A probabilistic temporal epistemic logic: Strong completeness

ZORAN OGNJANOVIĆ, *Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia, 11000, Belgrade, Serbia.*

ANGELINA ILIĆ STEPIĆ*, *Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia, 11000, Belgrade, Serbia.*

ALEKSANDAR PEROVIĆ, *Faculty of Transport and Traffic Engineering, University of Belgrade, Serbia, 11000, Belgrade, Serbia.*

Abstract

The paper offers a formalization of reasoning about distributed multi-agent systems. The presented propositional probabilistic temporal epistemic logic **PTEL** is developed in full detail: syntax, semantics, soundness and strong completeness theorems. As an example, we prove consistency of the blockchain protocol with respect to the given set of axioms expressed in the formal language of the logic. We explain how to extend **PTEL** to axiomatize the corresponding first-order logic.

1 Introduction

Reasoning about knowledge, time and probability has a long and fruitful history. Starting in early sixties, development of formal systems for studying of these concepts have been a prominent line of research in logic and computer science. The main topics are as follows:

- introduction of syntax and semantics tailored to capture interesting phenomena (e.g., about distributed systems),
- creating of decision procedures and analysis of complexity and
- providing complete axiomatizations.

Curiously enough, neither completeness nor decidability have been studied for the combination of all three.

This paper presents a propositional (**PTEL**) and a first-order (**FOPTEL**) probabilistic temporal epistemic logics. The main and, to the best of our knowledge, novel contributions of these papers are as follows:

- the language of the temporal epistemic logic with non-rigid set of agents from [26] is extended with probabilistic operators and the temporal operators for the past;
- the strong completeness theorem ('every consistent set of formula is satisfiable') is proven for **PTEL**, and it is shown how this approach can be extended to first-order logic; and

*E-mail: angelina@turing.mi.sanu.ac.rs

Vol. 32, No. 1,
Advance Access published 31 October 2022 https://doi.org/10.1093/jigpal/jzac072

- we extend **PTEL** with an appropriate set of axioms that provide sufficient conditions to prove some uncertain features of the blockchain protocol, in particular to show consistency of the protocol, i.e., that with high probability consensus among agents is achieved concerning their ledgers.

The paper [26] analyzes a temporal epistemic logic with a set of agents that may alternately become active and nonactive and gives a strongly complete axiomatization for a class of models that essentially are interpreted systems defined in [9, 22]. Formal systems for reasoning about time and knowledge are generally useful in modeling distributed multiagent systems and [26] illustrates expressiveness of the logic introduced there by describing behavior of the blockchain protocol. Since the language of the logic from [26] contains only temporal and epistemic operators, it cannot express arbitrary probabilistic features of distributed systems protocols. Here, probabilistic operators are included in the language of **PTEL**, so it is possible to formally express that 'the probability of a formula is s', but also that an agent will know that in the next moment. Additionally, the language of **PTEL** extends the formal language from [26] with the temporal past operators Previous and Since.

As the first result about **PTEL** we provide a possible world semantics with nonrigid set of agents and a Hilbert-style axiomatization, and prove its strong completeness with respect to the corresponding class of Kripke-like models with possible worlds. In models there are two kinds of relations among possible worlds that corresponds to the temporal part and to the epistemic part of **PTEL**, respectively. The temporal part of a model consists of a set of runs isomorphic to nonnegative integers, so for temporal reasoning we use LTL, discrete linear time logic, with both past and future temporal operators. Since an agent can be active in some possible worlds and nonactive otherwise, epistemic accessibility relations among possible worlds do not have to be reflexive, i.e., when an agent a is not active in a possible world w, according to a no possible worlds are accessible from w. From the syntactical side, the epistemic operators $\mathtt{K}_a$ representing knowledge of an agent and common knowledge $\mathtt{C}$ are used. Additionally, each possible world is equipped with two kinds of probability functions that measure runs in the model and, according to each agent, sets of possible worlds. This type of models is similar to interpreted systems with probabilities on runs [17].

In such a modal framework, an issue connecting compactness and completeness appears. Namely, if compactness ('a set of formulas is satisfiable iff all its finite subsets are satisfiable') does not hold then no recursive axiomatization can be strongly complete. As we illustrate in Section 3 compactness fails for all three parts of **PTEL** (temporal, epistemic and probabilistic). In absence of compactness any complete finitary axiomatization suffers from the logical problem that syntactic and semantical consequences do not coincide, i.e., there are consistent (w.r.t. the finitary complete axiomatic system) unsatisfiable sets of formulas. So, following [29, 32] we give an axiomatization with some infinitary inference rules for which we prove strong completeness and that avoids the mentioned obstacle. To connect the modal and probabilistic parts of the logic some of the crucial steps are to prove the strong necessitation theorem and to introduce the notion of k-nested implications that addresses combinations of different kinds of operators and is used in formulations of infinitary inference rules. This proof-theoretical approach is applicable for all three parts of **PTEL** and allows their fusion in a comprehensive logical system. Additionally, it ensures that it is straightforward to extend **PTEL** to the first-order logic, which cannot be done using any finitary axiomatization. Infinitary axiomatizations for logics formalizing probabilistic-temporal, temporal-epistemic and probabilistic-epistemic reasoning can be found in [26, 28, 37], respectively. Except [26] these papers do not discuss nonrigid sets of agents, but [37] allows infinitary many agents to be modeled. Finitary axiomatizations for particular parts of **PTEL** are given, for example, in [8] for probabilistic logic, in [11, 23] for LTL, in [9] for epistemic logic with common knowledge operator, in [18] for a temporal-epistemic logic and [7, 22] for a probabilistic-epistemic logic. Note that in each of those logics, due to noncompactness, the above-mentioned discrepancy between syntax and semantics holds. Furthermore, in the first-order framework [38] shows that there is no finite recursive axiomatization for first-order common knowledge logics, and similar results for temporal and probability logics are presented in [36] and [1], respectively. Thus, to achieve completeness for those first-order logics one is forced to use infinitary axiomatizations and we sketch how to axiomatize the corresponding first-order logic **FOPTEL**.

To illustrate the expressiveness of **PTEL** in this paper we describe a set of axioms that formalize some basic properties of the blockchain protocol [27]. Blockchain relies on a set of agents that autonomously, without third authority, synchronize and maintain copies of a distributed append-only ledger, which records transactions (transfers of some units of crypto-currency, smart contracts, etc.). The protocol guarantees immutability, i.e., that transactions cannot be changed after they have been added to the ledger, and also that multiple spendings of a digital asset cannot happen. Being executed in a distributed way, the blockchain protocol is essentially probabilistic. Starting from the set of blockchain axioms we entail consistency of the protocol, i.e., that 'it is common knowledge among agents that with high probability they have a long common prefix of the ledger'. This idea follows the approach from [26]. However, due to absence of probabilistic means in [26] it is not possible to discuss the probabilistic nature of Blockchain, and high probabilities are expressed as knowledge of agents. Some of the papers that are more or less related to our formal logical analysis of the blockchain protocol are [2, 17]. The paper [2] introduces a dynamic logic BCL to describe changes in agents' knowledge that occur when a new block that might be added to the ledger arrives. A model-theoretic approach to analyze probability of achieving consensus among a nonrigid set of agents on a long-enough prefix of the public ledger (called consistency of the protocol) implemented as a blockchain was given in [17]. Some variants of common knowledge (i.e., Δ-, and Δ-$\Box$-common knowledge) that rely on the assumption that agents' local clocks can be synchronized reasonably closely—with a delay of Δ time instants are used in [17]. While it is true that synchronicity is a strong and an unrealistic assumption in distributed framework of the blockchain protocol, we note that [33] states that synchronous protocols can be considered as Δ-delayed protocols as far as crypto-properties are not discussed. Since the aim of this paper is to present and analyze **PTEL** and modeling of Blockchain is an example of expressiveness of the logic, to keep things simple we assume that agents are synchronized as it is done in [12].

The rest of the paper is organized as follows. In Section 2 we describe syntax and semantics of **PTEL**. Section 3 discusses noncompactness of **PTEL**. Section 4 presents its infinitary strongly complete axiomatization and formulates the main statements about the logic. Section 5 provides the basics of the blockchain protocol, a set of proper axioms which describes it and relying on the presented strongly complete axiomatization proves consistency of the protocol. In Section 6 the first-order probabilistic temporal epistemic logic **FOPTEL** is described, its axiomatization and a sketch of strong completeness are given. Section 7 contains concluding remarks and directions for further work. In Appendix a proof of strong completeness of the presented axiomatization for **PTEL** is given.

2 Temporal Epistemic Logic with Probabilities

In this section we give syntax and semantics for **PTEL**. The set of well formed formulas is constructed using temporal, epistemic and probabilistic operators. A semantic structure for the temporal-epistemic part of **PTEL** contains a set of runs, i.e., sequences of possible worlds, where the time flow is isomorphic to nonnegative integers. On the other hand, the epistemic part of a structure is a multiagent Kripke-model with accessibility relations over possible worlds. Finally, in a model of **PTEL** probabilities are added to such structures to measure runs and possible worlds.

2.1 Syntax

Let $\mathbb{N}$ be the set of nonnegative integers, $[0,1]_{\mathbb{Q}}$ the set of all rational numbers from the unit interval and $\mathbb{P}(A)$ powerset set of a set A. We use $\mathbb{A}$ to denote the set of agents $\{a_1,\ldots,a_m\}$, where m is a positive integer. The formal language of **PTEL** consists of a nonempty at most countable set of propositional letters denoted **Var** and the following operators:

- classical: $\neg$, $\wedge$,
- temporal: $\bigcirc$, $\mathtt{U}$, $\bullet$, $\mathtt{S}$,
- epistemic: $\mathtt{K}_a$, $\mathtt{C}$, where $a \in \mathbb{A}$,
- probabilistic: $\mathtt{P}_{\geqslant s}$, $\mathtt{P}_{a,\geqslant s}$, where $a \in \mathbb{A}$, $s \in [0,1]_{\mathbb{Q}}$.

The classical operators $\vee$ and $\rightarrow$ for disjunction and implication are defined as usual: $\alpha \vee \beta =_{def} \neg(\neg\alpha \wedge \neg\beta)$ and $\alpha \rightarrow \beta =_{def} \neg(\alpha \wedge \neg\beta)$, respectively. The set **Var** contains a particular subset $\mathbf{A} = \{A_a | a \in \mathbb{A}\}$, where the intuitive meaning of A_a is that 'agent a is active'. All operators are unary, except $\wedge$, $\mathtt{U}$ and $\mathtt{S}$ that are binary operators. The operators $\bigcirc$, $\mathtt{U}$, $\bullet$ and $\mathtt{S}$ are the future and past temporal operators Next, Until, Previous and Since. The operators $\mathtt{K}_a$ and $\mathtt{C}$ refer to knowledge of an agent a, and to common knowledge, respectively. Finally, $\mathtt{P}_{\geqslant s}\alpha$ and $\mathtt{P}_{a,\geqslant s}\alpha$ are read 'the probability of a set of runs satisfying α is at least s' and 'according to the agent a, the probability of a set of possible worlds satisfying α is at least s'.

Let **For** denotes the set of formulas defined in the usual way. We will use the following:

- the lowercase Latin letters p and q, possibly with indices, to denote propositional variables, and
- the lowercase Greek letters $\alpha, \beta, \gamma, \ldots$ to denote formulas.

The epistemic operator *everybody knows* (denoted $\mathtt{E}$) is introduced as: $\mathtt{E}\alpha =_{def} \bigwedge_{a\in\mathbf{A}} \mathtt{K}_a\alpha$. A theory is a set of formulas $\mathbf{T} \subset \mathbf{For}$.

In this paper we will employ the notion of k-nested implications. Formulas of this form will be used to formulate inference rules in Section 4, and allow that those rules can be applied not only on outermost operators, but also on the operators inside formulas. This form of inference rules is, for example, used to prove the Strong necessitation Theorem 5, which is essential in obtaining strong completeness for **PTEL**.

DEFINITION 1 (k-nested implication).
Let $k \in \mathbb{N}$. Let $\mathbf{B} = (\beta_0,\ldots,\beta_{k-1},\beta_k)$ be a sequence of $k+1$ formulas, $\alpha \in \mathbf{For}$ a formula and $\mathbf{X} = (X_1,\ldots,X_{k-1},X_k)$ a sequence of k operators from $\{\mathtt{K}_a : a \in \mathbb{A}\} \cup \{\bigcirc,\bullet\}$. The *k-nested implication* formula $\Phi_{k,\mathbf{B},\mathbf{X}}(\tau)$ is defined inductively, as follows:

$$\Phi_{k,\mathbf{B},\mathbf{X}}(\alpha) = \begin{cases} \beta_0 \rightarrow \alpha, \ k = 0 \\ \beta_k \rightarrow X_k \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\alpha), \ k \geq 1, \end{cases}$$

where $\mathbf{B}_{j=0}^{k-1} = (\beta_0,\ldots,\beta_{k-1})$ and $\mathbf{X}_{j=1}^{k-1} = (X_1,\ldots,X_{k-1})$.

For example, if $k = 4$, $\mathbf{X} = (\bullet, \mathtt{K}_{a_1}, \bigcirc, \mathtt{K}_{a_3})$, and $a_1, a_3 \in \mathbb{A}$, then

$$\Phi_{k,\mathbf{B},\mathbf{X}}(\alpha) = \beta_4 \to \mathtt{K}_{a_3}(\beta_3 \to \bigcirc(\beta_2 \to \mathtt{K}_{a_1}(\beta_1 \to \bullet(\beta_0 \to \alpha)))).$$

The following abbreviations will be used. For $\bigstar \in \{\bigcirc, \bullet, \mathtt{K}_a, \mathtt{E}\}$, $\mathbf{T} \subset \mathbf{For}$ and $\alpha \in \mathbf{For}$:

- $\bigstar^0\alpha =_{def} \alpha$; $\bigstar^{n+1}\alpha = \bigstar\bigstar^n\alpha, n \geqslant 0$,
- $\bigstar\mathbf{T} =_{def} \{\bigstar\alpha : \alpha \in \mathbf{T}\}$, $\bigstar^{i+1}\mathbf{T} =_{def} \bigstar(\bigstar^i\mathbf{T})$, and
- $\mathbf{T}^{-\bigstar} =_{def} \{\alpha : \bigstar\alpha \in \mathbf{T}\}$, $\mathbf{T}^{-\bigstar^{i+1}} =_{def} (\mathbf{T}^{-\bigstar^i})^{-\bigstar}$,

e.g., $\bigcirc^{n+1}\alpha = \bigcirc\bigcirc^n\alpha$, $\mathtt{K}_a\mathbf{T} =_{def} \{\mathtt{K}_a\alpha : \alpha \in \mathbf{T}\}$, and $\mathbf{T}^{-\bullet} =_{def} \{\alpha : \bullet\alpha \in \mathbf{T}\}$.

The remaining temporal operators eventually, once, always in the future and always in the past are defined as usual: $\mathtt{F}\alpha =_{def} (\alpha \to \alpha)\mathtt{U}\alpha$, $\mathtt{P}\alpha =_{def} (\alpha \to \alpha)\mathtt{S}\alpha$, $\mathtt{G}\alpha =_{def} \neg\mathtt{F}\neg\alpha$ and $\mathtt{H}\alpha =_{def} \neg\mathtt{P}\neg\alpha$, while other probabilistic operators are introduced as $\neg\mathtt{P}_{\geqslant s}\alpha$ by $\mathtt{P}_{<s}\alpha$, $\mathtt{P}_{\geqslant 1-s}\neg\alpha$ by $\mathtt{P}_{\leqslant s}\alpha$, $\neg\mathtt{P}_{\leqslant s}\alpha$ by $\mathtt{P}_{>s}\alpha$, $\mathtt{P}_{\geqslant s}\alpha \wedge \mathtt{P}_{\leqslant s}\alpha$ by $\mathtt{P}_{=s}\alpha$, $\neg\mathtt{P}_{a,\geqslant s}\alpha$ by $\mathtt{P}_{a,<s}\alpha$, $\mathtt{P}_{a,\geqslant 1-s}\neg\alpha$ by $\mathtt{P}_{a,\leqslant s}\alpha$, $\neg\mathtt{P}_{a,\leqslant s}\alpha$ by $\mathtt{P}_{a,>s}\alpha$, and $\mathtt{P}_{a,\geqslant s}\alpha \wedge \mathtt{P}_{a,\leqslant s}\alpha$ by $\mathtt{P}_{a,=s}\alpha$.

