}\supset \psi$ and $SC(\pi, k) \vdash \varphi \restriction_{\pi,k}\supset K_{\pi_k}\psi$, using induction on ψ.

(When $\psi = P$, an atomic formula) Either $R(\varphi, \pi), w_{k'} \models P$ or $I_{\pi_k} = P$ holds. In the former case, by induction hypothesis. In the latter case, similarly as the base case.

(When $\psi = \psi_0 \wedge \psi_1$ or $\psi_0 \vee \psi_1$) Induction goes smoothly.

(When $\psi = K_x\psi'$) If $\pi_k \neq x$, $f_{\pi_k}((o, k)) \models K_x\psi'$ implies $(o, k') \models K_x\psi'$. By outer induction hypothesis, $SC(\pi, k') \vdash \varphi \restriction_{\pi,k'}\supset K_x\psi'$ and $SC(\pi, k') \vdash \varphi \restriction_{\pi,k'}\vdash \varphi \restriction_{\pi,k'}\supset K_x\psi'$ hold. Here, we can safely replace k' with k. If $\pi_k = x$, $(o, k) \models K_x\psi'$ imply $(o, k) \models \psi'$. By inner induction hypothesis, we obtain $SC(\pi, k) \vdash \varphi \restriction_{\pi,k}\supset K_x\psi'$. This also implies $SC(\pi, k) \vdash \varphi \restriction_{\pi,k}\supset K_xK_x\psi'$.

□

After showing this generalised lemma, proving Theorem 4.3.4 is easy.

Proof of Theorem 4.3.4. Since $R(\varphi, p), w_{|P|} \models \psi$, $SC(p, |P|) \vdash \varphi \supset \psi$. By Lemma 4.3.7, $\vdash_{\mathrm{SC}} \varphi \supset \psi$. □

Any models induced by a partial schedule is finite. For a waitfree assertion φ, it is decidable whether $\vdash_{\mathrm{SC}} \varphi$ holds or not.

4.4 Decidability of Solvability of Waitfree Task Specification

Definition 4.4.1. *A waitfree task specification ψ is solvable if there is such a waitfree protocol description φ that the relation $R(\varphi, \sigma), (o, n) \models \psi$ holds for any compatible partial schedule σ where the state (o, n) is the last state of the model $R(\varphi, \sigma)$.*

Fact. The set of solvable waitfree task specifications are recursively enumerable because the relation $\vdash_{\mathrm{SC}}$ is axiomatised.

Fact. The set of unsolvable waitfree task specifications are recursively enumerable because partial schedule-induced models are recursively enumerable.

Theorem 4.4.2. *It is decidable whether a waitfree task specification is solvable or not.*

Proof. These two facts imply that it is decidable whether a waitfree task specification is solvable or not. □

This does not contradict to the undecidability of waitfreely solvable tasks by Gafni and Koutsoupias [12] because the undecidability proof utilises tasks that cannot be expressed by waitfree task specifications. They use tasks involving consensus: the tasks involving making agreements among processes, where whether an output value is allowed or not depends on other processes' output values. Waitfree task specifications cannot describe such tasks.

Chapter 5

Related Work

Van Benthem [39] investigates the connection between intuitionistic logic and information dynamics. He speculates:

> It might be that intuitionistic logic points the way towards a grand synthesis of information analysis in the standard model-theoretic style with the dynamic view of logic as embodied in proof and games.

This paper replies his speculation by defining knowledge in terms of BHK-interpretation and defining a proof system **IEC** embodying the interpretation.

Ondrej Majer's Epistemic Logic with Relevant Agents [28] is similar to **IEC** in that both logics have epistemic modalities and that both logics are not classical. However, the logic given in [28] contains only one modality K for knowledge. This implicitly assumes that there is a single agent, not multiple agents so that it is impossible for their logic to treat communication between multiple agents.

