

Stalnaker’s Epistemic Logic in Isabelle/HOL.*

Laura P. Gamboa Guzman

Iowa State University
Ames, IA 50011, USA
lpgamboa@iastate.edu

Kristin Y. Rozier

Iowa State University
Ames, IA 50011, USA
kyrozier@iastate.edu

The foundations of formal models for epistemic and doxastic logics often rely on certain logical aspects of modal logics such as S4 and S4.2 and their semantics; however, the corresponding mathematical results are often stated in papers or books without including a detailed proof, or a reference to it, that allows the reader to convince themselves about them. We reinforce the foundations of the epistemic logic S4.2 for countably many agents by formalizing its soundness and completeness results for the class of all weakly-directed pre-orders in the proof assistant Isabelle/HOL. This logic corresponds to the knowledge fragment, i.e., the logic for formulas that may only include knowledge modalities in Stalnaker’s system for knowledge and belief. Additionally, we formalize the equivalence between two axiomatizations for S4, which are used depending on the type of semantics given to the modal operators, as one is commonly used for the relational semantics, and the other one arises naturally from the topological semantics.

1 Introduction

Epistemic logics are a family of logics that allow us to reason about knowledge among a group of agents, as well as their knowledge about other’s knowledge [12]. Reasoning about knowledge is useful for detecting and identifying faults during the operation of complex critical systems [7, 27], where important safety properties are formalized using a modal language that combines temporal, in particular, LTL (Linear Temporal Logic), and epistemic modal operators, so to verify the correctness of the system using model checking and related formal fault-detection techniques [9, 21, 24].

When it comes to modal logics for knowledge, most of these logics correspond to normal logics between S4 and S5 [11, 25]. In particular, we consider Stalnaker’s epistemic logic, which coincides with the logic S4.2. It is known that this logic is strictly stronger than S4, but weaker than S5 [8]. This logic is known to be sound and complete with respect to all weakly directed S4-frames, that is, all frames consisting of reflexive and transitive binary relations that are confluent [23], but this proof is often omitted in textbooks where most extensions to system K (the weakest normal modal logic) are usually treated informally.

Additionally, we encode in Isabelle/HOL the axiomatization of S4 obtained from the study of the topological interpretation for modal languages, which was introduced prior to the relational one that is more commonly found in the literature. This topological interpretation is done by reading the modal necessity operator as an interior operator on a topological space, for which is known that the modal logic S4 is complete with respect to all topological spaces [1]. The preferred axiomatization for the logic of topological spaces differs from the one presented in [15], not only from the set of axioms, but also the deductive rules, since it captures the axioms for an interior operator instead of a reflexive and transitive binary relation. As a consequence, this makes the topological axiomatization not directly recognizable as a normal modal logic, since the deduction rules seem to be weaker at first glance. Since several authors

*Supported by NSF CAREER Award CNS-1552934 and NSF:CCRI Award CNS-2016592.

have been recently developing topological semantics for notions of knowledge and belief [2, 4, 3, 16], we provide a formalization for this result, which often gets briefly mentioned and applied without being proved in detail.

Contributions

We formalize Stalnaker’s epistemic logic, which is expressively equivalent to S4.2 [25], as well as some intermediate results for the underlying propositional logic and the modal logics K, .2, and S4 mainly regarding rewriting rules, properties for maximal consistent sets of formulas, and frame properties that are induced by the chosen set of axioms in the proof assistant Isabelle/HOL [17]. Our main result is a formalization of the soundness and completeness of Stalnaker’s epistemic logic (restricted to countably many agents) with respect to all weakly directed (also referred to as *confluent* or *convergent* in the literature [22, 23]) S4 frames, this is, all frames consisting of a non-empty set W and a binary relation R_i on W , one for each agent label i , that is reflexive, transitive, and that satisfies the property described by the following condition

$$\forall x \forall y \forall z (xR_i y \wedge xR_i z \implies \exists w yR_i w \wedge zR_i w).$$

The proof uses a Henkin-style completeness method, which is commonly used for these kinds of logics [5] and was already available on Isabelle’s Archive of Formal Proofs [14].

As far as we know, all systems corresponding to some multi-agent epistemic logic already formalized in Isabelle/HOL, which are all contained in [14] (the ground base for our formalization), were complete with respect to a class of frames characterized by a universal formula, i.e., a property of frames given by a first order formula of the form $\forall \bar{x} \phi(\bar{x})$, where $\phi(\bar{x})$ is a quantifier-free formula with variable symbols in $\bar{x} = (x_1, \dots, x_n)$. However, the logic S4.2 is complete with respect to a class of frames that cannot be characterized using a universal formula; instead it is characterized by a universal-existential formula. This universal-existential characterization makes it harder to formalize its completeness result, since one has to show the existence of an object in the universe of the canonical model satisfying a condition on a union of consistent sets of formulas. For this, we followed an argument given by Stalnaker in [26] that includes a set of theorems that are consequences of the axiom (.2) in K, which imply the consistency of a set obtained by taking the union of all known facts for an agent in two different worlds that were accessible from a third one.

Nonetheless, our formalization also includes some intermediate results that are well-known for all normal modal logics, and that are commonly used when dealing with formal proofs in Hilbert-style systems. Finally, we formalized the equivalence between two of the most used axiomatizations of S4, the one presented in [15] which is commonly used when dealing with the relational semantics [5], and the one introduced by McKinsey and Tarski for the topological semantics [1].

Related work

Our ground base is the Isabelle/HOL theory `EpistemicLogic.thy` [14], which contains not only the formalization of other epistemic logics such as S4 and S5, but also formalizes the definition of an abstract canonical model, as well as a simple and convenient way to work with any desired normal modal logic by adding necessary the axioms to the basic system K [15]. A related paper to this formalization is [28], which contains a broad and updated summary on formalizations of logical systems and correspondent important results using different theorem provers. Other ways to formalize logical systems and their completeness results on Isabelle have also been studied in [10] and [6], which include (but are not limited

to) the use of natural deduction rules, sequent-style rules, and tableau rules for the formal systems, and coinductive methods for soundness and completeness results.

However, given the already existent formalization of LTL in Isabelle/HOL [24], as well as the prevalence of Isabelle as a tool for formal verification of safety requirements for critical systems, it becomes important to provide this formalization for this particular proof assistant. In addition to this, in [19] the authors defined and investigated the notion of KB_R -structures, which are used to represent a description of the epistemic status of a rational agent that is not necessarily aware of their ignorance, and provided a result that matches them with models of the epistemic logic S4.2. Modal logics between S4.2 and S5 are of special interest for applications in epistemic logic, since they allow formalizations of several degrees of ignorance for each one of the agents [22].