2.2 Semantics

Semantics of formulas is given by Kripke-like models with possible worlds that combine temporal, epistemic and probabilistic properties. Intuitively,

- a model consists of a set of runs;
- a run is an infinite sequence of possible worlds which represents a possible execution of a system; and
- to every possible world are associated the set of propositional letters that holds in the world, a set of agents that are active in the world, relations that attach accessible (according to active agents) possible worlds and probabilities that measure sets of possible worlds and runs.

In the formal definition of models we use the notion of algebras (an algebra is a family of subsets of a set that contains that set and is closed under finite unions and complements) and finitely additive probabilities defined on those algebras. The next Section 2.3 discusses definitions that follows:

DEFINITION 2
A model $\mathcal{M}$ is any tuple $\langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ such that

- $\mathbf{R}$ is a non-empty set of runs, where
    - Every *run* r is a function from $\mathbb{N}$ to $\mathbb{P}(\mathbf{Var})$;
    - The pair (r, n), where $r \in \mathbf{R}$ and $n \in \mathbb{N}$, is called a *possible world*; the set of all possible worlds in $\mathcal{M}$ is denoted by $\mathbf{W}$.
- $\mathcal{A}$ is a function from the set of possible worlds $\mathbf{W}$ to $\mathbb{P}(\mathbb{A})$, where
    - $\mathcal{A}((r, n))$ denotes the set of *active agents* associated to the possible world (r, n); and
    - $a \in \mathcal{A}((r, n))$ iff $A_a \in r(n)$.
- $\mathcal{K}$ is the set $\{\mathcal{K}_a : a \in \mathbb{A}\}$ of symmetric and transitive binary *accessibility relations* on $\mathbf{W}$, such that
    - $a \notin \mathcal{A}((r, n))$ iff $(r, n)\mathcal{K}_a(r', n')$ is false for all (r', n');
    - $\mathcal{K}_a(r, n)$ denotes the set of all possible worlds *accessible*, according to the agent a, from (r, n).

- $\mathcal{P}$ is a function defined on $\mathbf{W}$, such that $\mathcal{P}((r,n))$ is a structure $\langle H^{(r,n)}, \mu^{(r,n)}, \{\mathcal{P}_a : a \in \mathbb{A}\}\rangle$, where
  - $H^{(r,n)}$ is an algebra of subsets of $\mathbf{R}$;
  - $\mu^{(r,n)} : H^{(r,n)} \to [0,1]$ is a finitely-additive probability measure on $H^{(r,n)}$;
  - $\{\mathcal{P}_a : a \in \mathbb{A}\}$ is the set of functions defined on $\mathbf{W}$, where $\mathcal{P}_a((r,n))$ is a probability space $\langle \mathbf{W}_a^{(r,n)}, H_a^{(r,n)}, \mu_a^{(r,n)}\rangle$ such that
    - $\mathbf{W}_a^{(r,n)}$ is a non-empty subset of $\mathbf{W}$;
    - $H_a^{(r,n)}$ is an algebra of subsets of $\mathbf{W}_a^{(r,n)}$; and
    - $\mu_a^{(r,n)} : H_a^{(r,n)} \to [0,1]$ is a finitely-additive probability measure.

Using the notion of satisfiability relation we formalize what it means that a formula is satisfied in a possible world. Here an issue appears when we consider probabilistic formulas, e.g., $\mathtt{P}_{a,\geqslant s}\alpha$. Namely, $\mathtt{P}_{a,\geqslant s}\alpha$ should be satisfied in a possible world (r,n) if, according to the agent a, the probability of the set $\mathbf{X} \subset \mathbf{W}_a^{(r,n)}$ of all worlds from $\mathbf{W}_a^{(r,n)}$ in which α holds is at least s. However, it is necessary here that the set $\mathbf{X}$ definable by α is measurable, i.e., that $\mathbf{X} \in H_a^{(r,n)}$, since otherwise $\mu_a^{(r,n)}(\mathbf{X})$ would not be defined. We adopt the approach from [7] where this problem is solved by using the totally defined inner measure $\mu_{\star,a}^{(r,n)}(\mathbf{X}) = \sup\{\mu_a^{(r,n)}(\mathbf{Y}) : \mathbf{Y} \subset \mathbf{X}, \mathbf{Y} \in H_a^{(r,n)}\}$ based on $\mu_a^{(r,n)}$, and then by considering a subclass of models in which sets of worlds definable by formulas are measurable.

DEFINITION 3
Let $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P}\rangle$ be a model. The satisfiability relation $\models$ fulfils:

1. if $p \in \mathbf{Var}$, $(r,n) \models p$ iff $p \in r(n)$,
2. $(r,n) \models \alpha \wedge \beta$ iff $(r,n) \models \alpha$ and $(r,n) \models \beta$,
3. $(r,n) \models \neg\beta$ iff not $(r,n) \models \beta$ (i.e., $(r,n) \not\models \beta$),
4. $(r,n) \models \bigcirc\beta$ iff $(r,n+1) \models \beta$,
5. $(r,n) \models \alpha \mathtt{U} \beta$ iff there is an integer $j \geqslant n$ such that $(r,j) \models \beta$, and for every integer k, such that $n \leqslant k < j$, $(r,k) \models \alpha$,
6. $(r,n) \models \CIRCLE\beta$ iff $n = 0$, or $n \geqslant 1$ and $(r,n-1) \models \beta$,
7. $(r,n) \models \alpha \mathtt{S} \beta$ iff there is an integer $j \in [0,n]$ such that $(r,j) \models \beta$, and for every integer k, such that $j < k \leqslant n$, $(r,k) \models \alpha$,
8. $(r,n) \models \mathtt{K}_a\beta$ iff $(r',n') \models \beta$ for all $(r',n') \in \mathcal{K}_a(r,n)$,
9. $(r,n) \models \mathtt{C}\beta$ iff for every integer $k \geqslant 0$, $(r,n) \models \mathtt{E}^k\beta$,
10. $(r,n) \models \mathtt{P}_{\geqslant s}\beta$ iff $\mu_\star^{(r,n)}(\{r \in \mathbf{R} : (r,0) \models \beta\}) \geqslant s$.
11. $(r,n) \models \mathtt{P}_{a,\geqslant s}\beta$ iff $\mu_{\star,a}^{(r,n)}(\{(r',n') \in \mathbf{W}_a^{(r,n)} : (r',n') \models \beta\}) \geqslant s$.

To simplify the notation, we use the following abbreviations:

- $[\beta]^{(r,n)} = \{r' \in \mathbf{R} \;\; (r',0) \models \beta\}$, and
- $[\beta]_a^{(r,n)} = \{(r',n') \in \mathbf{W}_a^{(r,n)} : (r',n') \models \beta\}$.

Note that by Definition 2, $[\beta]^{(r,n)}$ does not depend on the possible world (r,n). Still, we keep the superscript (r,n) since the corresponding algebra of sets of runs is associated to every possible world.

The next example illustrates the previous definitions.

EXAMPLE 1
Let $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ be a model such that:

- $\mathbf{R} = \{r_1, r_2\}$,
- $\neg q \in r_1(k-1)$, $p, q \in r_1(k)$, and $p, \neg q \in r_1(k+1)$,
- $q \in r_2(k-1)$, $p, q \in r_2(k)$,
- $a \in \mathcal{A}((r_1, k+1))$, $a \in \mathcal{A}((r_2, k))$,
- $\mathcal{K}_a(r_1, k+1) = \{(r_1, k+1), (r_2, k)$, $\mathcal{K}_a(r_2, k) = \{(r_1, k+1), (r_2, k)$,
- $r_1, r_2 \in H^{(r_1,k+1)}$, $\mu^{(r_1,k+1)}(r_1) = \mu^{(r_1,k+1)}(r_2) = \frac{1}{2}$,
- $\mathbf{W}_a^{(r_2,k)} = \{(r_1, k), (r_1, k+1), (r_2, k)\}$,
- $\{(r_1, k), (r_2, k)\}, \{(r_1, k), (r_1, k+1), (r_2, k)\} \in H_a^{(r_2,k)}$, and
- $\mu_a^{(r_2,k)}(\{(r_1, k), (r_1, k+1), (r_2, k)\}) = 1$, and $\mu_a^{(r_2,k)}(\{(r_1, k), (r_2, k)\}) = \frac{2}{3}$.

Then, by Definition 3:

- $(r_1, k+1) \models \mathtt{K}_a p \wedge \mathtt{K}_a \bullet q \wedge \neg \mathtt{K}_a q \wedge \neg q$,
- $(r_2, k) \models \mathtt{K}_a p \wedge \mathtt{K}_a \bullet q \wedge \neg \mathtt{K}_a q \wedge q$,
- $(r_1, 0) \models \bigcirc^k q \wedge \neg \bigcirc^{k+1} q \wedge \bigcirc^k p \wedge \bigcirc^{k+1} p$ and
- $(r_2, 0) \models \bigcirc^k q \wedge \bigcirc^k p$.

Since

- $[\bigcirc^k p]^{(r_1,k+1)} = \{r_1, r_2\}$, $[\bigcirc^k (p \wedge q) \wedge \bigcirc^{k-1} q]^{(r_1,k+1)} = \{r_2\}$ and
- $[p]_a^{(r_2,k)} = \{(r_1, k), (r_1, k+1), (r_2, k)\}$, $[q]_a^{(r_2,k)} = \{(r_1, k), (r_2, k)\}$

we also have that

- $(r_1, k+1) \models \mathtt{P}_{\geqslant 1} \bigcirc^k p$,
- $(r_1, k+1) \models \mathtt{P}_{\leqslant \frac{1}{2}} \bigcirc^k (p \wedge q) \wedge \bigcirc^{k-1} q$,
- $(r_2, k) \models \mathtt{P}_{a, \geqslant 1} p$ and
- $(r_2, k) \models \mathtt{P}_{a, \leqslant \frac{5}{6}} q$.

Note that in Example 1 the sets of runs and possible worlds definable by formulas belong to the corresponding algebras which guarantees that the satisfiability relation is well defined. More formally, to ensure that, we will consider only models satisfying that all sets of the forms $[\beta]^{(r,n)}$ and $[\beta]_a^{(r,n)}$ are measurable:

DEFINITION 4
A model $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ is measurable if

- for all (r, n) and β, $[\beta]^{(r,n)} \in H^{(r,n)}$ and
- for all (r, n), a and β, $[\beta]_a^{(r,n)} \in H_a^{(r,n)}$.

The class of all measurable models is denoted $\mathtt{Mod}$.

DEFINITION 5
A formula α is valid in a model $\mathcal{M} \in \mathtt{Mod}$ (denoted $\mathcal{M} \models \alpha$) if for every possible world (r, n) from $\mathcal{M}$, $(r, n) \models \alpha$. A formula α is valid (denoted $\models \alpha$) if for every model $\mathcal{M} \in \mathtt{Mod}$, $\mathcal{M} \models \alpha$.

A set of formulas $\mathbf{T}$ is satisfied in a possible world (r, n) from a model $\mathcal{M} \in \mathtt{Mod}$ (denoted $(r, n) \models \mathbf{T}$), if for every $\alpha \in \mathbf{T}$, $(r, n) \models \alpha$. A set of formulas $\mathbf{T}$ is satisfiable if there is a possible world (r,n) from a model $\mathcal{M} \in \texttt{Mod}$ such that $(r,n) \models \mathbf{T}$. A formula α is satisfiable if the set $\{\alpha\}$ is satisfiable.

A formula α is a semantical consequence of the set $\mathbf{T}$ of formulas (denoted $\mathbf{T} \models \alpha$) if for every model $\mathcal{M} \in \texttt{Mod}$ and for every possible world (r,n) from $\mathcal{M}$, if $(r,n) \models \mathbf{T}$, then $(r,n) \models \alpha$.

In the above defined notion of semantical consequences, $\mathbf{T} \models \alpha$, formulas from the theory $\mathbf{T}$ correspond to local assumptions described in the context of modal logics [10].

EXAMPLE 2
Let $\mathbf{T} = \{\bigcirc^k\alpha \;\; k \in \mathbb{N}\}$ be satisfied in a possible world (r,n) from a model $\mathcal{M} \in \texttt{Mod}$. It means that $(r,n) \models \bigcirc^k\alpha$ for every k. Then, is follows that $(r,n) \models \texttt{G}\alpha$, which means that $\{\bigcirc^k\alpha \;\; k \in \mathbb{N}\} \models \texttt{G}\alpha$.

2.3 Comments on definitions of models and satisfiability

Let us first comment on Definition 2. The intuition behind runs is that they describe possible executions of a system. Here, $r(n)$ is a truth function on propositional letters associated to the possible world (r,n). Each run r has the starting possible world $(r,0)$ and its time flow is isomorphic to the set $\mathbb{N}$ of non-negative integers. Thus, the past is bounded and it is not symmetric to the future. In Example 3 some consequences of this choice are given. The function $\mathcal{A}$ formalizes the intended property that the set of active agents needs not to be rigid. For every agent $a \in \mathbb{A}$, a particular accessibility relation $\mathcal{K}_a$ in a model is defined. In situations when agents are not active in possible worlds there appear (in the terminology of the modal logics community) 'dead end worlds'. If an agent a is not active in (r,n), $a \notin \mathcal{A}((r,n))$, there is no possible world (including (r,n) itself) accessible from (r,n) by $\mathcal{K}_a$. Note that in that case the agent a knows all formulas, including the false ones, i.e., $(r,n) \models \texttt{K}_a(\alpha \wedge \neg\alpha)$. It is well known that such situations correspond to belief (and not knowledge) of inactive agents. Section 4.3 considers a possible axiomatization of models without dead ends, where agents are active in all possible worlds and each $\mathcal{K}_a$ is an equivalence relation. Here we just note that, if a is active in (r,n), she knows only formulas that are true in (r,n) since reflexivity of $\mathcal{K}_a(r,n)$ follows from symmetry and transitivity and the existence of at least one accessible world. To address this, in Section 4, axioms AKR–AKDE are in the form of implications with antecedents that prevent ascribing 'knowledge to an agent at any world where she is not present' (see [14]). Furthermore, if (according to the agent a) (r',n') is accessible from (r,n), then a is active not only in (r,n), but also in (r',n'), i.e., $a \in \mathcal{A}((r',n'))$, since $\mathcal{K}_a$ is symmetric.

Measurable sets of objects in Mod-models are definable by formulas, and objects can be runs or possible worlds. We distinguish between two different kinds of probabilities:

- local probabilities assessed by agents involved in executions of a system, and
- a global probability assessed by an observer, or a system designer, independent of agents.

Generally, it is possible that agents and observes measure either possible worlds or runs. The choice of measurable sets and who measures those sets is not unique. For example, in [16, 17] probabilities of runs are determined by agents and it is showed how to derive measures of possible worlds from measures of runs. Here, because of the example discussed in Section 5, we are interested in global probabilities of sets of runs having certain properties. Thus, we find it more suitable that sets of runs are measured globally, while sets of possible worlds are measured locally by agents. Consequently, in Definition 2, local probabilities ($\mu_a^{(r,n)}$) are defined on sets of possible worlds, while the global probability ($\mu^{(r,n)}$) measures sets of runs. Similarities in axiomatic descriptions of those probabilities suggest that other choices of probabilities can be analogously formalized. Finally, we note that, when probabilities of runs are discussed, we can consider definable sets of runs of the following forms:

1. $[\alpha]^{(r,n)} = \{r : (r,0) \models \mathtt{G}\alpha\}$, i.e., the set of runs such that α holds in every world of those runs;
2. $[\alpha]^{(r,n)} = \{r : (r,0) \models \mathtt{FG}\alpha\}$, i.e., the set of runs such that in each run α eventually starts to hold forever;
3. $[\alpha]^{(r,n)} = \{r : (r,0) \models \mathtt{F}\alpha\}$, the set of runs such that in each run α holds at least once;
4. $[\alpha]^{(r,n)} = \{r : (r,0) \models \alpha\}$, the set of runs such that in each run α holds in the initial possible world.