Many logics have both temporal and epistemic modalities [35, 43]. Ewald [10] proposes an intuitionistic logic with temporal modality. We unify the intuitionistic semantics and temporal semantics so that the logic **IEC** lacks temporal modality yet represents some temporal notions. Adding a temporal modality like Ewald [10] would increase the expressivity of the logic, but it would complicate the syntax and semantics. We would like to investigate the simple logic **IEC** first and then expand **IEC** with additional constructs.

In Kobayashi and Yonezawa's logic [24], processes appear in formulas but time does not appear in formulas because time is implicit in the system of logic programming. This logic is different from **IEC** in that this logic is based on linear logic and that their usage is logic programming.

Belnap and Harper's "seeing to it that" (stit) logical operator aims at describing interaction between agents. The semantics for the operator involves both agency and temporal notion, which is more complicated than the meaning of K_a operator in **IEC**. A fundamental difference of the stit operator and the epistemic operator in **IEC** is whether the modalities mention the future or tha past. The stit operator mentions the future while the epistemic operator mentions the past.

Dynamic epistemic logic is a logic that aims at reasoning about communication. However the semantics of the logic involves instantaneous change of models. We argue such instantaneous change of the whole world it is not a natural description of asynchronous communication.

Chapter 6

Conclusion

We defined an intuitionistic modal logic called intuitionistic epistemic logic (**IEC** for short). We defined both a natural deduction system and a Kripke model for it. We proved both soundness and strong completeness. The deduction system of **IEC** is similar to that of classical epistemic logic, but lacks negative introspection and double negation elimination and has distribution of disjunction over epistemic modalities instead. The semantics of **IEC** is similar to that of intuitionistic propositional logic, but has an additional function on the states for each agent, which we call a modal function. We defined the syntactic counterpart of the modal function and used it for extending Aczel's slash and proving disjunction property of **IEC**. The syntactic counterpart of the modal function was also useful for proving strong completeness and finite model property for **IEC**. By disjunction property, we know that the logic **IEC** is a constructive logic. Also, decidability suggests the possibility of typed lambda calculus using **IEC** as the typing system.

On the logic **IEC**, we analysed the concept of sequential consistency and wait-free communication. The deepness of our anlaysis is represented in a deep proof tree (Figure 3.1) for a property of a relatively simple and small wait-free protol involving two processes. Distributed programming over shared memory can be seen as a game involving the scheduler and the program. Logic can be seen as a game involving the models and the formulas. We modelled schedules as a model of logic and programs as formulas. Since sequential consistency is a restriction on schedules, we modeled sequential consistency as a restriction on models. The restriction on the models representing sequential consistency could actually axiomatized using an axiom type that is similar to the axiom type for prelinerity defining a famous intermediate logic. Since waitfreedom is a restriction on programs, we modelled waitfree programs as a set of

formulas called waitfree protocol description. We also modelled specification for waitfree programs as a set of formulas called waitfree task specification. We used a waitfree assertion, which is an implication formula consisting of a waitfree protocol description and a waitfree task specification, to represent an assertion that a waitfree protocol meets a specification.

Chapter 7

Discussion

7.1 Waitfree Computation

The Gödel Prize in 2004 was given to Herlihy and Shavit [19] and Saks and Zaharoglou [34]. This work was motivated by these works. Herlihy and Shavit [19] used subdivision of coloured simplicial complex to model waitfree computation. Each vertex is coloured by an agent. Each simplex contains vertices with distinct colours. A vertex may have an ancestor simplex called carrier. The minimum subset of $(S \cup V) \times (S \cup V)$ containing the ancestor relation and the relation $\in$ forms an order $\sqsubset$. We can define a partial $f_a : S \to S$ where S is the set of simplex in a simplicial complex by letting $f_a(s) = \{x\}$ where x is the maximum vertex below s (w.r.t. $\sqsubset$) whose colour is a. When we add a bottom simplex $\bot$ and make f_a total, we can regard a simplicial complex as a model of **IEC** as in an example (Figure 7.1).