The paper is organized as follows: Section 2 introduces the necessary background on epistemic logic, including its relational and topological semantics, and how the syntax and the relational semantics were formalized in Isabelle/HOL in [14]. Section 3 explains our formalization of Stalnaker's epistemic logic, including the intermediate results necessary to prove the main results, and the limitations of these to only countably many agents. Section 4 explains our formalization of the equivalence between the two most common axiomatizations for S4, the one that arises from the topological semantics, and the one commonly used when working with the relational semantics. Finally, in Section 5, we conclude with a discussion about the results, limitations, and future work.

2 Background

2.1 Stalnaker's Epistemic logic

We briefly present the axiomatic system developed by R. Stalnaker for both notions of knowledge and belief, as well as the main result for the “knowledge formulas” (i.e., for those formulas that do not contain any belief modal operators), which correspond to the multimodal system S4.2 [25]. We omit the proof for this result, as the Isabelle theory “Epistemic logic: Completeness of Modal Logics” [14] does not support belief formulas.

Consider the well-formed formulas obtained from the following grammar, where x ranges over the set of propositional symbols and i ranges over the set of agent labels:

$$\phi, \psi ::= \perp \mid x \mid \phi \vee \psi \mid \phi \wedge \psi \mid \phi \rightarrow \psi \mid K_i \phi \mid B_i \phi.$$

The operators K_i and B_i mean “agent i knows” and “agent i believes,” respectively. Although Stalnaker does not present his logic of knowledge and belief using this exact set of propositional connectives, but a proper subset of these, we added the remaining ones given that From's formalization includes all of them [15].

Stalnaker's principles (axioms) for knowledge and belief appear in Table 1, along with their interpretations in natural language. *Stalnaker's logic for knowledge and belief* corresponds to the formal system obtained by adding these axioms to the axioms and rules of the multi-modal logic S4, that is, the smallest logic containing the following axioms:

- all propositional tautologies,
- axiom K: $(K_i(\phi \rightarrow \psi) \wedge K_i\phi) \rightarrow K_i\psi$,
- axiom T: $K_i\phi \rightarrow \phi$, and
- axiom 4: $K_i\phi \rightarrow K_iK_i\phi$;

and that is closed under Modus Ponens and the Necessitation rule, “from ϕ infer $K_i\phi$ ”, where i ranges over the set of agents.

Table 1: Axioms for knowledge and belief.

$B_i\phi \rightarrow K_iB_i\phi$	Positive introspection
$\neg B_i\phi \rightarrow K_i\neg B_i\phi$	Negative introspection
$K_i\phi \rightarrow B_i\phi$	Knowledge implies belief
$B_i\phi \rightarrow \neg B_i\neg\phi$	Consistency of belief
$B_i\phi \rightarrow B_iK_i\phi$	Strong belief

The following proposition summarizes some relevant properties of this logic.

Proposition 1. *The following are some key properties of Stalnaker’s logic for knowledge and belief [25].*

1. *The following equivalences, one for each agent label i and formula ϕ , are theorems in this logic:*

$$B_i\phi \longleftrightarrow \neg K_i\neg K_i\phi.$$

2. *As a consequence of the previous property, by replacing ‘ B_i ’ with ‘ $\neg K_i\neg K_i$ ’ in the Consistency of belief axiom, we get that $\neg K_i\neg K_i\phi \rightarrow K_i\neg K_i\neg\phi$ (also known as axiom .2) is a theorem in this logic. This implies that the knowledge formulas of this logic correspond exactly to the logic given by the system S4.2, i.e., those that can be obtained from the rules and axioms of the multi-modal logic S4 in presence of the axiom .2.*

The above proposition allows us to interpret this logic by giving a semantics only for the propositional variables, Boolean connectives and knowledge operators. Formally, we use structures $\mathfrak{M} = (\mathcal{F}, \pi)$ known as Kripke models, where the frame $\mathcal{F} = (W, (R_i)_i)$ is a pair consisting of a non-empty set of worlds W , a set of binary accessibility relations $R_i \subseteq W \times W$, one for each agent i , and $\pi : \text{Var} \rightarrow 2^W$ is a valuation of propositional symbols. Formula satisfiability at a given world $w \in W$ is defined as follows:

$$\begin{aligned} \mathfrak{M}, w &\not\models \perp \\ \mathfrak{M}, w &\models x && \text{iff } w \in \pi(x) \\ \mathfrak{M}, w &\models \phi \vee \psi && \text{iff } \mathfrak{M}, w \models \phi \text{ or } \mathfrak{M}, w \models \psi \\ \mathfrak{M}, w &\models \phi \wedge \psi && \text{iff } \mathfrak{M}, w \models \phi \text{ and } \mathfrak{M}, w \models \psi \\ \mathfrak{M}, w &\models \phi \rightarrow \psi && \text{iff } \mathfrak{M}, w \not\models \phi \text{ or } \mathfrak{M}, w \models \psi \\ \mathfrak{M}, w &\models K_i\phi && \text{iff } \forall v \in W (wR_iv \rightarrow \mathfrak{M}, v \models \phi) \\ \mathfrak{M}, w &\models B_i\phi && \text{iff } \mathfrak{M}, w \models \neg K_i\neg K_i\phi. \end{aligned}$$

One can use functions $\mathcal{K} : W \rightarrow 2^W$ instead of sets of ordered pairs $R \subseteq W \times W$, as there is a correspondence between these objects by setting

$$wRv \iff v \in \mathcal{K}(w),$$

for all $w, v \in W$.