While all these possibilities can be used, it seems that the last one is more flexible than the others, in the sense that these first three can be expressed using the last one. For example, if we are interested in runs in which α always (sometime) holds, we can describe them using $[\mathtt{G}\alpha]^{(r,n)}$ and $[\mathtt{F}\alpha]^{(r,n)}$, respectively, in terms of the last possibility. So, we used the last interpretation called anchored in [23]. In [17] measurable sets of runs are determined by the first possibility, i.e., $(r,n) \models P_{\geqslant s}\alpha$ iff $\mu^{(r,n)}(\{r : (r,0) \models \mathtt{G}\alpha\}) \geqslant s$.

Next, consider Definition 3. The previous time operator $\bullet$, is the 'weak previous operator' [23]. One can also use the strong previous operator' $\ominus = \neg\bullet\neg$. Formulas of the form $\ominus\beta$ do not hold in $(r,0)$, for any run r. The next example illustrates some properties of the operator $\bullet$.

EXAMPLE 3

By Definition 3, $(r,0) \models \bullet\alpha$ holds for each formula α. It implies that for $j \in \mathbb{N}$:

- $(r,j) \models \bigwedge_{l=0}^{j} \neg\bullet^{l}(\alpha \wedge \neg\alpha)$;
- $(r,j) \models \bullet^{j+l}(\alpha \wedge \neg\alpha)$, for every integer $l > 0$; and
- $(r,j) \models \mathtt{P}\bullet(\alpha \wedge \neg\alpha)$.

The existence of starting time instants implies that the past and the future are not symmetric. The operator $\bullet$ is not self-dual (while the operator $\bigcirc$ is, i.e., $\models (\neg \bigcirc \neg\alpha) \leftrightarrow \bigcirc\alpha)$ because for every run r, $(r,0) \models \bullet\alpha$, $(r,0) \not\models \neg\bullet\neg\alpha$, and

- $(r,0) \not\models \bullet\alpha \to \neg\bullet\neg\alpha$.

On the other hand, note that the opposite direction is valid: $\models \neg\bullet\neg\alpha \to \bullet\alpha$.

Similarly, while $\models \bigcirc\bullet\alpha \to \bullet\bigcirc\alpha$, the other direction $(\bullet\bigcirc\alpha \to \bigcirc\bullet\alpha)$ is not valid, since it may happen that $(r,0) \not\models \alpha$ and $(r,0) \not\models \bigcirc\bullet\alpha$, while $(r,0) \models \bullet\bigcirc\alpha$ always holds. However, if we are not in a starting possible world (i.e., $(r,i) \models \neg\bullet(\alpha \wedge \neg\alpha)$), then $(r,i) \models \bullet\bigcirc\alpha \to \bigcirc\bullet\alpha$. Finally, the formula $(\bullet\alpha \wedge \bullet\beta) \to \bullet(\alpha \wedge \beta)$ is also valid.

In Definition 3 it is assumed that both the future and the past include the present:

- $(r,n) \models \mathtt{F}\alpha$ iff there is an integer $j \geqslant n$, such that $(r,j) \models \alpha$ and
- $(r,n) \models \mathtt{P}\alpha$ iff there is a nonnegative integer $j \leqslant n$, $(r,j) \models \alpha$,

and the reflexive, strong version of the until operator is considered, i.e., if $\alpha\mathtt{U}\beta$ holds in a time instant, then β must eventually hold (and similarly for $\mathtt{S}$).

Sometimes it is useful to formulate satisfiability of formulas of the form $\mathtt{C}\beta$ in an alternative, but equivalent, way. First, let us say that the possible world (r',k') is reachable from the possible world (r,k) if there is a finite sequence of possible worlds $(r_0,k_0) = (r,k)$, (r_1,k_1), $\dots$, $(r_n,k_n) = (r',k')$ such that for every integer $j \in [0,n-1]$, $(r_j,k_j)\mathcal{K}_{a_j}(r_{j+1},k_{j+1})$ for some $a_j \in \mathbb{A}$. Then,

- $(r,n) \models \mathtt{C}\beta$ iff for every (r',k') reachable from (r,n), $(r',k') \models \beta$.

When definable sets of runs are examined above, we assume that $r' \in [\beta]^{(r,n)}$ if $(r',0) \models \beta$. Alternatively we can use $[\beta]^{(r,n)} = \{r' \in \mathbf{R}\ (r',0) \models \mathtt{G}\beta\}$ or $[\beta]^{(r,n)} = \{r' \in \mathbf{R}\ (r',0) \models \mathtt{F}\beta\}$. While these definitions can be used, it seems that the first one is more flexible than the other two, since it can express the others. For example, if we are interested in runs in which β always (sometime) holds, we can describe them using $[\mathtt{G}\beta]^{(r,n)}$ ($[\mathtt{F}\beta]^{(r,n)}$).

The next example illustrates expressibility of **PTEL** by giving formulas which combines the temporal, epistemic and probabilistic operators.

EXAMPLE 4
The formula

$$\mathtt{P}_{=s}(\mathtt{G}(\bigwedge_{a\in\mathbb{A}} \mathtt{K}_a\mathtt{P}_{b,\geqslant r}\alpha \rightarrow \bigcirc\mathtt{C}\mathtt{P}_{a,\geqslant r}\alpha))$$

can be read as 's is the probability of the set of runs satisfying that always holds for every agent a if a knows that the probability of α given by the agent b is at least r, then in the next time instant it is common knowledge among agents that the probability of α given by a is at least r'.

The well-known knowledge axiom, which states that everything an agent knows is true, can be written as

$$\mathtt{K}_a\alpha \rightarrow \alpha.$$

The formula

$$\mathtt{K}_a \bigcirc \alpha \rightarrow \bigcirc\mathtt{K}_a\alpha$$

means that the agent a does not forget [9].

3 Non-compactness

An important theorem

THEOREM 1 (Compactness).
A set of formulas is satisfiable iff every finite subset of it is satisfiable.

does not hold for **PTEL**. Here are some examples of sets of formulas that violate compactness:

- $\{\bigcirc^k\alpha\ \ k \in \mathbb{N}\} \cup \{\neg\mathtt{G}\alpha\}$;
- $\{\mathtt{E}^k\alpha\ \ k \in \mathbb{N}\} \cup \{\neg\mathtt{C}\alpha\}$;
- $\{\mathtt{P}_{\leqslant 1/k}\alpha\ \ k \in \mathbb{N}\} \cup \{\neg\mathtt{P}_{=0}\alpha\}$, etc.

For example, consider the last set and one of its finite subsets denoted $\mathbf{T}$. Let α be a propositional letter p and k the largest integer such that $\mathtt{P}_{\leqslant 1/k}p \in \mathbf{T}$. It is not hard to see that there is a model $\mathcal{M} \in \mathtt{Mod}$ such that the probability of the set $[p]^{(r,n)}$ is $\frac{1}{k+1} > 0$ so that all formulas from $\mathbf{T}$ are satisfied. On the other hand, there is no real-valued probability such that the measure of the set $[p]^{(r,n)}$ is positive and less than $\frac{1}{k}$, for every $k \in \mathbb{N}$.

Existence of the mentioned sets implies that there is no recursive strongly complete axiomatization of our logic [32]. We will provide an infinitary axiomatization such that infiniteness is present only in meta language which means that

– formulas are finite;
– there are inference rules with countably many premises (and one conclusion); and
– proofs are allowed to be infinite.

Note that any finitary axiomatization for **PTEL** could be only weakly complete. In that case the above unsatisfiable sets would be consistent since finite satisfiability implies consistency w.r.t. any finitary axiomatization. It means that syntactic and semantical consequences do not coincide. To resolve this logical issue, we introduce infinitary inference rules. It is illustrated in Example 5 that the above discussed set of probabilistic formulas is inconsistent w.r.t. our axiomatization, while similar proofs can be given for all sets that violate compactness.

4 Strongly complete axiomatization

The axiomatic system $\mathtt{Ax}_{\mathbf{PTEL}}$ for **PTEL** contains the following axiom schemata and inference rules:

I Propositional axioms and rules

Prop. All instances of classical propositional tautologies

MP. $\dfrac{\alpha, \alpha \to \beta}{\beta}$ (Modus Ponens)

II Axioms and rules for reasoning about time

A$\bigcirc\neg$. $\neg\bigcirc\alpha \leftrightarrow \bigcirc\neg\alpha$

A$\bigcirc\!\to$. $\bigcirc(\alpha \to \beta) \to (\bigcirc\alpha \to \bigcirc\beta)$ (Distribution Axiom for $\bigcirc$)

AU$\bigcirc$. $\alpha \mathtt{U} \beta \leftrightarrow \beta \vee (\alpha \wedge \bigcirc(\alpha \mathtt{U} \beta))$

AUF. $\alpha \mathtt{U} \beta \to \mathtt{F}\beta$

A$\bullet\neg$. $\neg\bullet\neg\alpha \to \bullet\alpha$

A$\bullet\!\to$. $\bullet(\alpha \to \beta) \to (\bullet\alpha \to \bullet\beta)$ (Distribution Axiom for $\bullet$)

A$\bullet\wedge$. $(\bullet\alpha \wedge \bullet\beta) \to \bullet(\alpha \wedge \beta)$

A$\bigcirc\bullet$. $\bigcirc\bullet\alpha \leftrightarrow \alpha$ (Inversion for $\bigcirc$ and $\bullet$)

A$\bigcirc\bullet$C$_1$. $\bigcirc\bullet\alpha \to \bullet\bigcirc\alpha$ (Commutativity for $\bigcirc$ and $\bullet$)

A$\bigcirc\bullet$C$_2$. $\neg\bullet(\gamma \wedge \neg\gamma) \to (\bigcirc\bullet\alpha \leftrightarrow \bullet\bigcirc\alpha)$ (Commutativity for $\bullet$ and $\bigcirc$)

AS$\bullet$. $\alpha \mathtt{S} \beta \leftrightarrow [\beta \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge [\alpha \wedge \bullet(\alpha \mathtt{S} \beta)])]$

AP$\bullet$. $\mathtt{P}\bullet\beta$

R$\bigcirc$N. $\dfrac{\alpha}{\bigcirc\alpha}$ (Necessitation for $\bigcirc$)

R$\bullet$N. $\dfrac{\alpha}{\bullet\alpha}$ (Necessitation for $\bullet$)

RU. $$\frac{\{\Phi_{k,B,X}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \alpha) \wedge \bigcirc^i \beta)) \ : \ i \in \mathbb{N}\}}{\Phi_{k,B,X}(\neg(\alpha \mathtt{U} \beta))}$$

RS. $$\frac{\{\Phi_{k,B,X}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\alpha \wedge \neg\alpha)) \wedge \bullet^i \beta)) \ : \ i \in \mathbb{N}\}}{\Phi_{k,B,X}(\neg(\alpha \mathtt{S} \beta))}$$

III Axioms and rules for reasoning about knowledge

AK→. $\mathtt{K}_a(\alpha \to \beta) \to (\mathtt{K}_a\alpha \to \mathtt{K}_a\beta)$ (Distribution Axiom for $\mathtt{K}_a$)

AKR. $A_a \to (\mathtt{K}_a\alpha \to \alpha)$ (Reflexivity for $\mathtt{K}_a$)

AKA. $A_a \to \mathtt{K}_a A_a$ (Self awareness for $\mathtt{K}_a$)

AKDE. $\neg A_a \to \mathtt{K}_a(\alpha \wedge \neg\alpha)$ (Dead end)

AKS. $\neg\alpha \to \mathtt{K}_a\neg\mathtt{K}_a\alpha$ (Symmetry for $\mathtt{K}_a$)

AKT. $\mathtt{K}_a\alpha \to \mathtt{K}_a\mathtt{K}_a\alpha$ (Transitivity for $\mathtt{K}_a$)

ACE. $\mathtt{C}\alpha \to \mathtt{E}^m\alpha, m \in \mathbb{N}$

RK$_a$N. $\dfrac{\alpha}{\mathtt{K}_a\alpha}$ (Knowledge Necessitation)

RC. $\dfrac{\{\Phi_{k,B,X}(\mathtt{E}^i\alpha) \ : \ i \in \mathbb{N}\}}{\Phi_{k,B,X}(\mathtt{C}\alpha)}$

IV Axioms and rules for reasoning about probability on runs

AGP1. $\mathtt{P}_{\geqslant 0}\alpha$

AGP2. $\mathtt{P}_{\leqslant r}\alpha \to \mathtt{P}_{<t}\alpha, t > r$

AGP3. $\mathtt{P}_{<t}\alpha \to \mathtt{P}_{\leqslant t}\alpha$

AGP4. $(\mathtt{P}_{\geqslant r}\alpha \wedge \mathtt{P}_{\geqslant t}\beta \wedge \mathtt{P}_{\geqslant 1}\neg(\alpha \wedge \beta)) \to \mathtt{P}_{\geqslant \min(1,r+t)}(\alpha \vee \beta)$

AGP5. $(\mathtt{P}_{\leqslant r}\alpha \wedge \mathtt{P}_{<t}\beta) \to \mathtt{P}_{<r+t}(\alpha \vee \beta), r + t \leqslant 1$

AGP●. $\mathtt{P}_{\geqslant 1}\bullet(\alpha \wedge \neg\alpha)$

RGPN. $\dfrac{\alpha}{\mathtt{P}_{\geqslant 1}\alpha}$ (Probabilistic Necessitation)

RGA. $\dfrac{\{\Phi_{k,B,X}(\mathtt{P}_{\geqslant r-\frac{1}{i}}\alpha) \ : \ i \geqslant \frac{1}{r}\}}{\Phi_{k,B,X}(\mathtt{P}_{\geqslant r}\alpha)}, r \in (0, 1]_{\mathbb{Q}}$ (Archimedean rule)

V Axioms and rules for reasoning about probability on possible worlds

AP1. $\mathtt{P}_{a,\geqslant 0}\alpha$

AP2. $\mathtt{P}_{a,\leqslant r}\alpha \to \mathtt{P}_{a,<t}\alpha, t > r$

AP3. $\mathtt{P}_{a,<t}\alpha \to \mathtt{P}_{a,\leqslant t}\alpha$

AP4. $(\mathtt{P}_{a,\geqslant r}\alpha \wedge \mathtt{P}_{a,\geqslant t}\beta \wedge \mathtt{P}_{a,\geqslant 1}\neg(\alpha \wedge \beta)) \to \mathtt{P}_{a,\geqslant \min(1,r+t)}(\alpha \vee \beta)$

AP5. $(\mathtt{P}_{a,\leqslant r}\alpha \wedge \mathtt{P}_{a,<t}\beta) \to \mathtt{P}_{a,<r+t}(\alpha \vee \beta), r + t \leqslant 1$

RPN. $\dfrac{\alpha}{\mathtt{P}_{a,\geqslant 1}\alpha}$ (Probabilistic Necessitation)

RA. $\dfrac{\{\Phi_{k,B,X}(\mathtt{P}_{a,\geqslant r-\frac{1}{i}}\alpha) \mid i \geqslant \frac{1}{r}\}}{\Phi_{k,B,X}(\mathtt{P}_{a,\geqslant r}\alpha)}, r \in (0, 1]_{\mathbb{Q}}$ (Archimedean rule)

Now, we can define the notions of proofs and derivability, theorems and syntactic consequences, (in)consistency, maximal consistent sets and deductively closed sets that are crucial in the completeness proof.

DEFINITION 6

Let λ be a finite or countable ordinal.

A formula α is a *theorem*, denoted by $\vdash \alpha$, if there is an (at most countable) sequence of formulas $\alpha_0, \alpha_1, \ldots, \alpha_{\lambda+1}$ from **For**, such that

– $\alpha_{\lambda+1} = \alpha$; and

– every α_i is an instance of some axiom schema or is obtained from the preceding formulas by an application of an inference rule.