Saks and Zaharoglou [34] use full-information protocol [42]. Even the shared variables remember the whole history. In every component, knowledge increases monotonically through time. This monotonicity suggests that their model can be analysed effectively in Kripke models for intuitionistic logic. Saks and Zaharoglou [34] also suggest that "We believe that it will be worthwhile to explore the connection with the formal theory of distributed knowledge." This work is following their remark in treating waitfree communication in a formal way, especially using a logic with epistemic modality.

7.2 Sequential Consistency or Linearizability

Attiya and Welch [2] pointed out that sequential consistency [26] and linearizability [20] are often confused. We briefly make sure that the deduction system $\vdash_{SC}$ does not

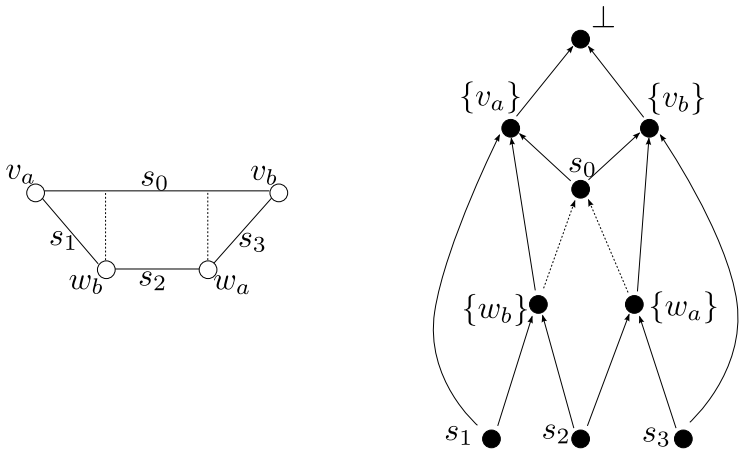

Figure 7.1: How subdivision of simplicial complexes is transformed into **IEC** model. Left: A simplex $s_0 = \{v_a, v_b\}$ is subdivided into $s_1 = \{v_a, w_b\}, s_2 = \{w_a, w_b\}$ and $s_3 = \{w_a, v_b\}$. Right: **IEC** frame obtained from the left subdivision.

characterise linearizability. Herlihy [20] stated that linearizability is a local property; in other words, when each memory object satisfies linearizability, the combined system also has linearizability. However, the axiom type SC is not local. To see that, assume there are two memory objects m and m'. The axiom type SC for m is $(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$. The axiom type SC for m' is $(K_{\mathsf{m}'}\varphi \supset K_{\mathsf{m}'}\psi) \vee (K_{\mathsf{m}'}\psi \supset K_{\mathsf{m}'}\varphi)$. Even when both of these axiom types are available, the *mixed* axiom type $(K_{\mathsf{m}'}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}'}\varphi)$ is not derivable. This shows the characterised property is not local.

7.3 Other Consistency Models

Steinke and Nutt [36] gave a lattice of consistency properties including: sequential consistency, causal consistency, processor consistency, PRAM consistency, cache consistency, slow consistency and local consistency. It is our future work modelling other consistency properties.

7.4 The Cost of Monotonic Reasoning: Latency versus Throughput

The logic **IEC** is more suitable in a situation where latency is more important than throughput. Since we consider time as the partial order of intuitionistic Kripke models,

all knowledge must be preserved during time progress. Communication must be done in full-information manner (as in full-information protocols in [42]) because messages define the partial order. Although there are some methods [13–15, 42] for extracting implementable protocols from full-information protocols, Our logic is advantageous when latency is important so that it is important to know how many message interactions are needed to accomplish a certain task. We plan to investigate network protocols with **IEC**.

We speculate that replacing intuitionistic modalities with linear modalities might enable us to deal with throughput oriented properties.

7.5 λ-calculus

It would be interesting to consider reduction of proofs because it leads to typed programming language for asynchronous communication.