2.2 Epistemic Logic: Completeness of Modal Logics

The “Epistemic Logic: Completeness of Modal Logics” entry on Isabelle’s AFP [14] contains not only a formalization for the completeness results for some epistemic logics, but also a formalization of the

general strategy for Henkin-style proofs for completeness. This is what enabled us to formalize a proof for the completeness result for S4.2. We show here the formalization of the Kripke models from [14], which are structures consisting of a set of worlds of type $'w$, a truth assignment for each propositional variable on each world given by the function denoted π , and a set of accessible worlds from each possible world for each agent $'i$.

datatype $\langle 'i, 'w \rangle$ kripke =

Kripke (\mathcal{W} : $\langle 'w \text{ set} \rangle$) (π : $\langle 'w \Rightarrow id \Rightarrow bool \rangle$) (\mathcal{K} : $\langle 'i \Rightarrow 'w \Rightarrow 'w \text{ set} \rangle$)

Consequently, given a Kripke model $\mathfrak{M} = (W, (\mathcal{K}_i)_{i \in I}, \pi)$ with accessibility functions \mathcal{K}_i for each agent i , formula satisfiability is defined by setting

$$\mathfrak{M}, w \models K_i \phi \quad \text{iff} \quad \forall v \in \mathcal{K}_i(w) (\mathfrak{M}, v \models \phi).$$

Additionally, the *dual* operator for each knowledge operator K_i is denoted in this formalization as L_i and is defined as a short hand for “agent i does not know if something is false.” In other words, $L_i \phi := \neg K_i(\neg \phi)$, for all formulas ϕ . The Kripke semantics for this operator corresponds to [5, 8]

$$\mathfrak{M}, w \models L_i \phi \quad \text{iff} \quad \exists v \in \mathcal{K}_i(w) (\mathfrak{M}, v \models \phi).$$

We show here the corresponding formalization presented in [15] for the Kripke semantics, which is defined inductively on formulas for each world.

primrec semantics :: $\langle 'i, 'w \rangle$ kripke $\Rightarrow 'w \Rightarrow 'i$ fm $\Rightarrow bool$

$(-, - \models - [50, 50] 50)$ **where**

$\langle M, w \models \perp \rangle = \text{False}$

$\langle M, w \models \text{Pro } x \rangle = \pi M w x$

$\langle M, w \models (p \vee q) \rangle = ((M, w \models p) \vee (M, w \models q))$

$\langle M, w \models (p \wedge q) \rangle = ((M, w \models p) \wedge (M, w \models q))$

$\langle M, w \models (p \longrightarrow q) \rangle = ((M, w \models p) \longrightarrow (M, w \models q))$

$\langle M, w \models K i p \rangle = (\forall v \in \mathcal{W} M \cap \mathcal{K} M i w. M, v \models p)$

From's formalization then focuses on proving the soundness and completeness results for each of the most commonly found *normal modal logics* in the literature concerning certain *classes of frames* [5, 8, 15]. We now summarize the relevant ones for our formalization.

1. The basic logic, K, whose corresponding axiomatic system consists of all propositional tautologies and the axiom K, and is closed under Modus Ponens and the Necessitation Rule, is sound and complete with respect to the class of all frames.
2. The logic S4 is sound and complete with respect to the class of all transitive and reflexive frames.

Notice that From's formalization does not include modal operators for belief, this restricts us to the knowledge fragment of the language. However, Proposition 1 tells us that belief is equivalent to knowledge, thus we do not lose any information by restricting to the knowledge fragment.

2.3 Topological semantics and its axioms

The topological semantics for modal logics was introduced before the relational semantics that presently dominate the field [1], and the first semantics completeness proof for S4 was derives from there. Recall the notion of this topological semantics for a language with a single modal operator \Box . Let \mathcal{L} be the language composed of all formulas given by the following grammar:

$$\phi, \psi ::= x \mid \neg \phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \longrightarrow \psi \mid \Box \phi,$$

where x ranges over the set of propositional symbols Var . Formulas in \mathcal{L} are interpreted in a topological model $M = \langle W, \tau, v \rangle$, consisting of a non-empty set W , a topology τ over W , and a valuation $v : \text{Var} \rightarrow 2^W$ in the following way:

- $M, w \models x$ iff $x \in v(x)$;
- $M, w \models \neg\phi$ iff $M, x \not\models \phi$;
- $M, w \models \phi \wedge \psi$ iff $M, x \models \phi$ and $M, x \models \psi$;
- $M, w \models \phi \vee \psi$ iff $M, x \models \phi$ or $M, x \models \psi$;
- $M, w \models \phi \rightarrow \psi$ iff $M, x \not\models \phi$ or $M, x \models \psi$;
- $M, w \models \Box\phi$ iff there exists $U \in \tau$ such that $w \in U$ and $M, y \models \phi$ for all $y \in U$.

Although there is nothing inherently wrong with using the deductive system presented in [15] for the logic S4, the following axiomatization is often preferable when working with the topological semantics, as the meaning of the axioms and rules under this semantics resembles some well-known properties of topological spaces [1].

Table 2: Topological S4 axioms and rules.

Axiom	Formula	Rule	Formula
N	$\Box\top$	MP	$\frac{\phi \rightarrow \psi \quad \phi}{\psi}$
R	$\Box(\phi \wedge \psi) \leftrightarrow (\Box\phi \wedge \Box\psi)$		
T	$\Box\phi \rightarrow \psi$	M	$\frac{\phi \rightarrow \psi}{\Box\phi \rightarrow \Box\psi}$
4	$\Box\phi \rightarrow \Box\Box\phi$		

Notice that at first it is not obvious whether or not the logic obtained from this axiomatization is a normal modal logic, often defined as a logic that *extends* system K [5], as neither axiom K nor the Necessitation Rule are present in the list of axioms and rules. However, we formalized a proof for the equivalence between both axiomatizations in the context of a multi-agent epistemic logic, as in recent years several authors have been developing topological semantics for notions of knowledge and belief [2, 4, 3], where this result is often briefly mentioned and applied, but not proved in detail. Nonetheless, it is also worth noticing here that the relational semantics of S4 is no more than a particular case for the topological semantics, as one can assign a binary relation to each topological space by defining what is known as the *specialization order* [1].

3 Formalization

We now consider the epistemic logic based on the axioms in Table 1 and the results in Proposition 1 for the knowledge fragment of the language. We prove the soundness and completeness of the pure epistemic logic obtained from this system with respect to all frames consisting of weakly directed pre-orders by combining and applying the results formalized in [15] with some auxiliary results provided in the *Utility* section of our Isabelle theory. This allows us to utilize the canonical model strategy to prove completeness of the obtained system. We do not formalize a logic for both knowledge and belief, since we aimed to work on top of the formalization in [14], which considers modalities only for knowledge. Formalizing the whole logic for both knowledge and belief will then require developing a new theory almost from scratch that includes modalities for both notions.

In order to do this, we prove first some intermediate results towards the completeness of the system obtained by adding axiom .2 to the system K, also known as system G in the literature [8], including some results about the underlying propositional logic. This system is known to be complete with respect to the class of weakly directed frames, and, although we do not formalize this result completely, we do formalize a version of the Truth lemma for this system, which is needed so that we can combine it with the results for system S4 formalized in [15] to achieve our goal of formalizing the completeness result for the logic S4.2 with respect to all weakly directed pre-orders.