A formula α is *derivable from* a set **T** of formulas ($\mathbf{T} \vdash \alpha$, α is a syntactic consequence of **T**) if there is an (at most countable) sequence of formulas $\alpha_0, \alpha_1, \ \ldots, \alpha_{\lambda+1}$ from **For** such that

– $\alpha_{\lambda+1} = \alpha$; and
– every α_i is an instance of some axiom schema or a formula from the set **T**, or it is obtained from the previous formulas by an application of an inference rule, with the exception that the premises of the inference rules R$\bigcirc$N, R$\bullet$N, RK_aN, RGPN and RPN must be theorems.

The corresponding sequence of formulas is a *proof* for α (from the set **T**).

Note that the length of a proof is an at most countable successor ordinal, and that a formula is a theorem if it is derivable from the empty set.

DEFINITION 7
A set **T** of formulas is *inconsistent* w.r.t. $\mathtt{Ax}_{\mathbf{PTEL}}$ (or simply *inconsistent*) if $\mathbf{T} \vdash \alpha$ for every formula α, otherwise it is $\mathtt{Ax}_{\mathbf{PTEL}}$-*consistent* (or simply *consistent*). A set **T** of formulas is $\mathtt{Ax}_{\mathbf{PTEL}}$-*maximal consistent* (or simply *maximal consistent*) if it is consistent, and each proper superset of T is inconsistent.

A set of formulas **T** is *deductively closed* (w.r.t. $\mathtt{Ax}_{\mathbf{PTEL}}$) if it contains all formulas derivable from **T**, i.e., $\alpha \in \mathbf{T}$ whenever $\mathbf{T} \vdash \alpha$.

4.1 Comments on $\mathtt{Ax}_{\mathbf{PTEL}}$

It is not uncommon in infinitary logics that a proof from a theory **T** is defined as any sequence of formulas $\langle \alpha_i \;\; i < \lambda \rangle$ (here λ is an ordinal) such that for each i, α_i is either an axiom, or $\alpha_i \in \mathbf{T}$, or it can be derived by certain derivation rule applied on some previous members of the sequence. As a consequence, it is possible that a proofs does not have the endpoint (the case when λ is a limit ordinal). For example, one such sequence is given by

$$\langle P_{\geq 10^{-n}} p \vee P_{\leq 10^{-n}} p \;\; n \in \omega \rangle.$$

However, $T \vdash \alpha$ always means that there is a proof $\langle \alpha_i \;\; i < \lambda \rangle$ from **T** ending with α, which means that λ is a successor ordinal. Hence, we have restricted the ordered type of proofs to such ordinals (the proofs whose ordered type is a limit ordinal are redundant, at least with respect to the study of the consequence relation $\vdash$).

Another natural question that may arise is why are the lengths of proofs limited to countable ordinals, i.e., why we do not allow for λ to be any successor ordinal. Again, the reason is that such proofs are redundant. Namely, they can be reduced to countable proofs. This can be shown by transfinite induction on the length of inference as follows.

Suppose that λ is any ordinal, **T** is a theory, $\langle \alpha_i \;\; i \leq \lambda \rangle$ is a proof from **T**, and that, for all $i < \lambda$, α_i has a countable proof from **T**. There are the following cases:

– α_λ is an axiom, or $\alpha_\lambda \in \mathbf{T}$. Then the required proof is a single formula sequence $\langle \alpha_\lambda \rangle$;
– α_λ is derived from α_i and $\alpha_i \to \alpha_\lambda$ by application of MP. By induction hypothesis, there are successor ordinals $\lambda_1, \lambda_2 < \omega_1$ and proofs $\langle \beta_i \; i \leq \lambda_1 \rangle$ and $\langle \gamma_i \; i \leq \lambda_2 \rangle$ form **T** so that $\beta_{\lambda_1} = \alpha_i$ and $\gamma_{\lambda_2} = \alpha_i \to \alpha_\lambda$. Now the concatenation of the sequences

$$\langle \beta_i \;\; i \leq \lambda_1 \rangle + \langle \gamma_i \;\; i \leq \lambda_2 \rangle + \langle \alpha_\lambda \rangle$$

is a proof of α_λ from $\mathbf{T}$ whose ordered type is $\lambda_1 + \lambda_2 + 1 < \omega_1$, i.e. we have obtained a countable proof for α_λ. The cases for the necessitation rules (R◯N, R●N, R$\mathtt{K}_a$N, RGPN, RPN) follow in the same way;

– α_λ is obtained by an application of some infinitary inference rule on the set of premises $\{\alpha_{i,n} \; n < \omega\}$. By induction hypothesis, there are countable successor ordinals λ_n, $n < \omega$ and proofs $\langle \beta_{n,j} \; j \leq \lambda_n \rangle$ from $\mathbf{T}$ so that, for each n, $\beta_{n,\lambda_n} = \alpha_{i,n}$. Now the concatenation of the sequences

$$\bigoplus_{n<\omega} \langle \beta_{n,j} \; j \leq \lambda_n \rangle + \langle \alpha_\lambda \rangle$$

is a proof of α_λ from $\mathbf{T}$ whose order type is $\sum_{n<\omega} \lambda_n + 1 < \omega_1$, i.e. we have obtained a countable proof for α_λ.

Axiom schemas and rules A◯¬–A$\mathtt{UF}$, R◯N, and A$\mathtt{K}\rightarrow$, A$\mathtt{K}$S, A$\mathtt{K}$T, AC$\mathtt{E}$ and R$\mathtt{K}_a$N are used in standard finitary axiomatizations [9, 11, 20, 23] for reasoning about the temporal future operators in linear discrete time, and about knowledge, respectively. The axioms A$\mathtt{K}\rightarrow$, A$\mathtt{K}$R (without the antecedent), A$\mathtt{K}$S and A$\mathtt{K}$T are known as the modal axioms K,T,B and 4, respectively. In the framework of epistemic logic A$\mathtt{K}$R (without the antecedent) and A$\mathtt{K}$T are also referred to as the axioms of knowledge and positive introspection. It is well known that A$\mathtt{K}\rightarrow$, A$\mathtt{K}$R (without the antecedent), A$\mathtt{K}$S and A$\mathtt{K}$T implies so-called axiom of negative introspection $\neg\mathtt{K}_a\alpha \rightarrow \mathtt{K}_a\neg\mathtt{K}_a\alpha$. Axiom schemas and rules A●¬–A$\mathtt{P}$● and R●N are related to the temporal past operators, while A$\mathtt{K}$R–A$\mathtt{K}$DE are introduced to deal with knowledge of (non)active agents.

The axioms and rules from the groups IV and V are similar, which is not surprising since they formalize reasoning about probabilities. They are versions of the strongly complete axiomatization for the class of measurable models with real valued probability functions [32]. We need both groups since the language of our logic contains probabilistic operators for probabilities defined on runs and on possible worlds. The only exception is Axiom AGP● in the group IV without a counterpart in the group V. This axiom guarantees that the probability of the set of all runs is 1. Note that the set of runs beginning with possible worlds in which ●$(\alpha \wedge \neg\alpha)$ holds and the set of all runs coincide.

The rules R$\mathtt{U}$, R$\mathtt{S}$, RC, RGA and RA are infinitary, i.e., each of them has a countable set of assumptions and one conclusion. An equivalent form of Rule RGA is [[Insert image06]] A similar form can be given for Rule RA. The infinitary rules guarantee that sets from Section 3 that violate compactness are inconsistent. The next example illustrates this property for the set with probabilistic formulas.

Example 5

Let $\mathbf{T} = \{\mathtt{P}_{\leqslant 1/k}\alpha \;:\; k \in \mathbb{N}\} \cup \{\neg\mathtt{P}_{=0}\alpha\}$. Then,

$\mathbf{T} \vdash \neg\mathtt{P}_{=0}\alpha$, since $\neg\mathtt{P}_{=0}\alpha \in \mathbf{T}$
$\mathbf{T} \vdash \mathtt{P}_{\leqslant 1/k}\alpha$, since $\mathtt{P}_{\leqslant 1/k}\alpha \in \mathbf{T}$, for every $k \in \mathbb{N}$
$\mathbf{T} \vdash \mathtt{P}_{\leqslant 0}\alpha$, by Rule RGA$'$
$\mathbf{T} \vdash \mathtt{P}_{=0}\alpha$, by Axiom AGP1 and definition of $\mathtt{P}_{=0}$
$\mathbf{T} \vdash \bot$.

Note that, if $k = 0$ the infinitary inference rules are reduced to much simpler forms. For example, the rule RA becomes:

$$\text{RA.} \qquad \frac{\{\beta_0 \to \mathrm{P}_{a,\geqslant r-\frac{1}{i}}\alpha \;:\; i \geqslant \frac{1}{r}\}}{\beta_0 \to \mathrm{P}_{a,\geqslant r}\alpha}, r \in (0,1]_{\mathbb{Q}}$$

Using the mentioned abbreviations for the probabilistic operators, the following versions of the above axioms can be obtained:

AGP1′. $\mathrm{P}_{\leqslant 1}\alpha$
AGP2′. $\mathrm{P}_{\geqslant t}\alpha \to \mathrm{P}_{>r}\alpha,\ t > r$
AGP3′. $\mathrm{P}_{>t}\alpha \to \mathrm{P}_{\geqslant t}\alpha$
AP1′. $\mathrm{P}_{a,\leqslant 1}\alpha$
AP2′. $\mathrm{P}_{a,\geqslant t}\alpha \to \mathrm{P}_{a,>r}\alpha,\ t > r$
AP3′. $\mathrm{P}_{a,>t}\alpha \to \mathrm{P}_{a,\geqslant t}\alpha$

and used where it is appropriate.

Finally, we should mention that in the proofs given below we will often use induction on the structure of a formulas, where the structure is expressed using the rank function $\mathsf{rk}(\cdot)$ [3] which assigns ordinal ranks to formulas, e.g., $\mathsf{rk}(\mathrm{C}\gamma) := \omega + \mathsf{rk}(\gamma)$, and satisfies that

1. $\mathsf{rk}(\gamma_1) < \mathsf{rk}(\gamma)$ if γ_1 is a proper subformula of γ; and
2. $\mathsf{rk}(\mathrm{E}^i\gamma) < \mathsf{rk}(\mathrm{C}\gamma)$ for every $i \in \mathbb{N}$.

4.2 Strong completeness of $\mathtt{Ax}_{\mathbf{PTEL}}$

In this Section we state the main theorems related to soundness and strong completeness of the axiomatic system $\mathtt{Ax}_{\mathbf{PTEL}}$. Their proofs and auxiliary statements are given in Appendix A. The main idea in proving strong completeness is to follow the steps of Henkin's procedure [19] adapted for our non-compact modal framework with infinitary inference rules. The procedure consists of the following main steps:

- We first prove a Deduction Theorem 4, and some auxiliary statements, where of particular importance is the Strong necessitation Theorem 5.
- Next, using Lindenbaum's Theorem 6 we show how to extend a consistent set **T** of formulas to a maximal consistent set.
- Then, we use maximal consistent sets of formulas to define the canonical model and prove that it is a Mod-model.
- Finally, we prove that a formula is satisfied in a possible world of the canonical model iff it belongs to the maximal consistent set of formulas which corresponds to the considered possible world.

THEOREM 2 (Soundness for $\mathtt{Ax}_{\mathbf{PTEL}}$).
$\vdash \beta$ implies $\models \beta$.

THEOREM 3 (Soundness for $\mathtt{Ax}_{\mathbf{PTEL}}$).
$\vdash \beta$ implies $\models \beta$.

THEOREM 4 (Deduction theorem).
If $\mathbf{T} \subset \mathbf{For}$, then

$$\mathbf{T}, \{\alpha\} \vdash \beta \text{ iff } \mathbf{T} \vdash \alpha \rightarrow \beta.$$

THEOREM 5 (Strong necessitation).
If $\mathbf{T} \subset \mathbf{For}$ and $\mathbf{T} \vdash \gamma$, then

1. $\bigcirc\mathbf{T} \vdash \bigcirc\gamma$;
2. $\CIRCLE\mathbf{T} \vdash \CIRCLE\gamma$; and
3. $\mathtt{K}_a\mathbf{T} \vdash \mathtt{K}_a\gamma$, for every $a \in \mathbf{A}$.

THEOREM 6 (Lindenbaum's theorem).
Every $\mathtt{Ax}_{\mathbf{PTEL}}$-consistent set of formulas $\mathbf{T}$ can be extended to a maximal $\mathtt{Ax}_{\mathbf{PTEL}}$-consistent set $\mathbf{T}^*$.

Now, we define the notion of canonical model. First note that the set $\mathbf{X}_0 = \{\CIRCLE(\alpha \wedge \neg\alpha) : \alpha \in \mathbf{For}\}$ is consistent. Indeed, by Lemma 6.12 each maximal consistent set $\mathbf{T}$ contains $\{\CIRCLE^i(\alpha \wedge \neg\alpha) : \alpha \in \mathbf{For}\}$ for some positive i. If $i = 1$, it means that $\mathbf{X}_0$ is consistent as a subset of a consistent set. If $i > i$, then by Lemma 6.13, $\mathbf{T}^{-\CIRCLE}$ is maximal consistent. By the same argument, it follows that the set $\mathbf{X}_0$ is consistent.

Possible worlds of the canonical model correspond to maximal consistent sets of formulas, while we define sequences of maximal consistent sets and the corresponding runs as follows:

- Let the set $\mathbf{Mcs}$ contain all maximal consistent extensions of the set $\mathbf{X}_0$. Elements of $\mathbf{Mcs}$ correspond to starting possible worlds of runs in the canonical model. Theorem 6 guarantees that $\mathbf{Mcs}$ is nonempty. Note also that Lemma 5.7 shows that for every $\alpha \in \mathbf{For}$, and every $\mathbf{S} \in \mathbf{Mcs}$, $\CIRCLE\alpha \in \mathbf{S}$.
- For an arbitrary $\mathbf{S} \in \mathbf{Mcs}$, we define the sequence of maximal consistent sets and the corresponding run $r^{\mathbf{S}}$ in the following way:
  - $\mathbf{S}_0 = \mathbf{S}$;
  - for $i \in \mathbb{N}$, $\mathbf{S}_{i+1} = \mathbf{S}_i^{-\bigcirc}$. Every $\mathbf{S}_{i+1}$ is maximal consistent (see Lemma 6.14);
  - for $i \in \mathbb{N}$ and every propositional letter $p \in \mathbf{Var}$, $p \in r^{\mathbf{S}}(i)$ iff $p \in \mathbf{S}_i$.