7.6 Disjunction Distribution Over K Modality

Since the semantics for modalities is defined by functions on Kripke frames, the disjunction distributes modalities in **IEC**. Kojima and Igarashi [25] avoids the distribution of modalities over disjunction by giving up functional modality. On the other hand, **IEC** has distribution of modalities over disjunction. We speculate that the difference comes from the interpretation of modalities according to time: in [25], inner subformulas within the scope of the modality are interpreted in the future; while in **IEC**, inner subformulas within the scope of the modalities are interpreted in the past.

By translation of Suzuki [37], when A is a singleton set, a model of **IEC** corresponds to a model of intuitionistic predicate logic with singleton domain in the same manner a model of the logic L_3 of Ono [29] corresponds to the models of intuitionistic predicate logic with constant domain. This fact suggests that the semantics of **IEC** is very simple when A is a singleton set. Simplicity was our aim at the beginning.

7.7 Relationship with Intuitionistic Predicate Logic

The translation of Suzuki [37] suggests **IEC** with a single agent corresponds to a singleton domain. In intuitionistic predicate logic, the quantifiers $\forall$ and $\exists$ quantify over elements of domain. These facts suggest quantification over the set of agents like $\forall x K_x \varphi$. From the logic allowing such quantification, we speculate that, by the method

of program extraction, we can obtain programs whose input and output contain names of agents.

Also, extending the translation of Suzuki— [37] to intuitionistic logic with multiple modailities would be an interesting work.

References

[1] N. Alechina, M. Mendler, V. de Paiva, and E. Ritter. Categorical and Kripke semantics for constructive S4 modal logic. *LNCS*, pages 292–307, 2001.

[2] H. Attiya and J.L. Welch. Sequential consistency versus linearizability. *ACM Transactions on Computer Systems (TOCS)*, 12(2):122, 1994.

[3] P. Balbiani et al. 'Knowable' as 'known after an announcement'. *The Review of Symbolic Logic*, 1(03):305–334, 2008.

[4] A. Baltag, B. Coecke, and M. Sadrzadeh. Epistemic actions as resources. *Journal of Logic and Computation*, 17(3):555, 2007.

[5] P. Bieber and T. Onera-Cert. A logic of communication in hostile environment. In *Computer Security Foundations Workshop III, 1990. Proceedings*, pages 14–22, 1990.

[6] G.V. Bochmann and J. Gesci. A unified method for the specification and verification of protocols. *Proc. of the IFIP'77*, (5), 1977.

[7] V. Costa and M. Benevides. Formalizing concurrent common knowledge as product of modal logics. *Logic Journal of IGPL*, 13(6):665, 2005.

[8] H. Ditmarsch, W. Hoek, and B. Kooi. Dynamic Epistemic Logic. 2007.

[9] M.A.E. Dummett. *Elements of intuitionism*. Oxford University Press, USA, 2000.

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

[11] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about knowledge*. The MIT Press, 2003.

[12] E. Gafni and E. Koutsoupias. Three-processor tasks are undecidable. *SIAM Journal on Computing*, 28(3):970–983, 1999.

[13] J.Y. Halpern. Using reasoning about knowledge to analyze distributed systems. *Annual Review of Computer Science*, 2(1):37–68, 1987.

[14] J.Y. Halpern and R. Fagin. A formal model of knowledge, action, and communication in distributed systems: preliminary report. In *Proceedings of the fourth annual ACM symposium on Principles of distributed computing*, pages 224–236. ACM, 1985.

[15] J.Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM (JACM)*, 37(3):549–587, 1990.

[16] J.Y. Halpern and L.D. Zuck. A little knowledge goes a long way: knowledge-based derivations and correctness proofs for a family of protocols. *Journal of the ACM (JACM)*, 39(3):449–478, 1992.

[17] R. Harrop. On the existence of finite models and decision procedures for propositional calculi. In *Proceedings of the Cambridge Philosophical Society*, volume 54, page 1, 1958.