3.1 Rewriting propositional and modal formulas

In the deductive system formalized in [14], deduction from a set of premises is defined as follows: given a set of formulas $\Gamma \cup \{\phi\}$, we say that “ ϕ is derived from Γ ” (denoted $\Gamma \vdash \phi$) if there are formulas ψ_1, \dots, ψ_k in Γ such that the formula $\psi_1 \rightarrow (\psi_2 \rightarrow \dots (\psi_k \rightarrow \phi))$ is a theorem in the system, where k is a non-negative integer. It is well-known that this formula is logically equivalent to $(\psi_1 \wedge \dots \wedge \psi_k) \rightarrow \phi$ in classical propositional logic, thus the notion can be defined by requiring the latter to be a theorem in the system instead. Being able to translate between these two equivalent formulas in our formal deductive system plays an important role for the proof of our main result, thus we provided a formalization of several results of this kind in the *Utility* section of our Isabelle theory, which includes some results that were not used later but that might become handy for the development of the formalizations of other related theories in the future.

Similarly to the **imply** function in [14], which produces, from a list of formulas $[\psi_1, \dots, \psi_k]$ and a formula ϕ , the formula $\psi_1 \rightarrow (\psi_2 \rightarrow \dots (\psi_k \rightarrow \phi))$, we introduce the function **conjunct**, which takes a list of formulas $[\psi_1, \dots, \psi_k]$ and produces the formula $\psi_1 \wedge \dots \wedge \psi_k \wedge \top$. (Notice that the input may be an empty list, in which case the output is \top .) We formalized some results about logical equivalences, and derived rules and maximal consistent sets regarding the **imply** and **conjunct** functions that are well-known for the logic K, some of which are presented in the following lemmas. These are required to prove in section 3.2 that the axiom .2 induces the weakly directed property on all frames that satisfy it, following [26]. We include the proofs for those lemmas that require elaborated arguments.

Lemma 2 (Derived rules). *For all formulas $\psi_1, \dots, \psi_k, \phi$, it is the case that $\vdash (\psi_1 \wedge \dots \wedge \psi_k) \rightarrow \phi$ if and only if $\vdash \psi_1 \rightarrow (\psi_2 \rightarrow \dots (\psi_k \rightarrow \phi))$.*

Lemma 3 (Logical equivalences). *The following two lemmas capture the fact that in system K, hence in any normal modal logic, the formulas $(K_i \psi_1 \wedge \dots \wedge K_i \psi_k)$ and $K_i(\psi_1 \wedge \dots \wedge \psi_k)$ are equivalent, for any finite set of formulas ψ_1, \dots, ψ_k and any agent i .*

Lemma 4 (Closure under conjunctions for MCSs). *The following lemma proves that maximal consistent sets of formulas are closed under conjunctions, that is, if Γ is a maximal consistent set of formulas and ψ_1, \dots, ψ_k are some formulas in Γ , then $\psi_1 \wedge \dots \wedge \psi_k \in \Gamma$.*

Lemma 5. *For all formulas ϕ, ψ, θ , it is the case that*

$$\vdash ((K_i \phi \wedge K_i \psi) \rightarrow \theta) \rightarrow (K_i(\phi \wedge \psi) \rightarrow \theta)$$

for any agent label i , as long as the type of i is countable.

lemma *K-conj-imply-factor:*

fixes $A :: \langle (i :: \text{countable}) \text{ fm} \Rightarrow \text{bool} \rangle$

shows $\langle A \vdash (((K i p) \wedge (K i q)) \rightarrow r) \rightarrow ((K i (p \wedge q)) \rightarrow r) \rangle$