Let $\mathbf{R}^*$ contain all such runs and $\mathbf{W}^*$ be the set of all possible worlds. Then we define

- $\mathcal{A}^* : \mathbf{W}^* \rightarrow \mathbb{P}(\mathbb{A})$ such that for every agent $a \in \mathbb{A}$:
  - $a \in \mathcal{A}^*((r^{\mathbf{S}}, n))$ iff $A_a \in \mathbf{S}_n$.
- $\mathcal{K}^*$, the set of accessibility relations on possible worlds such that for every agent $a \in \mathbb{A}$:
  - If $a \notin \mathcal{A}^*((r^{\mathbf{S}}, n))$, then $(r^{\mathbf{S}}, n)\mathcal{K}_a^*(r', n')$ is false for all (r', n'); otherwise
  - $(r^{\mathbf{S}}, n)\mathcal{K}_a^*(r^{\mathbf{S'}}, n')$ iff $\mathbf{S}_n^{-\mathtt{K}_a} = \{\alpha : \mathtt{K}_a\alpha \in \mathbf{S}_n\} \subset \mathbf{S'}_{n'}$.
- $\mathcal{P}^*$ is a function on the set $\mathbf{W}^*$ such that $\mathcal{P}^*((r^{\mathbf{S}}, n)) = \langle H^{*,(r^{\mathbf{S}},n)}, \mu^{*,(r^{\mathbf{S}},n)}, \{\mathcal{P}_a^* : a \in \mathbb{A}\}\rangle$ and
  - for every $\alpha \in \mathbf{For}$, $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} = \{r^{\mathbf{S'}} \in \mathbf{R}^* : \alpha \in \mathbf{S'}_0\}$;
  - $H^{*,(r^{\mathbf{S}},n)}$ is a family of sets $\{[\![\alpha]\!]^{(r^{\mathbf{S}},n)} : \alpha \in \mathbf{For}\}$;
  - $\mu^{*,(r^{\mathbf{S}},n)} : H^{*,(r^{\mathbf{S}},n)} \rightarrow [0,1]$ such that $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) = \sup\{t \in [0,1]_{\mathbb{Q}} : P_{\geqslant t}\alpha \in \mathbf{S}_n\}$; and

– for every agent $a \in \mathbb{A}$, $\mathcal{P}^*_a$ is a function on possible worlds $(r^{\mathbf{S}}, n) \in \mathbf{W}^*$ defined as $\mathcal{P}^*_a((r^{\mathbf{S}}, n)) = \langle \mathbf{W}^*_a(r^{\mathbf{S}}, n), H^*_a(r^{\mathbf{S}}, n), \mu^*_a(r^{\mathbf{S}}, n)\rangle$, where:
  * $\mathbf{W}^{*,(r^{\mathbf{S}},n)}_a = \mathbf{W}^*$;
  * for every $\alpha \in \mathbf{For}$, $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}_a = \{(r^{\mathbf{S'}}, n') \in \mathbf{W}^{*,(r^{\mathbf{S}},n)}_a : \alpha \in \mathbf{S'}_{n'}\}$;
  * $H^{*,(r^{\mathbf{S}},n)}_a$ is a family of sets $\{[\![\alpha]\!]^{(r^{\mathbf{S}},n)}_a : \alpha \in \mathbf{For}\}$; and
  * $\mu^{*,(r^{\mathbf{S}},n)}_a : H_a(r^{\mathbf{S}}, n) \to [0,1]$ such that $\mu^{*,(r^{\mathbf{S}},n)}_a([\![\alpha]\!]^{(r^{\mathbf{S}},n)}_a) = \sup\{t \in [0,1]_{\mathbb{Q}} : P_{a,\geqslant t}\alpha \in \mathbf{S}_n\}$.

DEFINITION 8
Let $\mathbf{R}^*$, $\mathcal{A}^*$, $\mathcal{K}^*$ and $\mathcal{P}^*$ be defined as above. The canonical model is the tuple $\mathcal{M}^* = \langle \mathbf{R}^*, \mathcal{A}^*, \mathcal{K}^*, \mathcal{P}^*\rangle$.

Note that Definition 8 of the canonical model $\mathcal{M}^*$ relies on sets of the forms $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}$ and $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}_a$, while in Definition 2 sets of the forms $[\alpha]^{(r,n)}$ and $[\alpha]^{(r,n)}_a$ are used. Recall that $[\alpha]^{(r,n)}$ and $[\alpha]^{(r,n)}_a$ are defined using the satisfiability relation, which is not the case for $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}$ and $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}_a$. So, we have to prove:

THEOREM 7
The canonical model $\mathcal{M}^*$ is a Mod-model.

For any $\texttt{Ax}_{\mathbf{PTEL}}$-consistent set of formulas $\mathbf{T}$ and its maximal consistent extension $\mathbf{T}^*$ Lemma 6.15 guarantees that there is a sequence of maximal consistent sets $\mathbf{S}_0$, $\mathbf{S}_1$, …, such that for some k, $\mathbf{S}_k = \mathbf{T}^*$. Finally, the following follows:

THEOREM 8 (Strong completeness for $\texttt{Ax}_{\mathbf{PTEL}}$).
A set $\mathbf{T}$ of formulas is $\texttt{Ax}_{\mathbf{PTEL}}$-consistent iff it is satisfiable.

4.3 *Characterization of some other classes of models*

In this section we discuss how different aspects of the proposed semantics can be adapted for some specific situations that can appear when one analysis multi-agent systems.

Let us start by considering a distinction between knowledge and belief. It is noted in [26] that the class Mod of models (defined there without the probabilistic part) characterizes a weaker form of knowledge–belief (where an agent might belief in false statements) and that to reason about knowledge of agents we should consider another class of models in which everything that agents know is true:

DEFINITION 9
The class $\texttt{Mod}_r$ of models contains all Mod-models which satisfies that the set of active agents is rigid and that all $\texttt{K}_a$ are equivalence relations, i.e., that for every possible world (r, n):

- $\mathcal{A}((r, n)) = \mathbb{A}$; and
- $\mathcal{K}_a(r, n)$ is a reflexive, transitive and symmetric accessibility relations.

It is well known that in models from the class $\texttt{Mod}_r$ everything that agents know is true. Note that the same holds in Mod-models for active agents. Also, note that for Mod-models the following holds: if $(r,n) \models A_a$ and $(r,n)\mathcal{K}_a(r',n')$, then $(r',n') \models A_a$. Otherwise, if $(r',n') \not\models A_a$, then it is not $(r',n')\mathcal{K}_a(r,n)$, which contradicts our assumption about symmetry of $\mathcal{K}_a$.

If the set of agents is rigid, to axiomatize the class $\mathtt{Mod}_r$ we should include an additional, so-called Knowledge axiom:

$$A\mathtt{K}2. \qquad \mathtt{K}_a\alpha \to \alpha$$

which implies reflexivity of the accessibility relations $\mathtt{K}_a$.

The above presented semantics is in some sense general, i.e., it does not address interactions of temporal, probabilistic, and epistemic parts, so there are no axioms with mixed temporal, probabilistic and/or epistemic operators that restrict the considered class of models. Such axioms can be introduced in various ways. For example, the paper [28] specifies an additional relationship between temporal and probabilistic features by adding an axiom (the notation is adjusted for this paper) $\neg\alpha \to (\mathtt{P}_{a,\geqslant s}\alpha \to \bigcirc\mathtt{P}_{a,\geqslant s}\alpha)$, which characterizes models with the property that if α does not hold in a time instant, then in the next time instant its probability will not decrease.

A set of conditions (consistency, objectivity, state determined property and uniformity) that relate knowledge and probability are introduced in [7]. It is explained in [37] how those conditions can be axiomatized using the language which is similar to the one used in this paper. For example, having in mind that in **PTEL** agents are allowed to be inactive, the consistency condition CONS requires that an active agent can assign probabilities only to subsets of accessible worlds, i.e., that $\mathbf{W}_a^{(r,n)} \subset \mathcal{K}_a(r,n)$ holds for every a active in (r,n). Then, the axiom $A_a \wedge (\mathtt{K}_a\alpha \to \mathtt{P}_{a,\geqslant 1}\alpha)$ is the syntactic counterpart of CONS.

EXAMPLE 6
Let us consider the following formulas:

- $\alpha = \mathtt{K}_a\neg p \wedge \mathtt{P}_{a,\geqslant 1}p$; and
- $\beta = \mathtt{C}(p \wedge \bigwedge_{a\in\mathbb{A}} \mathtt{P}_{a,=0}p)$.

They are $\mathtt{Mod}$-satisfiable, which might not follow intuition about interaction of knowledge and probability. This issue can be addressed by extending $\mathtt{Ax}_{\mathbf{PTEL}}$ with the CONS-axiom $A_a \wedge (\mathtt{K}_a\gamma \to \mathtt{P}_{a,\geqslant 1}\gamma)$. The formulas α and β can be satisfied only in possible worlds in which agents are inactive or $\mathbf{W}_a^{(r,n)} \not\subset \mathcal{K}_a(r,n)$. Since the CONS-axiom makes all agents active and provides that $\mathbf{W}_a^{(r,n)} \subset \mathcal{K}_a(r,n)$, α and β become contradictions.

Furthermore, examples of interactions between knowledge and time considered in [9] include synchronous systems, systems with perfect recall, etc. Strongly complete axiomatizations for the corresponding classes of models can be obtained following the ideas presented there.

In synchronous systems it is assumed that agents have access to a global clock, so that in a possible world (r,n) an agent considers accessible only possible worlds with the same second coordinate (which corresponds to time). More formally, the class of synchronous models $\mathtt{Mod}_{sync}$ is defined as follows:

DEFINITION 10
The class $\mathtt{Mod}_{sync}$ of models contains all $\mathtt{Mod}$-models which satisfies that:

- if $(r,n)\mathcal{K}_a(r',n')$, then $n = n'$.

It turns out that the axiom system $\mathtt{Ax}_{\mathbf{PTEL}}$ presented in Section 4 is also strongly complete w.r.t. the class $\mathtt{Mod}_{sync}$. The only change in the completeness proof should be made when the accessibility relations in the canonical model are defined so that

- $(r^{\mathbf{S}}, n)\mathcal{K}_a^*(r^{\mathbf{S'}}, n')$ iff $n = n'$ and $\mathbf{S}_n^{-\mathrm{K}_a} = \{\alpha : \mathrm{K}_a\alpha \in \mathbf{S}_n\} \subset \mathbf{S'}_{n'}$.

In systems with perfect recall agents do not forget, while a strongly complete axiomatizations for the corresponding class $\mathtt{Mod}_{pr}$ can be obtained by adding (see [9])

$$AKT2. \qquad \mathrm{K}_a \bigcirc \alpha \to \bigcirc \mathrm{K}_a\alpha$$

5 Modeling of the blockchain protocol

The nowadays very popular BlockChain protocol was introduced in the following way (quotation from [27]):

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

> Nodes always consider the longest chain, i.e., the one containing the most proofs-of-work, to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

A round of the protocol execution consists of the above steps (1–6). During a round an agent (called 'node' in [27]) collects transactions into a block *m* and tries to solve a cryptographic puzzle w.r.t. *m* and a pointer to the last block of its local ledger (called 'chain' in [27]). If it succeeds, the agent adds the block to its ledger and broadcasts it to other nodes. A situation called fork occurs when agents simultaneously receive several solutions. In that case, each agent chooses one of them, and works on it keeping the other ledgers (called 'branches' in [27]). Forks are resolved in later rounds when one branch becomes longer then the others and the agents that have been working on the other (now shorter) branches will then switch to the longer one. One of the essential properties that the blockchain protocol should guarantee, called consistency [17, 39], is that with a high probability agents achieve consensus about a long prefix of the public ledger.

In the sequel the notion '‘proof-of-work’ is used to denote production of a solution of the mentioned cryptographic puzzle related to a set of transactions, without considering what is the method to obtain a solution (e.g., ‘proof-of-work’ used for bitcoins, but also ‘proof-of-memory’, etc.). Also, we do not assume any specific way to achieve consensus between agents (it can be acceptance of fastest solution, Byzantine agreement, etc.). Concerning properties of the blockchain protocol that we analyse, our focus is on a high probability that all agents have a sufficiently long common prefix of their ledgers. The honesty of agents does not play any significant role in the stability of agents’ ledgers, so it is not considered in the sequel. On the other hand, coherence of reasoning of agents has significant impact on executions of the protocol. Hence, agents' soundness w.r.t. **PTEL** is required. Finally, since we do not analyze cryptographic properties of the protocol the assumption about asynchronicity, as the paper [33] explains, can be neglected and we suppose that the blockchain protocol runs in a synchronous setting. In the case of Bitcoin the average time until an agent receives a new block is 6.5 seconds whereas the next block will be only produced after 10 minutes (on average) [5]. In our model, in one round at least one (but maybe several) blocks are produced, they are immediately broadcasted, and each agent accepts one of them. Then the next round starts and next proofs-of-work are computed. So, our further assumptions about the execution scenario of the protocol are as follows:

- Blocks are sent across the network much faster than they are created. Every new block is received by agents in the round in which the block is produced.
- While some messages may get lost, in every round every active agent receives at least one new block.
- If an agent produces a new block, it adds that block to its chain.

In Bitcoin forks are resolved according to (see [15, 27]):

- Let z be the number of blocks validated by the honest agents and let $\mathtt{Pr}(z)$ be the probability that an attacker will win a double spend race (i.e., to succeed to spend the same money more than once) to replace the blocks in the ledger.
- Then $\mathtt{Pr}(z)$ tends exponentially to 0 as z increases.

Thus, in practice, forks will be resolved with some (high) probability.

Our aim is to define a set of axioms for BlockChain, which implies that agents with high probability obtain consensus that long prefixes of their ledgers coincide. In a different setting this is done in [25]. Namely, since the probabilistic part of **PTEL** is not present, in the logic from [25] high probabilities are approximated with knowledge of agents. Here we are able to formally express probabilities and directly model probabilistic features of consensus in BlockChain.

Let $\varepsilon \in [0, 1]_{\mathbb{Q}} \setminus \{0, 1\}$ be a predefined rational number. The intended meaning of ε is 'the lower bound of the probability that exactly one agent produces a proof-of-work in a round'. Next, let a, b and c denote agents from $\mathbb{A}$. We additionally structure the set **Var** of propositional letters by assuming that it contains the following pairwise disjoint sets of symbols:

- **POW** $= \{\mathsf{pow}_a | a \in \mathbb{A}\}$ is a set of atomic propositions, with the intended meaning of pow_a that the agent a produces a proof-of-work;
- **ACC** $= \{\mathsf{acc}_{a,b} | a, b \in \mathbb{A}\}$ is a set of atomic propositions, with the intended meaning of $acc_{a,b}$ that the agent a accepts the proof-of-work produced by the agent b; and
- **LDG** $= \{\mathsf{ldg}_{a,b,k} \;\; a, b \in \mathbb{A}, k \in \mathbb{N}, k \geq 1\}$ is a set of atomic propositions, with the intended meaning of $\mathsf{ldg}_{a,b,k}$ that agents a and b have the same first k blocks in their ledgers.

We also use the following abbreviations:

- $e_a = \bigwedge_{b\in\mathbb{A}}(A_b \to \mathsf{acc}_{b,a})$, with the intended meaning that every active agent accepts the proof-of-work produced by the agent a;
- $\mathsf{ech}_b = \bigvee_{a\in\mathbb{A}} \mathsf{acc}_{b,a}$, with the intended meaning that the agent b accepts some proof-of-work; and
- $(\mathsf{pow} = k) = \bigvee_{\mathbf{X}\subset\mathbb{A},|\mathbf{X}|=k}(\bigwedge_{a\in\mathbf{X}} \mathsf{pow}_a \wedge \bigwedge_{b\notin\mathbf{X}} \neg\mathsf{pow}_b)$, with the intended meaning that exactly k agents produce proof-of-work. Formulas of the form $(\mathsf{pow} \geqslant k)$, $(\mathsf{pow} > k)$, etc., have the obvious meaning.

We will consider a subclass of $\mathtt{Mod}$, denoted $\mathtt{Mod}_{BC}$, whose elements we use to semantically model BlockChain.