[18] M. Herlihy. Wait-free synchronization. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 13(1):124–149, 1991.

[19] M. Herlihy and N. Shavit. The topological structure of asynchronous computability. *Journal of the ACM (JACM)*, 46(6):858–923, 1999.

[20] M. Herlihy and J.M. Wing. Linearizability: A correctness condition for concurrent objects. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 12(3):463–492, 1990.

[21] A. Heyting. Die formalen Regeln der intuitionistischen Logik. 1930.

[22] A. Heyting. Die intuitionistische grundlegung der mathematik. *Erkenntnis*, 2(1):106–115, 1931.

[23] L. Jia and D. Walker. Modal proofs as distributed programs. *LNCS*, pages 219–233, 2004.

[24] N. Kobayashi and A. Yonezawa. Asynchronous communication model based on linear logic. *Formal Aspects of Computing*, 7(2):113–149, 1995.

[25] K. Kojima and A. Igarashi. On constructive linear-time temporal logic. *Proc. of IMLA*, 8, 2008.

[26] L. Lamport. How to make a multiprocessor computer that correctly executes multiprocess programm. *IEEE transactions on computers*, 100(28):690–691, 1979.

[27] C.J. Liau. Belief, information acquisition, and trust in multi-agent systems—A modal logic formulation. *Artificial Intelligence*, 149(1):31–60, 2003.

[28] O. Majer and M. Peliš. Epistemic logic with relevant agents. In *The Logica Yearbook 2008*, pages 123–135. Kings College Publications, 2009.

[29] H. Ono. On some intuitionistic modal logics. *Publ. Res. Inst. Math. Sci.*, 13(3):687–722, 1977.

[30] D. Peleg. Communication in concurrent dynamic logic. *J. COMP. SYST. SCI.*, 35(1):23–58, 1987.

[31] J. Plaza. Logics of public communications. *Synthese*, 158(2):165–179, 2007.

[32] G. Plotkin and C Stirling. A framework for intuitionistic modal logics: extended abstract. In *TARK '86: Proceedings of the 1986 conference on Theoretical aspects of reasoning about knowledge*, pages 399–406. Morgan Kaufmann Publishers Inc., 1986.

[33] D. Prawitz. Ideas and results in proof theory. In *Proceedings of the second scandinavian logic symposium*, volume 63, pages 235–307, 1971.

[34] M. Saks and F. Zaharoglou. Wait-free k-set agreement is impossible: The topology of public knowledge. *SIAM journal on computing(Print)*, 29(5):1449–1483, 2000.

[35] M. Sato. A study of Kripke-type models for some modal logics by Gentzen's sequential method. *Publications of the research institute for mathematical sciences*, 13:381, 1977.

[36] R.C. Steinke and G.J. Nutt. A unified theory of shared memory consistency. *Journal of the ACM (JACM)*, 51(5):800–849, 2004.

[37] N.Y. Suzuki. Kripke bundles for intermediate predicate logics and Kripke frames for intuitionistic modal logics. *Studia Logica*, 49(3):289–306, 1990.

[38] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics: An Introduction: Vol.: 1.* North-Holland, 1988.

[39] J. van Benthem. The information in intuitionistic logic. *Synthese*, 167(2):251–270, 2009.

[40] HP Van Ditmarsch, W. Van Der Hoek, and BP Kooi. Concurrent dynamic epistemic logic for MAS. In *Proceedings of the second international joint conference on Autonomous agents and multiagent systems*, pages 201–208. ACM, 2003.

[41] W. Veldman. An intuitionistic completeness theorem for intuitionistic predicate logic. *The Journal of Symbolic Logic*, 41(1):159–166, 1976.

[42] T.Y.C. Woo and S.S. Lam. A lesson on authentication protocol design. *SIGOPS Oper. Syst. Rev.*, 28(3):24–37, 1994.

[43] B. Wozna and A. Lomuscio. A logic for knowledge, correctness, and real time. *LNCS*, 3487:1, 2005.