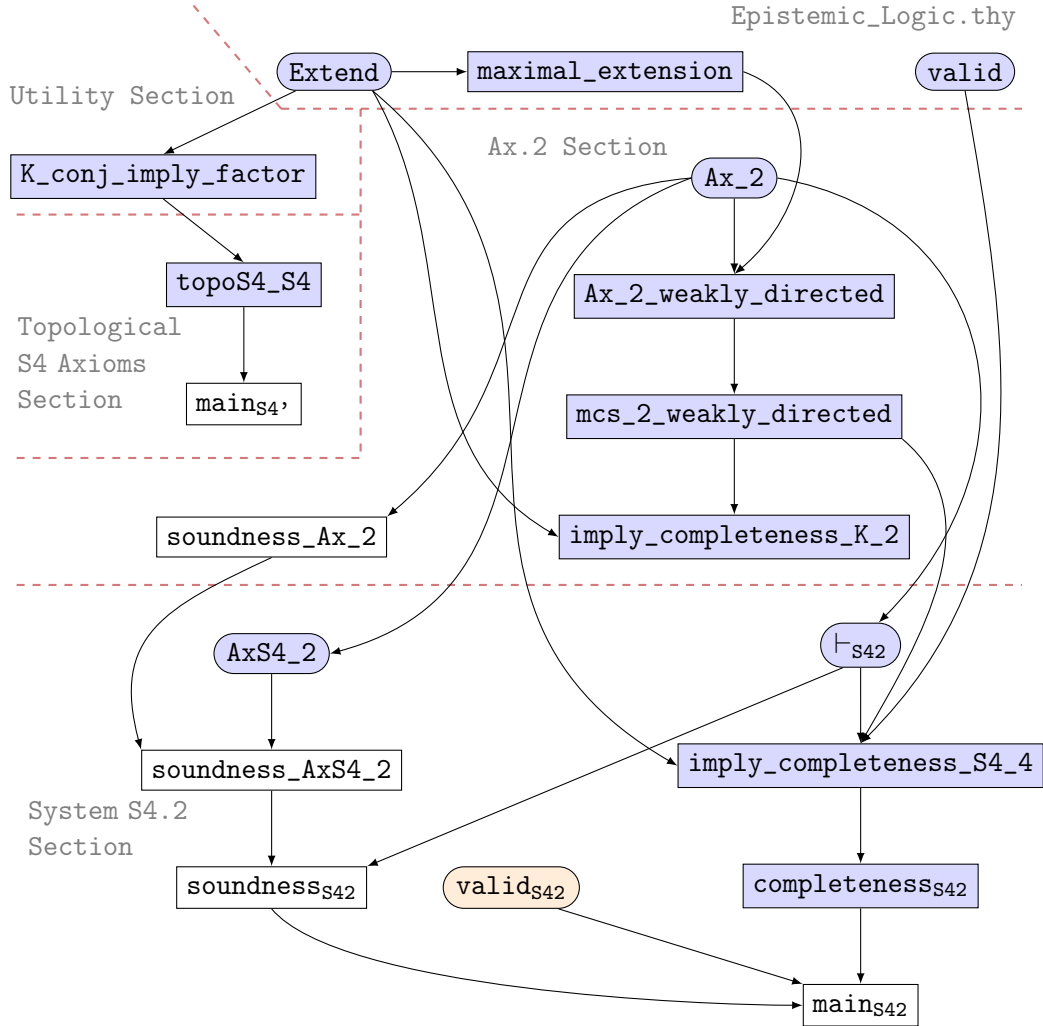


Figure 1: Dependency graph showing the main results and the definitions, abbreviations, and intermediate results from their proofs that require the countable type condition. The dotted lines and the gray text show the files or sections of the Isabelle theory corresponding to our formalization where these can be found. Definitions and abbreviations appear in rounded rectangles, whereas lemmas and theorems appear in rectangles. Those that explicitly mention the countability condition are colored in blue, and the color orange means that this result is applied using the set of natural numbers to label the agents.

The assumption over the set of agent labels for the previous lemma is imposed by the proof that was formalized for it, as it relies on the proof for the completeness of K in [14], which requires this condition, as depicted in Figure 1.

Additionally, we formalize the following lemma, which plays a significant role in the proof of the completeness result for Stalnaker’s epistemic logic that follows [26].

Lemma 6. *Given any pair of formulas ϕ, ψ , $(K_i\phi \wedge L_i\psi) \rightarrow L_i(\phi \wedge \psi)$ is a theorem in system K , for every agent label i .*

Proof. Notice that, for any formulas ϕ and ψ , $\vdash \phi \rightarrow (\neg(\phi \wedge \psi) \rightarrow \neg\psi)$, hence

$$\vdash K_i\phi \rightarrow K_i(\neg(\phi \wedge \psi) \rightarrow \neg\psi).$$

On the other hand, we have that $\vdash K_i(\neg(\phi \wedge \psi) \rightarrow \neg\psi) \rightarrow ((K_i\neg(\phi \wedge \psi)) \rightarrow K_i\neg\psi)$, thus

$$\vdash K_i\phi \rightarrow ((K_i\neg(\phi \wedge \psi)) \rightarrow K_i\neg\psi).$$

This implies that $\vdash K_i\phi \rightarrow (L_i\psi \rightarrow L_i(\phi \wedge \psi))$, which is equivalent to

$$\vdash (K_i\phi \wedge L_i\psi) \rightarrow L_i(\phi \wedge \psi).$$

□

3.2 Axiom .2

We formalize axiom schema .2, which when added to the axioms and rules of system K imposes a structure on the canonical model, namely, we obtain a weakly directed frame. For this, the **inductive** command lets us define the axiom schema in such a way that i and p can be instantiated at will, as long as the type for the agents labels is countable.

inductive *Ax-2* :: $\langle ('i :: \text{countable}) \text{fm} \Rightarrow \text{bool} \rangle$ **where**

$$\langle \text{Ax-2 } (\neg K i (\neg K i p) \longrightarrow K i (\neg K i (\neg p))) \rangle$$

A frame $\mathcal{F} = (W, (R)_{i \in I})$ is said to be *weakly directed* if whenever vR_iw and vR_iu , there exists $x \in W$ such that wR_ix and uR_ix , for each $i \in I$. Accordingly, we formalize this property for Kripke frames as follows:

definition *weakly-directed* :: $\langle ('i, 's) \text{kripke} \Rightarrow \text{bool} \rangle$ **where**

$$\langle \text{weakly-directed } M \equiv \forall i. \forall s \in \mathcal{W} M. \forall t \in \mathcal{W} M. \forall r \in \mathcal{W} M.$$

$$(r \in \mathcal{X} M i s \wedge t \in \mathcal{X} M i s) \longrightarrow (\exists u \in \mathcal{W} M. (u \in \mathcal{X} M i r \wedge u \in \mathcal{X} M i t)) \rangle$$

The soundness of axiom schema .2 with respect to weakly directed frames is formalized in our Isabelle theory, and it follows from the definitions for the semantics and the weakly directed property. However, proving that the property holds for the canonical model when adding the axiom to a normal modal logic is non-trivial. Unlike the frame properties imposed by the axioms considered in the Epistemic Logics formalized in [15], which are all universal properties, this property is universal-existential, so to prove that the canonical model has this property means that one has to show the existence of a possible world satisfying a property under some assumptions.

Recall that the *canonical frame*, $\mathcal{F}^{\text{can}} = (W^{\text{can}}, (R_i^{\text{can}})_{i \in I})$, consists of the set all maximal consistent sets of formulas (with respect to K+.2) as the set of possible worlds, W^{can} , and the accessibility relations R_i^{can} are defined as follows:

$$\Gamma R_i^{\text{can}} \Delta \quad \text{iff} \quad \{\phi : K_i\phi \in \Gamma\} \subseteq \Delta,$$

for each agent i . Thus, showing that the canonical frame for a system including axiom .2 is weakly directed involves verifying that if we have $\{\phi : K_i\phi \in \Gamma\} \subseteq \Delta_1$ and $\{\phi : K_i\phi \in \Gamma\} \subseteq \Delta_2$ for some maximal consistent sets Γ , Δ_1 and Δ_2 , then there exists a maximal consistent set Θ such that $\{\phi : K_i\phi \in \Delta_1\} \cup \{\phi : K_i\phi \in \Delta_2\} \subseteq \Theta$. We capture this in our formalization by the following lemma.