DEFINITION 11
A $\mathtt{Mod}$-model $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ is a $\mathtt{Mod}_{BC}$-model if the following holds for every possible world (r, n):

- there is at least one pow_a such that $(r, n) \models \mathsf{pow}_a$;
- if $(r, n) \models \mathsf{pow}_a$, then $(r, n) \models A_a$, i.e., only active agents can produce proofs-of-work;
- if $(r, n) \models \mathsf{acc}_{b,a}$, then $(r, n) \models \mathsf{pow}_a$, i.e., an agent can only accept proof-of-work that has been produced;
- if $(r, n) \models A_a$, then there is exactly one b such that $(r, n) \models \mathsf{acc}_{a,b}$, i.e., in each possible world an active agent accepts exactly one proof-of-work for;
- the probability $\mu^{(r,n)}$ of the event $\bigcirc^i(\mathsf{pow} > 1)$ has an upper bound $1 - \varepsilon$;
- the events $\bigcirc^{i_1}(\mathsf{pow} = k_1), \ldots, \bigcirc^{i_m}(\mathsf{pow} = k_m)$ for $i_j \neq i_l$ are independent w.r.t. to the probability $\mu^{(r,n)}$, i.e.,

$$\mu^{(r,n)}\left(\left[\bigwedge_{i \in \mathbf{Y}} \bigcirc^i \mathsf{pow} = k_i\right]^{(r,n)}\right) = \prod_{i \in \mathbf{y}} \mu^{(r,n)}([\bigcirc^i \mathsf{pow} = k_i]^{(r,n)});$$

- for every integer $k \geqslant 1$:
  - $(r, n) \models \mathsf{ldg}_{a,a,k}$ iff $k \leqslant n + 1$, i.e., in the $n + 1$th round any ledger cannot contain more that $n + 1$ blocks;
  - $(r, n) \models \mathsf{ldg}_{a,b,k} \to \mathsf{ldg}_{b,a,k}$, i.e., the equality between ledgers is symmetric;
  - $(r, n) \models \mathsf{ldg}_{a,b,k} \wedge \mathsf{ldg}_{b,c,k} \to \mathsf{ldg}_{a,c,k}$, i.e., the equality between ledgers is transitive; and
  - $(r, n) \models \mathsf{ldg}_{a,b,k} \to \mathsf{ldg}_{a,b,j}$, $j \leq k$, i.e., the corresponding prefixes of equal ledgers coincide,
- so, the equality between ledgers is an equivalence relation which is sound w.r.t. to the length of ledgers;
- $(r, n) \models \bullet\bot \wedge \bigcirc^k \mathsf{acc}_{a,b} \to \mathsf{ldg}_{a,b,k+1}$, i.e., if a accepts b's proof-of-work, a also accepts b's ledger; and
- $(r, n) \models \bot \wedge \bigcirc^k e_a \wedge \bigcirc^{k+j} A_b \to \mathsf{ldg}_{b,a,k+1}$, i.e., if all accepted proofs-of-work coincide, agents will not change the corresponding part of their ledgers.

$\mathtt{Mod}_{BC}$-models associate rounds with possible worlds, so that the round i ($i \geqslant 1$) of an execution of the blockchain protocol represented by an run r corresponds to $(r, i - 1)$. Blocks in a ledger are enumerated 1, 2, ... The next lemma shows that the class $\mathtt{Mod}_{BC}$ is not empty.

LEMMA 1
There is a model $\mathcal{M} \in \mathtt{Mod}_{BC}$.

PROOF. Let $a \in \mathbb{A}$ and $\mathcal{M} = \langle \mathbf{R}, \mathcal{A}, \mathcal{K}, \mathcal{P} \rangle$ be any $\mathtt{Mod}$ such that:

- $\mathbf{R} = \{r\}$;
- $i \geq 0$, $\mathcal{K}_a((r, i)) = \{(r, i)\}$, $\mathcal{A}((r, i)) = \{a\}$, $H^{(r,i)} = \{\{r\}, \emptyset\}$, $\mu^{(r,i)}(\{r\}) = 1$, $H_a^{(r,i)} = \{\emptyset, \mathbf{W}\}$, $\mu_a^{(r,i)}(\mathbf{W}) = 1$;

- $(r, i) \models \mathsf{pow}_a$;
- $(r, i) \models \mathsf{acc}_{a,a}$; and
- $(r, i) \models \mathsf{ldg}_{a,a,k}$ iff $k \in \{1, \ldots, i+1\}$.

This model satisfies all properties of $\mathtt{Mod}_{BC}$-models. □

Note also that Theorem 10 witnesses existence of models with multiple runs and active agents, and with more complex accessibility relations and measures.

To axiomatize $\mathtt{Mod}_{BC}$ we extend the axiom system $\mathtt{Ax}_{\mathbf{PTEL}}$ with the axioms given in Table 1. The obtained system is denoted by $\mathtt{Ax}_{\mathbf{BC}}$. In particular, the axioms AB1–AB5 provide essential relations between producing and accepting proofs-of-work. Axiom AB6 gives an upper bound that more than one agent produce proofs-of-work. The axioms AB7 and AB8 (combined with RGA) imply independence of the events described by $\mathsf{pow} = k$ in different rounds. The axioms AB9–AB12 express the essential properties of the equality of ledgers. Axiom AB13 connects acceptance of a proof-of-work and updating the ledger by an agent. Axiom AB14 guarantees that once established consensus on the ledgers never changes.

The symbols $\models_{\mathtt{Mod}_{BC}}$ and $\vdash_{\mathtt{Ax}_{\mathbf{BC}}}$ are used to denote validity and provability w.r.t. the class $\mathtt{Mod}_{BC}$ and the axiom system $\mathtt{Ax}_{\mathbf{BC}}$, respectively. By straightforward adaptations of proofs of the theorems 3 and 8 the following theorems can be shown:

THEOREM 9 (Soundness for $\mathtt{Ax}_{\mathbf{BC}}$).
$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \beta$ implies $\models_{\mathtt{Mod}_{BC}} \beta$.

THEOREM 10 (Strong completeness for $\mathtt{Ax}_{\mathbf{BC}}$).
A set $\mathbf{T}$ of formulas is $\mathtt{Ax}_{\mathbf{BC}}$-consistent iff it is $\mathtt{Mod}_{BC}$-satisfiable.

PROOF. We can build the canonical model by following the procedure from Section 4.2. The axioms AB1–AB14 correspond to semantical constraints from Definition 1. Particularly, the axioms AB7 and AB8 guarantee independence w.r.t the measures $\mu^{(r,n)}$, which can be shown by a direct application of rule RGA as in [34,Theorem 4.4]. It follows that the canonical model belongs to $\mathtt{Mod}_{BC}$. □

In the remaining part of the section we prove statements about properties of BlockChain. A trivial consequence of AB1 and AB2 is that at least one agent is active in each round:

LEMMA 2

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \bigvee_{b \in \mathbb{A}} A_b.$$

Lemma 2 and AB4 imply that there cannot be an agreement of acceptance of two different proofs-of-work.

LEMMA 3
For $a, c \in \mathbb{A}$, $a \neq c$:

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} e_a \rightarrow \neg e_c.$$

PROOF. Note that $\bigwedge_{b \in \mathbb{A}}(A_b \rightarrow \mathsf{acc}_{b,a}) \rightarrow \neg \bigwedge_{b \in \mathbb{A}}(A_b \rightarrow \mathsf{acc}_{b,c})$ does not hold only if for each active agent b both $\mathsf{acc}_{b,a}$ and $\mathsf{acc}_{b,c}$ hold, which contradicts AB4. □

We can also prove that the common history persists, i.e., agreements cannot be undone.

TABLE 1 Blockchain axioms **BCTP**

AB1	$\bigvee_{a\in\mathbb{A}} \mathsf{pow}_a$	In each round at least one agent produces proof-of-work.
AB2	$\mathsf{pow}_a \to A_a$	Only active agents can produce proofs-of-work.
AB3	$\mathsf{acc}_{b,a} \to \mathsf{pow}_a$	One can only accept proof-of-work that has been produced.
AB4	$\mathsf{acc}_{b,a} \to \neg\mathsf{acc}_{b,c}$, for each $c \neq a$	An agent accepts at most one proof-of-work for a given round.
AB5	$A_a \to \mathsf{ech}_a$	Each active agent must accept one of the produced proofs-of-work. Note that we do not have any assumption on how an agent accepts a proof.
AB6	$P_{\leqslant 1-\varepsilon} \bigcirc^i (\mathsf{pow} > 1)$	The probability that more than one agent create proof-of-work for a round is bounded from above.
AB7	$\bigwedge_{i\in\mathbf{Y}} P_{\geqslant s_i} \bigcirc^i (\mathsf{pow} = k_i) \to P_{\geqslant s} \bigwedge_{i\in\mathbf{Y}} \bigcirc^i(\mathsf{pow} = k_i) s = \prod_{a\in\mathbf{X}} s_a$, $\mathbf{Y}$ is a finite subset of $\mathbb{N}$, $k_i \in \{1,\dots,\lvert\mathbb{A}\rvert\}$	Necessary condition for independence of $(\mathsf{pow} = k)$'s in different rounds.
AB8	$\bigwedge_{i\in\mathbf{Y}} P_{\leqslant s_i} \bigcirc^i (\mathsf{pow} = k_i) \to P_{\leqslant s} \bigwedge_{i\in\mathbf{Y}} \bigcirc^i(\mathsf{pow} = k_i) s = \prod_{a\in\mathbf{X}} s_a$, $\mathbf{Y}$ is a finite subset of $\mathbb{N}$, $k_i \in \{1,\dots,\lvert\mathbb{A}\rvert\}$	Necessary condition for independence of $(\mathsf{pow} = k)$'s in different rounds.
AB9	$(\bullet^{n+1}\bot \wedge \neg\bullet^{n}\bot) \to \mathsf{ldg}_{a,a,k}$, $k \leqslant n+1$	Reflexivity for equality of ledgers.
AB10	$\mathsf{ldg}_{a,b,k} \to \mathsf{ldg}_{b,a,k}$	Symmetry for equality of ledgers.
AB11	$\mathsf{ldg}_{a,b,k} \wedge \mathsf{ldg}_{b,c,k} \to \mathsf{ldg}_{a,c,k}$	Transitivity for equality of ledgers.
AB12	$\mathsf{ldg}_{a,b,k} \to \mathsf{ldg}_{a,b,j}$, $j \leq k$	Soundness: equality of prefixes of equal ledgers.
AB13	$\bullet\bot \wedge \bigcirc^k \mathsf{acc}_{a,b} \to \mathsf{ldg}_{a,b,k+1}$	Accepting of a pow in the k-th round implies the acceptance of the corresponding ledger.
AB14	$\bullet\bot \wedge \bigcirc^k e_a \wedge \bigcirc^{k+j} A_b \to \mathsf{ldg}_{b,a,k+1}$	Persistence: once achieved consensus cannot be changed in the future.

LEMMA 4
If all active agents agree to accept the same proof-of-work in the round k, then in any future all active agents will have the same first $k+1$ blocks in their ledgers.

PROOF. Let e_a hold in the round k. By AB13 all active agents have the same first $k+1$ blocks in their ledgers. By AB14 this holds in every future round. □

Finally, Theorem 11 states that it is common knowledge among agents that with high probability long prefixes of their ledgers coincide. This can be compared to [17, Theorem 6.3] and [39, Theorem 2].

THEOREM 11
Let ε be the predefined probability threshold and $z \in \mathbb{N}$. Then,

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{C}\, \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}} \bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a.$$

PROOF. First note that $\mathsf{pow} = 1$ implies $\bigvee_{a\in\mathbb{A}} e_a$, i.e., all active agents accept the same proof-of-work.

Since by AB1, $\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \neg(\mathsf{pow} = 0)$, from the valid formula $\models \neg(\mathsf{pow} > 1) \leftrightarrow ((\mathsf{pow} = 0) \vee (\mathsf{pow} = 1))$ it follows that

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \neg(\mathsf{pow} > 1) \leftrightarrow (\mathsf{pow} = 1). \tag{1}$$

Using (1) and AB15 we have that

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \neg \bigwedge_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} > 1) \leftrightarrow \bigvee_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} = 1). \tag{2}$$

Next, from (2) by using Rule RGPN and Lemma 5.14 it follows that for every $s \in [0,1]_{\mathbb{Q}}$

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{P}_{\leqslant s}(\bigwedge_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} > 1)) \leftrightarrow \mathtt{P}_{\geqslant 1-s}(\bigvee_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} = 1)). \tag{3}$$

By AB6–AB8 we have that

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{P}_{\leqslant (1-\varepsilon)^{z+1}}(\bigwedge_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} > 1)). \tag{4}$$

Then, (3) and (4) give

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}}(\bigvee_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} = 1)). \tag{5}$$

Since $\vdash_{\mathtt{Ax}_{\mathbf{BC}}} (\mathsf{pow} = 1) \to \bigvee_{a\in\mathbb{A}} e_a$, we have that

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \bigvee_{i=0}^{z} \bigcirc^{i}(\mathsf{pow} = 1) \to \bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a. \tag{6}$$

Thus, from (5) and (6) it follows

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}}(\bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a). \tag{7}$$

From (7) using Rule R$\mathtt{K}_a$N we obtain:

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{K}_c\, \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}}(\bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a)$$

for arbitrary c and hence

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{E}\ \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}}(\bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a).$$

By repeating applications of Rule $\mathrm{R}\mathtt{K}_a\mathrm{N}$ we have

$$\vdash_{\mathtt{Ax}_{\mathbf{BC}}} \mathtt{E}^{m}\ \mathtt{P}_{\geqslant 1-(1-\varepsilon)^{z+1}}(\bigvee_{i=0}^{z} \bigcirc^{i} \bigvee_{a\in\mathbb{A}} e_a)$$

for arbitrary m and so by Rule RC the statement follows. □

6 The first-order case

As it is mentioned in Section 1, the papers [1, 36, 38] prove that the set of valid formulas in epistemic (and temporal and probabilistic, respectively) first-order logic is not recursively enumerable. It means that no complete finitary axiomatization is possible at all and that there are no finitary tools to adequately model reasoning in this framework. In this section we introduce **FOPTEL**, a first-order extension of **PTEL**. The previously described approach allows this transition to be obtained smoothly without much technical effort, by extending the formal language and adding the corresponding first-order axioms to the axiom system $\mathtt{Ax}_{\mathbf{PTEL}}$. To avoid repetition of details mentioned above, we just sketch the main ideas following [28, 31, 37]. The language of **FOPTEL**, beside classical, temporal, epistemic and probabilistic operators, contains the first-order quantifier $\forall$, and m-ary relation symbols $R_0^m, R_1^m, \ldots$, and function symbols $F_0^m, F_1^m, \ldots$, for every $m \in \mathbb{N}$. The notions of constants, terms, free variables, term that is free for a variable, formulas, and $\exists$ are defined as usual. The set of sentences, i.e., formulas without free variables, is denoted by **Sent**. If α is a formula, $\alpha(t/x)$ is obtained by substituting all free occurrences of x in α by the term t which is free for x in α

A model $\mathcal{M}$ is any tuple $\langle \mathbf{R}, \mathcal{D}, \mathcal{I}, \mathcal{A}, \mathcal{K}, \mathcal{P}\rangle$ such that $\mathbf{R}$, $\mathcal{A}$, $\mathcal{K}$ and $\mathcal{P}$ are defined in the same way as in Definition 2, and

- $\mathcal{D}$ is a non empty domain, and
- $\mathcal{I}$ associates an interpretation $\mathcal{I}((r,n))$ with every possible world $(r,n) \in \mathbf{W}$ such that for all j and k:
  - $\mathcal{I}((r,n))(F_j^k)$ is a function from $\mathcal{D}^k$ to $\mathcal{D}$;
  - for every $(r',n') \in \mathbf{W}$, $\mathcal{I}((r,n))(F_j^k) = \mathcal{I}((r',n'))(F_j^k)$; and
  - $\mathcal{I}((r,n))(P_j^k)$ is a relation over $\mathcal{D}^k$.

Let $\mathcal{M}$ be a model. A variable valuation v assigns some element of the domain to every variable x, $v(x) \in \mathcal{D}$. If $d \in \mathcal{D}$, and v is a valuation, then $v[d/x]$ is a valuation like v except that $v[d/x](x) = d$. The value of a term t in a possible world $(r,n) \in \mathbf{W}$ wrt. v (denoted by $\mathcal{I}((r,n))(t)_v$) is as follows:

- if t is a variable x, then $\mathcal{I}((r,n))(x)_v = v(x)$; and
- if $t = F_j^k(t_1,\ldots,t_k)$, then $\mathcal{I}((r,n))(t)_v = \mathcal{I}((r,n))(F_j^k)(\mathcal{I}((r,n))(t_1)_v,\ldots,\mathcal{I}((r,n))(t_k)_v)$.

Note that we assume that the domain is the same in all possible worlds and that terms are rigid, i.e., each term has the same meaning in all possible worlds of a model. Those assumptions guarantee that all instances of first-order axioms are valid (for more details, see, for example, [13]).