Lemma 7 (Weakly directed property and the axiom .2). *Suppose that V, U, W are three maximal consistent sets with respect to a normal modal logic containing the axiom .2. If $\forall R_i^{\text{can}} U$ and $\forall R_i^{\text{can}} W$, then there exists a maximal consistent set X such that $\forall R_i^{\text{can}} X$ and $\forall R_i^{\text{can}} X$.*

Proof. First, fix a set of formulas A and three maximal consistent sets of formulas V, U, W (with respect to A) satisfying the lemma assumptions for some agent label i of a countable type. Assume towards contradiction that such a set X does not exist, then

$$S := \{\phi : K_i\phi \in W\} \cup \{\phi : K_i\phi \in U\}$$

has to be inconsistent with respect to A , hence there are formulas $\theta_1, \dots, \theta_k \in \{\phi : K_i\phi \in U\}$ and $\psi_1, \dots, \psi_m \in \{\phi : K_i\phi \in W\}$, for some $k, m \in \mathbb{N}$, such that

$$A \vdash (\alpha \wedge \beta) \rightarrow \perp,$$

where $\alpha = \theta_1 \wedge \dots \wedge \theta_k$ and $\beta = \psi_1 \wedge \dots \wedge \psi_m$. This implies that $A \vdash K_i K_i (\neg(\alpha \wedge \beta))$, since $\phi \rightarrow \perp$ is equivalent to $\neg\phi$ for every formula ϕ , by applying the Necessitation rule twice. By definition, we have that $K_i\theta_1, \dots, K_i\theta_k \in U$ and $K_i\psi_1, \dots, K_i\psi_m \in W$, thus

$$K_i\theta_1 \wedge \dots \wedge K_i\theta_k \in U \quad \text{and} \quad K_i\psi_1 \wedge \dots \wedge K_i\psi_m \in W,$$

since these sets are closed under logical consequences. We then use the logical equivalences and properties for maximal consistent sets from the *Utility section* (see section 3.1) to obtain that $K_i\alpha \in U$ and $K_i\beta \in W$. This implies that the formulas $L_i K_i\alpha$ and $L_i K_i\beta$ are elements of V , and so is the formula $K_i L_i\alpha$, since V contains every instance of axiom .2 and is closed under logical consequences. This implies that $(L_i K_i\beta) \wedge (K_i L_i\alpha) \in V$, thus $L_i(K_i\beta \wedge L_i\alpha) \in V$, so there exists a maximal consistent set Z such that

$$VR_i^{\text{can}}Z \quad \text{and} \quad K_i\beta \wedge L_i\alpha \in Z.$$

Applying the lemma *K-thm* we get that $L_i(\beta \wedge \alpha) \in Z$, but notice that $K_i\neg(\alpha \wedge \beta) \in Z$, thus $K_i\neg(\beta \wedge \alpha) \in Z$, which is a contradiction because we have found a formula ϕ such that $\phi, \neg\phi \in Z$. \square

Note that we have restricted ourselves to countable types for the set of agent labels in formalization of the previous two lemmas, as we are only allowed to extend a consistent set into a maximal one when the language is countable, because of a dependency shown in Figure 1. Unlike in the respective result for each normal modal logic formalized in [15], this restriction to a countable type was necessary as we were dealing with a universal-existence property and not with a purely universal one. We then prove a version of the Truth lemma for the minimal normal modal logic that includes axiom .2, which is the relevant result about this system that will allow us to prove the completeness result for system S4.2 in the next section.

Lemma 8 (Imply completeness for Axiom .2). *Let $\Gamma \cup \{\phi\}$ be a set of formulas. Suppose that, for all weakly directed Kripke structures M , $M, w \models \Gamma$ implies $M, w \models \phi$, for each world $w \in M$. Then there are formulas $\gamma_1, \gamma_2, \dots, \gamma_m \in \Gamma$ such that*

$$\vdash_{.2} \gamma_1 \rightarrow (\gamma_2 \rightarrow \dots (\gamma_m \rightarrow \phi) \dots).$$

We omit the proof for this lemma, since it follows the same strategy as the correspondent ones for the systems formalized in [14].

3.3 System S4.2

We define system S4.2 as the one obtained by adding to system K the axioms T, 4 and .2, by making use of the abbreviation \oplus introduced in [14] that allows combining axiom predicates:

abbreviation *SystemS4-2* :: $\langle 'i :: \text{countable} \rangle \text{fm} \Rightarrow \text{bool}$ ($\vdash_{S4.2} - [50] 50$) **where**
 $\langle \vdash_{S4.2} p \equiv AxT \oplus Ax4 \oplus Ax-2 \vdash p \rangle$

Recall that axioms T and 4 impose reflexivity and transitivity on the canonical frame, respectively [5], which was formalized in [14]. This implies that the composition of these two with axiom .2 imposes all three conditions on the canonical frame, which leads to the soundness and completeness of S4.2 with respect to all weakly directed pre-orders. To prove the completeness result, we prove first the analog results to Lemmas 7 and 8 but for S4.2 and Kripke models based on weakly directed preorders.

Lemma 9 (S4.2 and Weakly directed preorders). *Let $\Gamma \cup \{\phi\}$ be a set of formulas. Suppose that, for all countable Kripke structures M based on weakly directed preorders, $M, w \models \Gamma$ implies $M, w \models \phi$, for each world $w \in M$. Then, there are formulas $\gamma_1, \dots, \gamma_m \in \Gamma$ such that*

$$\vdash_{S4.2} \gamma_1 \rightarrow (\dots \rightarrow (\gamma_m \rightarrow \phi) \dots).$$

lemma *imply-completeness-S4-2*:

assumes *valid*: $\forall (M :: ('i :: \text{countable}, 'i \text{ fm set}) \text{kripke}). \forall w \in \mathcal{W} M.$
 $w\text{-directed-preorder } M \longrightarrow (\forall q \in G. M, w \models q) \longrightarrow M, w \models p$
shows $\langle \exists qs. \text{set } qs \subseteq G \wedge (AxS4-2 \vdash \text{imply } qs p) \rangle$

This implies that if a formula is valid in all countable Kripke structures based on weakly directed preorders, then it is a theorem in S4.2.

lemma *completeness_{S4.2}*:

assumes $\forall (M :: ('i :: \text{countable}, 'i \text{ fm set}) \text{kripke}). \forall w \in \mathcal{W} M. w\text{-directed-preorder } M \longrightarrow M, w \models p$
shows $\langle \vdash_{S4.2} p \rangle$

Our main result follows: the completeness of S4.2 with respect to all frames consisting of weakly directed pre-orders.

Theorem 10 (Completeness of S4.2). *A formula is valid in all countable Kripke structures based on weakly directed preorders if and only if it is a theorem in S4.2.*

theorem *main_{S4.2}*: $\langle \text{valid}_{S4.2} p \longleftrightarrow \vdash_{S4.2} p \rangle$

4 An alternative axiomatization for System S4

Inspired by the last section of [14], we formalize an alternative axiomatization for System S4 that is often used when dealing with the *topological semantics* [1] for modal operators and we show its equivalence to the one considered in [15]. We formalize the system corresponding to the axioms and rules in Table 2 in Isabelle, which we call *topoS4*, and, if a formula ϕ is a theorem in this system, we denote this by $\vdash_{Top} \phi$.

inductive *System-topoS4* :: $\langle 'i \text{ fm} \Rightarrow \text{bool} \rangle$ ($\vdash_{Top} - [50] 50$) **where**

$A1'$: $\langle \text{tautology } p \Longrightarrow \vdash_{Top} p \rangle$
 $| AR$: $\langle \vdash_{Top} ((K i (p \wedge q)) \longleftrightarrow ((K i p) \wedge K i q)) \rangle$
 $| AT'$: $\langle \vdash_{Top} (K i p \longrightarrow p) \rangle$
 $| A4'$: $\langle \vdash_{Top} (K i p \longrightarrow K i (K i p)) \rangle$
 $| AN$: $\langle \vdash_{Top} K i \top \rangle$
 $| RI'$: $\langle \vdash_{Top} p \Longrightarrow \vdash_{Top} (p \longrightarrow q) \Longrightarrow \vdash_{Top} q \rangle$
 $| RM$: $\langle \vdash_{Top} (p \longrightarrow q) \Longrightarrow \vdash_{Top} ((K i p) \longrightarrow K i q) \rangle$

To show that this formulation is equivalent to the one in [15] (which is based on [5]), we provide derivations of axiom K and the Necessitation Rule (from ϕ deduct $\Box\phi$). This is enough as our system already includes axioms T and 4 in the same fashion as in [15], and is based on the same propositional logic.

Lemma 11. *For all formulas ϕ and ψ , $\vdash_{top} (K_i\phi \wedge K_i(\phi \rightarrow \psi)) \rightarrow K_i\psi$ and, if $\vdash_{top} \phi$, then $\vdash_{top} K_i\phi$.*

Proof. For the first part, notice that $\vdash_{top} (\phi \wedge (\phi \rightarrow \psi)) \rightarrow \psi$, since it is an instance of a propositional tautology. Then, we apply RM to obtain that $\vdash_{top} K_i(\phi \wedge (\phi \rightarrow \psi)) \rightarrow K_i\psi$, which implies that $\vdash_{top} (K_i\phi \wedge K_i(\phi \rightarrow \psi)) \rightarrow K_i\psi$. For the second one, suppose that $\vdash_{top} \phi$ and notice that $\vdash_{top} \phi \rightarrow (\top \rightarrow \phi)$, hence $\vdash_{top} \top \rightarrow \phi$. Applying RM we get that $\vdash_{top} K_i\top \rightarrow K_i\phi$, thus $\vdash_{top} K_i\phi$. \square

From this it then follows that any formula derivable in the classical S4 system (denoted \vdash_{S4}) can be derived in our system as well.

Lemma 12. *All S4 theorems are theorems in topoS4.*

lemma S4-topoS4: $\langle \vdash_{S4} p \implies \vdash_{top} p \rangle$

The converse follows by a similar argument, we show that axioms and rules from our system are all derivable in \vdash_{S4} , under the condition that there are only countably many agents.

Lemma 13. *All theorems in topoS4 are theorems in S4, assuming that there are only countably many agents.*

lemma topoS4-S4:

fixes $p :: \langle 'i :: \text{countable} \rangle \text{fm}$

shows $\langle \vdash_{top} p \implies \vdash_{S4} p \rangle$

By combining the last two results with the main result for S4 in [15], we obtain formalized soundness and completeness for this alternative axiomatization of S4 over the class of S4 frames, namely, all reflexive and transitive frames.

Theorem 14 (Soundness and Completeness of topoS4). *A formula is valid in all S4 Kripke models if and only if it is a theorem in topoS4.*

theorem main_{S4}': $\langle \text{valid}_{S4} p \longleftrightarrow (\vdash_{top} p) \rangle$

5 Results, Discussion, and Future work

We have formalized the soundness and completeness for Stalnaker's Epistemic Logic S4.2 with respect to the class of Kripke frames consisting of weakly-directed pre-orders for countably many agents, which has not been formalized before neither in Isabelle, nor in any other publicly available proof assistant. Additionally, the equivalence between the topological axiomatization of S4 and the one in [14] is also described in this document. The proofs for the main result, as well as for many of the intermediate results, have been sketched before in multiple sources, but we were not able to find a unique source, making this the first work of its kind. Additionally, given the recent interest in applications of the topological semantics for epistemic modal operators [2, 4, 3], some of which coincide with Stalnaker's epistemic logic, this provides a reinforcement for the foundations of these works.

We emphasize on the assumption of the cardinality of the set of agent labels, as it was necessary to impose such restriction even in some definitions in our formalization, thus creating a discrepancy with the definitions commonly found in the literature. We present in Figure 1 a summary of the definitions and results of our formalization and the one in [14] that rely on this condition, since the formalization

for the general strategy applied to obtain the completeness results in [14] requires it to be able to obtain maximal consistent sets. Although, in theory, it is possible to provide an argument for the general case using Zorn's lemma (this was also later noted in [15]), which is available in [13].

Further work in formalizing in Isabelle/HOL of different formal aspects of modal logics that include S4 operators, as is the case with many temporal logics like LTL with its *always* operator, for which a complete axiomatization is already known [18]; as well as concrete examples of epistemic scenarios based on Stalnaker's principles, like the example detailed in [20]. We hope that this work will facilitate further work in formalizing different logical systems in Isabelle/HOL.