Satisfiability of a formula α in a possible world (r,n) of a model $\mathcal{M}$ w.r.t. v is defined in the following way (only the new cases are given):

- $(r,n), v \models P^k_j(t_1,\ldots,t_k)$ iff $(\mathcal{I}((r,n))(t_1)_v,\ldots,\mathcal{I}((r,n))(t_k)_v) \in \mathcal{I}((r,n))(P^k_j)$; and
- $(r,n), v \models (\forall x)\beta$ iff for every $d \in \mathcal{D}$, $(r,n), v[d/x] \models \beta$.

If for every valuation v, $(r,n), v \models \alpha$, we write $(r,n) \models \alpha$ and say that α is satisfiable in (r,n). A sentence α is satisfiable if there is a possible world (r,n) from a model $\mathcal{M}$ such that $(r,n) \models \alpha$. As in the propositional case, we consider the class $\mathtt{Mod}_{FO}$ of all measurable models.

Example 7 illustrates expressibility of **FOPTEL**.

EXAMPLE 7
Let us consider the N-doors generalized Monty Hall problem. There are a host and a player, and

- There are N doors. There is a car behind one of them.
- A player initially chooses one door.
- Then, the host (who knows where the car is) opens n doors $(1 \leqslant n \leqslant N-2)$. Each of those doors does not hide the car and has not been chosen by the player.
- The host asks the player whether she wants to switch the door.

The question is: what is better winning strategy to switch the door or not? It is well known that the latter brings an advantage.

In the language of **FOPTEL** this problem can be described in the following way:

- Let $N \geqslant 3$ be an arbitrary number of doors.
- The formal language contains the following:
  - the unary relation symbols $\mathtt{Car}$ and $\mathtt{Bet}$;
  - the k-ary relation symbol $\mathtt{Open}_k$, for $k \in \{1,\ldots,N-2\}$; and
  - the binary relation symbol $=$.

The intended meaning is as follows:

- $\mathtt{Car}(x)$ reads 'the car is behind the door x';
- $\mathtt{Bet}(x)$ reads 'the player chooses the door x'; and
- $\mathtt{Open}_k(x_1,\ldots,x_k)$ reads 'the host opens the doors x_1, $\ldots$, x_k' and shows that the car is not behind them,

which is obtained by the following formulas:

- $=$ is the standard equality relation;
- $(\exists x_1,\ldots,x_N)(\bigwedge_{i\neq j}(x_i \neq x_j) \ \wedge\ (\forall y)\bigvee_{i=1}^{N}(y = x_i))$, i.e., there are exactly N doors;
- $(\exists x)\mathtt{Car}(x)$ and $(\exists x)\mathtt{Bet}(x)$, i.e., there is a car behind one of the doors, and the player chooses one of them;
- $\mathtt{Car}(x) \to \mathtt{G}\,\mathtt{Car}(x)$, i.e., the winning door is fixed;
- $(\mathtt{Car}(x) \wedge \mathtt{Car}(y)) \to (x = y)$, i.e., there is exactly one winning door;
- $(\mathtt{Bet}(x) \wedge \mathtt{Bet}(y)) \to (x = y)$, i.e., the player can chose exactly one door in each stage;
- $\mathtt{Open}_k(x_1,\ldots,x_k) \to \bigwedge_{i\neq j}(x_i \neq x_j)$, i.e., the host opens k different doors;
- $\mathtt{Open}_k(x_1,\ldots,x_k) \to \mathtt{Open}_k(x_{\sigma(1)},\ldots,x_{\sigma(1)})$ for an arbitrary permutation σ, i.e., the order of opening is irrelevant;

- $\mathtt{Car}(x) \rightarrow \neg\mathtt{Open}_k(\ldots, x, \ldots))$ and $\mathtt{Bet}(x) \rightarrow \neg\mathtt{Open}_k(\ldots, x, \ldots))$, i.e., the wining door and the door chosen by the player are not among the doors opened by the host;
- $\mathtt{C}\ (\forall x)\mathtt{P}_{=1/N}(\mathtt{Car}(x) \wedge \mathtt{Bet}(x))$, i.e., it is common knowledge that the initial probability distribution of the winning is uniform.

Now, the winning strategy can be coded as follows ($\overrightarrow{y}$ denotes $(y_1, \ldots, y_k)$):

$$\begin{aligned}\mathtt{C}\ \mathtt{P}_{=\frac{N-1}{N(N-k-1)}}(\forall x, \overrightarrow{y}, z)[\mathtt{Car}(z) \quad &\wedge \quad \mathtt{Bet}(x) \wedge \mathtt{G}((x \neq z) \wedge \bigwedge_{i=1}^{k}(x \neq y_i \wedge y_i \neq z)) \\ &\wedge \quad \bigcirc(\mathtt{Open}_k(\overrightarrow{y}) \wedge \mathtt{Bet}(z))].\end{aligned}$$

In other words, it is common knowledge that the probability of runs in which changing the initial choice leads to win the game is $\frac{N-1}{N(N-k-1)}$.

The probabilistic evaluation of the opposite strategy is given by the next formula:

$$\mathtt{C}\ \mathtt{P}_{=\frac{1}{N}}(\forall x, \overrightarrow{y})[\mathtt{Car}(x) \wedge \mathtt{Bet}(x) \wedge \mathtt{G} \bigwedge_{i=1}^{k}(x \neq y_i) \wedge \bigcirc(\mathtt{Open}_k(\overrightarrow{y}) \wedge \mathtt{Bet}(x))].$$

Since $\frac{N-1}{N(N-k-1)} > \frac{1}{N}$, the former strategy is better than the later one.

An infinitary axiomatic system $\mathtt{Ax}_{\mathbf{FOPTEL}}$ for **FOPTEL** contains the system $\mathtt{Ax}_{\mathbf{PTEL}}$ and additionally the following axiom schemas and an inference rule:

*FO*1. $(\forall x)(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow (\forall x)\beta)$, where x is not free in α

*FO*2. $(\forall x)\alpha \rightarrow \alpha(t/x)$,

FO$\bigcirc$. $(\forall x) \bigcirc \alpha \rightarrow \bigcirc(\forall x)\alpha$

*FO*K. $(\forall x)\mathtt{K}_a\alpha \rightarrow \mathtt{K}_a(\forall x)\alpha$

Gen. $\dfrac{\alpha}{(\forall x)\alpha}$ (Generalization)

The axioms FO$\bigcirc$ and FOK are variants of the well-known Barcan formula, which is valid in constant domain models. Also, these axioms are used to prove a first-order variant of the Strong necessitation Theorem 5. For example, assume that $(\forall x)\alpha$ is inferred from the set of formulas $\mathbf{T}$ using Rule Gen:

$\mathbf{T} \vdash \alpha$
$\mathbf{T} \vdash (\forall x)\alpha$, by Gen

Then,

$\bigcirc\mathbf{T} \vdash \bigcirc\alpha$, by the induction hypothesis;
$\bigcirc\mathbf{T} \vdash (\forall x) \bigcirc \alpha$, by Gen; and
$\bigcirc\mathbf{T} \vdash \bigcirc(\forall x)\alpha$, using FO$\bigcirc$.

Additionally, we have to consider so called saturated sets that satisfy maximality and consistency conditions and also that if $\neg(\forall x)\alpha(x)$ belongs to a set $\mathbf{T}$, then there is a term t such that $\neg\alpha(t/x) \in \mathbf{T}$. Instead of Theorem 6, we can prove

THEOREM 12
Let **T** be a consistent set of sentences in the language $\mathcal{L}$ of **FOPTEL**, and **C** an infinite enumerable set of new constant symbols. Then **T** can be extended to a saturated theory $\mathbf{T}^*$ in the language $\mathcal{L}^* = \mathcal{L} \cup \mathbf{C}$.

similarly as in [31], and by following the main steps from the propositional case we obtain

THEOREM 13 (Strong completeness for $\mathtt{Ax}_{\mathbf{FOPTEL}}$).
A set **T** of sentences is $\mathtt{Ax}_{\mathbf{FOPTEL}}$-consistent iff it is satisfiable.

7 Conclusion

To model and study distributed multiagent systems, one needs various temporal, epistemic and probabilistic operators. We have introduced propositional and first-order languages suitable for formalization of reasoning about such systems. We have provided the Kripke-like possible worlds semantics and the corresponding axiom systems. We have proved strong completeness w.r.t. the measurable classes of models, where one of important steps is to show the strong necessitation theorem. Regarding this, we define the notion of k-nested implications and use it in formulations of infinitary inference rules. In the first-order case we have considered models with constant domains and rigid terms.

One can argue that conditionals are more naturally modeled using conditional probability instead of implications (as we have done in this paper). We can extend our logics with conditional probability operators in a way described in [4, 35]. Also, reasoning about unbounded sets of agents can be obtained as in [37]. Another possible extension of the presented languages may concern the approach from [8] where formulas with linear combinations of probabilities are considered. The papers [4, 6, 30] give technical details for transition from modal like probabilistic operators to linear combinations of probabilistic weights.

Possible future work concerns decidability of **PTEL**, study of logics in which combinations of operators are restricted, e.g., iterations of probabilistic operators are not allowed [32] and/or temporal and epistemic operators cannot act on formulas with leading probabilistic operators. Another challenge is to refine our approach to model the asynchronous blockchain protocol.

Funding

This work was supported by the Science Fund of the Republic of Serbia, Grant AI4TrustBC: Advanced Artificial Intelligence Techniques for Analysis and Design of System Components Based on Trustworthy BlockChain Technology and by the Serbian Ministry of Education, Science and Technological Development (Agreement No. 451-03-9/2021-14/200029).

Acknowledgements

The authors wish to thank the anonymous referees whose comments helped clarify a number of points and improve the text.

References

[1] M. Abadi and Y. Halpern. Decidability and expressiveness for first-order logics of probability. *Information and Computation*, **112**, 1–36, 1994.

[2] K. Brünnler, D. Flumini and T. Studer. A logic of blockchain updates. *Journal of Logic and Computation*, **30**, 1469–1485, 2020.

[3] K. Brünnler and T. Studer. Syntactic cut-elimination for common knowledge. *Annals of Pure and Applied Logic*, **160**, 82–95, 2009.

[4] Š. Dautović, D. Doder and Z. Ognjanović. An epistemic probabilistic logic with conditional probabilities. In *Proceedings of the 17th European Conference Logics in Artificial Intelligence, JELIA 2021, Virtual Event, May 17–20, 2021*, W. Faber, G. Friedrich, M. Gebser and M. Morak., eds. Volume 12678 of Lecture Notes in Computer Science. Springer, 2021.

[5] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In *13th IEEE International Conference on Peer-to-Peer Computing*, pp. 1–10, IEEE, 2013.

[6] D. Doder and Z. Ognjanović. A probabilistic logic for reasoning about uncertain temporal information. In *Proceedings of the Thirty-First Conference on Uncertainty in Artificial Intelligence, UAI 2015, July 12-16, 2015*, M. Meila and T. Heskes., eds, pp. 248–257. Amsterdam, The Netherlands, AUAI Press, 2015.

[7] R. Fagin and J.Y. Halpern. Reasoning about knowledge and probability. *Journal of the ACM*, **41**, 340–367, 1994.

[8] R. Fagin, J. Y. Halpern and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, **87**, 78–128, 1990.

[9] R. Fagin, J. Y. Halpern, Y. Moses and M. Y. Vardi. *Reasoning About Knowledge*. The MIT Press, Cambridge, Massachusetts, 1995.

[10] M. C. Fitting. Basic modal logic. In *Handbook of Logic in Artificial Intelligence and Logic Programming*, D. M. Gabbay, C. Hogger and J. Robinson., eds, vol. 1, pp. 368–448. Oxford University Press, 1993.

[11] D. Gabbay, A. Pnueli, S. Shelah and J. Stavi. On the temporal basis of fairness. In *Conference Record of the 7th Annual ACM Symposium on Principles of Programming Languages, Las Vegas, Nevada, USA, January 1980*, pp. 163–173, Association for Computing Machinery, New York, USA, 1980.

[12] J. Garay, A. Kiayias and N. Leonardos. The bitcoin backbone protocol: analysis and applications. *Cryptology ePrint Archive*, 2017.

[13] J. W. Garson. Quantification in modal logic. In *Handbook of Philosophical Logic*, D. Gabbay and F. Guenthner., eds, vol. 2, pp. 249–307. D. Reidel Publishing Comp, 1984.

[14] A.J. Grove and J.Y. Halpern. Naming and identity in epistemic logics part I: the propositional case. *Journal of Logic and Computation*, **3**, 345–378, 1993.

[15] C. Grunspan and R. Péerez-Marco. Double spend races. *Technical Report* 1702.02867 [cs.CR], *arXiv.org*, 2017.

[16] J. Y. Halpern. *Reasoning About Uncertainty*. The MIT Press, 2003.

[17] J.Y. Halpern and R. Pass. A knowledge-based analysis of the blockchain protocol. In *Proceedings of the 16th Conference on Theoretical Aspects of Rationality and Knowledge, TARK 2017, Liverpool, UK, 24–26 July 2017*, J. Lang., ed. Volume 251 of Electronic Proceedings in Theoretical Computer Science, Open Publishing Association, 2017.

[18] J.Y. Halpern, R. van der Meyden and M.Y. Vardi. Complete axiomatizations for reasoning about knowledge and time. *SIAM Journal on Computing*, **33**, 674–703, 2004.

[19] L. Henkin. The completeness of the first-order functional calculus. *The Journal of Symbolic Logic*, **14**, 159–166, 1949.

[20] J. Hintikka. *Knowledge and Belief: an Introduction to the Logic of the Two Notions*. Cornell University Press, 1962.

[21] F. Kröger. *Temporal Logic of Programs. Monographs in Theoretical Computer Science – An EATCS Series*. Springer, Berlin, 1987.

[22] D. Lehmann. Knowledge, common knowledge and related puzzles. In *PODC '84: Proceedings of the 3rd Annual ACM Symposium on Principles of Distributed Computing*, pp. 62–672, Association for Computing Machinery, New York, USA, 1984.

[23] O. Lichtenstein and A. Pnueli. Propositional temporal logics: decidability and completeness. *Logic Journal of the IGPL*, **8**, 55–85, 2000.

[24] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems Specification*. Springer, 1992.

[25] B. Marinković, P. Glavan, Z. Ognjanović, D. Doder and T. Studer. Probabilistic consensus of the blockchain protocol. In *The 15th European Conference on Symbolic and Quantitative Approaches to Reasoning with Uncertainty, ECSQARU 2019, Belgrade, Serbia, 18–20 September 2019*, G. Kern-Isberner and Z. Ognjanović., eds. Volume 11726 of Lecture Notes in Computer Science, pp. 469–480. Springer, 2019.

[26] B. Marinković, P. Glavan, Z. Ognjanović and T. Studer. A temporal epistemic logic with a non-rigid set of agents for analyzing the blockchain protocol. *Journal of Logic and Computation*, **29**, 803–830, 2019.

[27] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. *Technical report,bitcoin.org*, 2009.

[28] Z. Ognjanović. Discrete linear-time probabilistic logics: completeness, decidability and complexity. *Journal of Logic and Computation*, **16**, 257–285, 2006.

[29] Z. Ognjanović., ed. *Probabilistic Extensions of Various Logical Systems*. Springer, Cham, Switzerland, 2020.

[30] Z. Ognjanović, Z. Marković, M. Rašković, D. Doder and A. Perović. A propositional probabilistic logic with discrete linear time for reasoning about evidence. *Annals of Mathematics and Artificial Intelligence*, **65**, 217–243, 2012.

[31] Z. Ognjanović and M. Rašković. Some first-order probability logics. *Theoretical Computer Science*, **247**, 191–212, 2000.

[32] Z. Ognjanović, M. Rašković and Z. Marković. *Probability logics*. In *Probability-Based Formalization of Uncertain Reasoning*. Springer, Cham, Switzerland, 2016.

[33] R. Pass, L. Seeman and A. Shelat. *Analysis of the blockchain protocol in asynchronous networks*. Technical report. Cryptology ePrint Archive, 2016.

[34] A. Perović, Z. Ognjanović, M. Rašković and D. Radojević. Finitely additive probability measures on classical propositional formulas definable by Gödel's t-norm and product t-norm. *Fuzzy Sets and Systems*, **169**, 65–90, 2011.