References

- [1] Marco Aiello, Johan van Benthem & Guram Bezhanishvili (2003): *Reasoning About Space: The Modal Way*. *Journal of Logic and Computation* 13(6), pp. 889–920, doi:10.1093/logcom/13.6.889. arXiv:<https://academic.oup.com/logcom/article-pdf/13/6/889/2936128/130889.pdf>.
- [2] Alexandru Baltag, Nick Bezhanishvili & Saúl Fernández González (2022): *Topological Evidence Logics: Multi-agent Setting*. In Aybüke Özgün & Yulia Zinova, editors: *Language, Logic, and Computation*, Springer International Publishing, Cham, pp. 237–257, doi:10.1007/978-3-030-98479-3_12.
- [3] Alexandru Baltag, Nick Bezhanishvili, Aybüke Özgün & Sonja Smets (2013): *The Topology of Belief, Belief Revision and Defeasible Knowledge*. In Davide Grossi, Olivier Roy & Huaxin Huang, editors: *Logic, Rationality, and Interaction*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 27–40, doi:10.1007/978-3-642-40948-6_3.
- [4] Alexandru Baltag, Nick Bezhanishvili, Aybüke Özgün & Sonja Smets (2016): *Justified Belief and the Topology of Evidence*. In Jouko Väänänen, Åsa Hirvonen & Ruy de Queiroz, editors: *Logic, Language, Information, and Computation*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 83–103, doi:10.1007/978-3-662-52921-8_6.
- [5] Robert Blackburn, Maarten de Rijke & Yde Venema (2001): *Modal Logic*. *Modal Logic*, doi:10.1017/CBO9781107050884.
- [6] Jasmin Christian Blanchette, Andrei Popescu & Dmitriy Traytel (2017): *Soundness and Completeness Proofs by Coinductive Methods*. *Journal of Automated Reasoning* 58(1), pp. 149 – 179, doi:10.1007/s10817-016-9391-3. Available at <https://hal.inria.fr/hal-01643157>.
- [7] Marco Bozzano, Alessandro Cimatti, Marco Gario & Stefano Tonetta (2014): *Formal design of fault detection and identification components using temporal epistemic logic*. In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, Springer, pp. 326–340, doi:10.1007/978-3-642-54862-8_22.
- [8] Alexander Chagrov (1997): *Modal Logic*. Oxford logic guides, Clarendon Press, doi:10.1093/oso/9780198537793.001.0001. Available at <https://books.google.com/books?id=dhgi5NF4RtcC>.
- [9] Alessandro Cimatti, Marco Gario & Stefano Tonetta (2016): *A Lazy Approach to Temporal Epistemic Logic Model Checking*. In: *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems*, AAMAS '16, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, p. 1218–1226.
- [10] F Miguel Dionísio, Paula Gouveia & Joao Marcos (2005): *Defining and using deductive systems with Isabelle*. *Computing, Philosophy, and Cognition*, pp. 271–293. Available at <http://temporallogic.org/courses/AppliedFormalMethods/DefiningAndUsingDeductiveSystemsWithIsabelle.pdf>.
- [11] Hans van Ditmarsch, Wiebe van der Hoek & Barteld Kooi (2008): *Dynamic Epistemic Logic*. Springer Netherlands, doi:10.1007/978-1-4020-5839-4.

- [12] Ronald Fagin, Joseph Y. Halpern, Yoram Moses & Moshe Vardi (1995): *Reasoning About Knowledge*. MIT Press, London, England.
- [13] Jacques D. Fleuriot, Tobias Nipkow & Christian Sternagel: *Zorn's Lemma (ported from Larry Paulson's Zorn.thy in ZF)*. Available at <https://isabelle.in.tum.de/dist/library/HOL/HOL/Zorn.html>.
- [14] Asta Halkjær From (2018): *Epistemic Logic: Completeness of Modal Logics*. *Archive of Formal Proofs*. https://isa-afp.org/entries/Epistemic_Logic.html, Formal proof development.
- [15] Asta Halkjær From (2021): *Formalized soundness and completeness of epistemic logic*. In: *International Workshop on Logic, Language, Information, and Computation*, Springer, pp. 1–15, doi:10.1007/978-3-030-88853-4_1.
- [16] Laura P. Gamboa Guzman (2021): *Dynamical operators on models with evidence*. Master's thesis, Universidad de los Andes, Bogota, Colombia. Available at <https://repositorio.uniandes.edu.co/handle/1992/55112>.
- [17] Laura P. Gamboa Guzman (2022): *Stalnaker's Epistemic Logic*. *Archive of Formal Proofs*. https://isa-afp.org/entries/Stalnaker_Logic.html, Formal proof development.
- [18] Robert Goldblatt (1992): *Logics of Time and Computation*. CSLI Publications.
- [19] Costas D. Koutras & Yorgos Zikos (2011): *Relating Truth, Knowledge and Belief in Epistemic States*. In Weiru Liu, editor: *Symbolic and Quantitative Approaches to Reasoning with Uncertainty*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 374–385, doi:10.1007/978-3-642-22152-1_32.
- [20] Costas D. Koutras & Yorgos Zikos (2015): *Relating Truth, Knowledge and Belief in epistemic states*. Online: <http://users.uop.gr/~ckoutras/KZ-KBstructures-Dec2015.pdf>.
- [21] Stephan Merz (2005): *TLA: Lamport's Temporal Logic of Actions*. Online: <https://isabelle.in.tum.de/library/HOL/HOL-TLA/README.html>. Directory in the Isabelle/HOL Library.
- [22] Leonardo Pacheco & Kazuyuki Tanaka (2022): *On the Degrees of Ignorance: via Epistemic Logic and μ -Calculus*. In: *Proceedings of SOCREAL2022 6th International Workshop on Philosophy and Logic of Social Reality*, pp. 74–78. Available at <http://hdl.handle.net/2115/84806>.
- [23] Rasmus Rendsvig & John Symons (2021): *Epistemic Logic*. In Edward N. Zalta, editor: *The Stanford Encyclopedia of Philosophy*, Summer 2021 edition, Metaphysics Research Lab, Stanford University.
- [24] Salomon Sickert (2016): *Linear Temporal Logic*. *Archive of Formal Proofs*. <https://isa-afp.org/entries/LTL.html>, Formal proof development.
- [25] Robert Stalnaker (2006): *On logics of knowledge and belief*. *Philosophical Studies* 128, pp. 169–199, doi:10.1007/S11098-005-4062-Y.
- [26] Robert Stalnaker (2009): *Lecture Notes | Modal Logic | Linguistics and Philosophy | MIT OpenCourseWare*. Available at <https://dspace.mit.edu/bitstream/handle/1721.1/100157/24-244-fall-2009/contents/lecture-notes/index.htm>.
- [27] Stefano Tonetta, Marco Gario, Alessandro Cimatti & Marco Bozzano (2015): *Formal design of asynchronous fault detection and identification components using temporal epistemic logic*. *Logical Methods in Computer Science* 11, doi:10.2168/LMCS-11(4:4)2015.
- [28] Jørgen Villadsen, Asta Halkjær From, Alexander Birch Jensen & Anders Schlichtkrull (2022): *Interactive Theorem Proving for Logic and Information*, pp. 25–48. Springer International Publishing, Cham, doi:10.1007/978-3-030-90138-7_2.