[35] M. Rašković, Z. Marković and Z. Ognjanović. A logic with approximate conditional probabilities that can model default reasoning. *International Journal of Approximate Reasoning*, **49**, 52–66, 2008.

[36] A. Szalas and L. Holenderski. Incompleteness of first-order temporal logic with until. *Theoretical Computer Science*, **57**, 317–325, 1988.

[37] S. Tomović, Z. Ognjanović and D. Doder. A First-Order Logic for Reasoning about Knowledge and Probability. *ACM Transactions on Computational Logic*, **21**, 16:1–16:30, 2020.

[38] F. Wolter. First-order common knowledge logics. *Studia Logica*, **65**, 249–271, 2000.

[39] J. Zhao, J. Tang, Z. Li, H. Wang, K.-Y. Lam and K. Xue. An analysis of blockchain consistency in asynchronous networks: deriving a neat bound. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pp. 179–189, IEEE Communications Society, 2020.

A Statements and proofs related to strong completeness

A.1 Soundness

THEOREM 2 (Soundness for $\mathrm{Ax}_{\mathbf{PTEL}}$).
$\vdash \beta$ implies $\models \beta$.

PROOF. We consider Rule RS:

$$\frac{\{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\alpha \wedge \neg\alpha)) \wedge \bullet^i \beta)) \ : \ i \in \mathbb{N}\}}{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta))}$$

and the other cases are left to the reader. We use induction on k to prove that the rule preserves validity, i.e., that in an arbitrary possible world, if all assumptions of the rule hold, then the conclusion holds, too.

Let $k = 0$ and

$$\gamma_i = \neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\alpha \wedge \neg\alpha)) \wedge \bullet^i \beta),$$

i.e., the assumptions are of the form

$$\beta_0 \to \gamma_i$$

and the conclusion is of the form

$$\beta_0 \to \neg(\alpha \mathtt{S} \beta).$$

Note that for every $j \in \mathbb{N}$:

- for every $i \in \mathbb{N}$, if $i \leqslant j$, then $(r,j) \models \bigwedge_{l=0}^{i} \neg\bullet^l(\alpha \wedge \neg\alpha)$ and
- for every $i \in \mathbb{N}$, if $i > j$, then $(r,j) \not\models \bigwedge_{l=0}^{i} \neg\bullet^l(\alpha \wedge \neg\alpha)$,

so, in any possible world (r,j), γ_i is reduced to

- $\gamma_i = \neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge \bullet^i \beta)$, if $i \leqslant j$, and
- $\gamma_i = \alpha \vee \neg\alpha$, if $i > j$.

Let (r,j) be an arbitrary possible world which satisfies all assumptions of the rule. If $(r,j) \not\models \beta_0$, obviously $(r,j) \models \beta_0 \to \neg(\alpha \mathtt{S} \beta)$. So, let $(r,j) \models \beta_0$. Then every γ_i holds in (r,j). Since γ_i, for $i > j$, is a tautology, we consider only the first $j+1$ formulas: $\gamma_0, \ \ldots, \gamma_j$. Then, there is no integer $i \in [0,j]$ such that

- $(r,j) \models \bullet^i \beta$, i.e., $(r,j-i) \models \beta$ and
- for every integer $l \leqslant i-1$, $(r,j) \models \bullet^l \alpha$, i.e., $(r,j-l) \models \alpha$,

which means that

- $(r,j) \not\models \alpha \mathtt{S} \beta$, i.e.,
- $(r,j) \models \neg(\alpha \mathtt{S} \beta)$.

Next, let us consider the case where $k > 0$. Let the statement hold for every instance of Rule R$\mathtt{S}$ with less than k nested implications. According to Definition 1, the assumptions are of the form

$$\beta_k \rightarrow X_k \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i} \neg \bullet^l (\alpha \wedge \neg\alpha)) \wedge \bullet^i \beta)),$$

where $X_k \in \{\mathrm{K}_a : a \in \mathbb{A}\} \cup \{\bigcirc, \bullet\}$. Let (r,j) be an arbitrary possible world which satisfies all assumptions of the rule. If $(r,j) \not\models \beta_k$, the statement trivially holds. Thus, assume $(r,j) \models \beta_k$. If $X_k = \mathrm{K}_a$, it means that

- all formulas
$$\Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i} \neg \bullet^l (\alpha \wedge \neg\alpha)) \wedge \bullet^i \beta)),$$
hold in all possible worlds accessible from (r,j);
- using the induction hypothesis, all possible worlds accessible from (r,j) satisfy $\Phi_{k-1,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta))$; and
- $(r,j) \models \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta))$.

A similar explanation can be used for $X_k = \bigcirc$. Finally, if $X_k = \bullet$, we can proceed in the same way, but we distinguish the case when we consider a world which is the beginning of a run r, in which case $(r,0)$ satisfies every formula with the leading operator $\bullet$, and obviously

- $(r,0) \models \beta_k \rightarrow \bullet \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg(\alpha \mathtt{S} \beta))$.

holds. □

A.2 Deduction theorem, strong necessitation theorem and auxiliary statements

THEOREM 4 (Deduction theorem).
If $\mathbf{T} \subset \mathbf{For}$, then

$$\mathbf{T}, \{\alpha\} \vdash \beta \text{ iff } \mathbf{T} \vdash \alpha \rightarrow \beta.$$

PROOF. The $(\leftarrow)$-direction is standard. To prove the $(\rightarrow)$-direction we use transfinite induction on the length of the proof of β from $\mathbf{T}$. Let us start with the case that β is an axiom. Then,

$\mathbf{T} \vdash \beta$
$\mathbf{T} \vdash \beta \rightarrow (\alpha \rightarrow \beta)$, since $\beta \rightarrow (\alpha \rightarrow \beta)$ is an axiom
$\mathbf{T} \vdash \alpha \rightarrow \beta$, by MP.

If β is obtained by an application of the rule MP we have

$\mathbf{T}, \alpha \vdash \gamma$
$\mathbf{T}, \alpha \vdash \gamma \rightarrow \beta$
$\mathbf{T}, \alpha \vdash \beta$, by MP
$\mathbf{T} \vdash \alpha \rightarrow \gamma$, by the induction hypothesis
$\mathbf{T} \vdash \alpha \rightarrow (\gamma \rightarrow \beta)$, by the induction hypothesis
$\mathbf{T} \vdash (\alpha \rightarrow (\gamma \rightarrow \beta)) \rightarrow ((\alpha \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta))$, since $(\alpha \rightarrow (\gamma \rightarrow \beta)) \rightarrow ((\alpha \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta))$ is an axiom

$\mathbf{T} \vdash (\alpha \to \gamma) \to (\alpha \to \beta)$, by MP
$\mathbf{T} \vdash \alpha \to \beta$, by MP.

Next, we will analyze the cases of the rules R$\bigcirc$N and RS, and left the rest to the reader. If $\beta = \bigcirc\gamma$ is obtained by an application of the rule R$\bigcirc$N, then γ and $\bigcirc\gamma$ are theorems and the statement holds:

$\vdash \alpha \to \bigcirc\gamma$, by propositional reasoning, and
$\mathbf{T} \vdash \alpha \to \bigcirc\gamma$, by the definition of a proof from the set $\mathbf{T}$.

Let us assume that $\beta = \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\gamma \mathrm{S} \delta))$ and

$\mathbf{T}, \alpha \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \gamma) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\gamma \wedge \neg\gamma)) \wedge \bullet^i \delta))$, for every $i \in \mathbb{N}$.

If $k > 0$, then

$\mathbf{T} \vdash \alpha \to \Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \gamma) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\gamma \wedge \neg\gamma)) \wedge \bullet^i \delta))$, for every $i \in \mathbb{N}$, by the induction hypothesis
$\mathbf{T} \vdash (\alpha \wedge \beta_k) \to X_k \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \gamma) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\gamma \wedge \neg\gamma)) \wedge \bullet^i \delta))$, for every $i \in \mathbb{N}$, by the definition of Φ_k and propositional reasoning.

Now, we define $\overline{\boldsymbol{B}} = (\beta_0, \ldots, \beta_{k-1}, \alpha \wedge \beta_k)$, and have

$\mathbf{T} \vdash \Phi_{k,\overline{\boldsymbol{B}},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bullet^l \gamma) \wedge (\bigwedge_{l=0}^{i} \neg\bullet^l(\gamma \wedge \neg\gamma)) \wedge \bullet^i \delta))$, for every $i \in \mathbb{N}$
$\mathbf{T} \vdash \Phi_{k,\overline{\boldsymbol{B}},\mathbf{X}}(\neg(\gamma \mathrm{S} \delta))$, by R$\mathrm{S}$
$\mathbf{T} \vdash (\alpha \wedge \beta_k) \to X_k \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg(\gamma \mathrm{S} \delta))$
$\mathbf{T} \vdash \alpha \to (\beta_k \to X_k \Phi_{k-1,\mathbf{B}_{j=0}^{k-1},\mathbf{X}_{j=1}^{k-1}}(\neg(\gamma \mathrm{S} \delta))$
$\mathbf{T} \vdash \alpha \to \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\gamma \mathrm{S} \delta))$.

If $k = 0$, we reason as above, with the proviso that $\overline{\boldsymbol{B}} = (\alpha \wedge \beta_0)$. □

THEOREM 5 (Strong necessitation).
If $\mathbf{T} \subset \mathbf{For}$ and $\mathbf{T} \vdash \gamma$, then

1. $\bigcirc\mathbf{T} \vdash \bigcirc\gamma$;
2. $\bullet\mathbf{T} \vdash \bullet\gamma$; and
3. $\mathrm{K}_a\mathbf{T} \vdash \mathrm{K}_a\gamma$, for every $a \in \mathbf{A}$.

PROOF. We consider the statement (2). The statements (1) and (3) can be proved in a similar way and are left to the reader. We use transfinite induction on the length of the proof of γ from $\mathbf{T}$. Assume that $\gamma = \gamma_{\lambda+1}$, that $\gamma_0, \gamma_1, \ldots, \gamma_{\lambda+1}$ is a proof of γ from T and that (2) holds for every γ_m, $m \leqslant \lambda$.

If γ is an instance of an axiom schema, $\vdash \gamma$, then also $\vdash \bullet\gamma$, and obviously $\bullet\mathbf{T} \vdash \bullet\gamma$. If $\gamma \in \mathbf{T}$, then $\bullet\gamma \in \bullet\mathbf{T}$, and $\bullet\mathbf{T} \vdash \bullet\gamma$. If γ is obtained by Rule MP from the previous formulas from the proof:

$\mathbf{T} \vdash \gamma_j$
$\mathbf{T} \vdash \gamma_j \to \gamma$
$\mathbf{T} \vdash \gamma$,

then

$\bullet\mathbf{T} \vdash \bullet\gamma_j$, by the induction hypothesis
$\bullet\mathbf{T} \vdash \bullet(\gamma_j \to \gamma)$, by the induction hypothesis
$\bullet\mathbf{T} \vdash \bullet\gamma_j \to \bullet\gamma$, using A$\bullet\!\to$ and MP and
$\bullet\mathbf{T} \vdash \bullet\gamma$, by MP.

If γ is obtained from γ_j by an application of one of the rules R$\bigcirc$N, R$\bullet$N, R$\mathtt{K}_a$N, RGPN, RPN, then $\vdash \gamma$, and reasoning as above we can prove the statement. Finally, assume that γ is obtained by an application of one of the infinitary rules R$\mathtt{U}$, R$\mathtt{S}$, RC, RGA, RA. Let us consider Rule R$\mathtt{U}$ and $\gamma = \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta))$. Then, we have the following:

$\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \alpha) \wedge \bigcirc^i \beta))$, for every $i \in \mathbb{N}$;
$\bullet\mathbf{T} \vdash \bullet\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \alpha) \wedge \bigcirc^i \beta))$, for every $i \in \mathbb{N}$, by the induction hypothesis; and
$\bullet\mathbf{T} \vdash (\beta_k \vee \neg\beta_k) \to \bullet\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \alpha) \wedge \bigcirc^i \beta))$, for every $i \in \mathbb{N}$.

We extend $\mathbf{B}$ and $\mathbf{X}$:

- $\overline{\boldsymbol{B}} = (\beta_0, \ldots, \beta_k, \beta_k \vee \neg\beta_k)$ and
- $\overline{\boldsymbol{X}} = (X_1, \ldots, X_k, \bullet)$

so that

$\bullet\mathbf{T} \vdash \Phi_{k+1,\overline{\boldsymbol{B}},\overline{\boldsymbol{X}}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l \alpha) \wedge \bigcirc^i \beta))$, for every $i \in \mathbb{N}$
$\bullet\mathbf{T} \vdash \Phi_{k+1,\overline{\boldsymbol{B}},\overline{\boldsymbol{X}}}(\neg(\alpha \mathtt{U} \beta))$, by R$\mathtt{U}$
$\bullet\mathbf{T} \vdash (\beta_k \vee \neg\beta_k) \to \bullet\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta)))$ and
$\bullet\mathbf{T} \vdash \bullet\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta))$.

The same idea can be used to prove the statement in the cases of the other infinitary inference rules. □

LEMMA 5
The following hold:

1. if $\vdash \alpha \leftrightarrow \beta$, then $\vdash \bigcirc\alpha \leftrightarrow \bigcirc\beta$
2. if $\vdash \alpha \leftrightarrow \beta$, then $\vdash \bullet\alpha \leftrightarrow \bullet\beta$
3. $\vdash \mathtt{K}_a(\alpha \wedge \neg\alpha) \to \mathtt{K}_a(\beta \wedge \neg\beta)$
4. $\vdash \neg\bullet\alpha \to \bullet\neg\alpha$
5. $\vdash \bullet(\alpha \wedge \beta) \leftrightarrow (\bullet\alpha \wedge \bullet\beta)$
6. $\vdash (\bullet\alpha \vee \bullet\beta) \to \bullet(\alpha \vee \beta)$
7. $\bullet(\alpha \wedge \neg\alpha) \vdash \bullet\beta$
8. $\vdash (\bigcirc\alpha \to \bigcirc\beta) \leftrightarrow \bigcirc(\alpha \to \beta)$,
9. $\vdash (\bigcirc\alpha \wedge \bigcirc\beta) \leftrightarrow \bigcirc(\alpha \wedge \beta)$,
10. $\vdash (\bigcirc\alpha \vee \bigcirc\beta) \leftrightarrow \bigcirc(\alpha \vee \beta)$,
11. for $j \in \mathbb{N}$, $\bigcirc^j\beta, \bigcirc^0\alpha, \ldots, \bigcirc^{j-1}\alpha \vdash \alpha \mathtt{U} \beta$
12. $\vdash \alpha \mathtt{S} \beta \leftrightarrow (\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge (\beta \vee (\alpha \wedge \bullet(\alpha \mathtt{S} \beta))))$.
13. for $j \in \mathbb{N}$, $\bullet^j\beta$, $\bigwedge_{k=1}^{j} \neg\bullet^k(\alpha \wedge \neg\alpha)$, $\bigwedge_{l=0}^{j-1} \bullet^l\alpha \vdash \alpha \mathtt{S} \beta$.
14. $\vdash \mathtt{P}_{\geqslant 1}(\alpha \to \beta) \to (\mathtt{P}_{\geqslant s}\alpha \to \mathtt{P}_{\geqslant s}\beta)$, for every $s \in [0,1]_{\mathbb{Q}}$.
15. If $\vdash \alpha \leftrightarrow \beta$, then $\vdash \mathtt{P}_{\geqslant s}\alpha \leftrightarrow \mathtt{P}_{\geqslant s}\beta$, for every $s \in [0,1]_{\mathbb{Q}}$.
16. $\vdash \mathtt{P}_{a,\geqslant 1}(\alpha \to \beta) \to (\mathtt{P}_{a,\geqslant s}\alpha \to \mathtt{P}_{a,\geqslant s}\beta)$,
17. If $\vdash \alpha \leftrightarrow \beta$, then $\vdash \mathtt{P}_{a,\geqslant s}\alpha \leftrightarrow \mathtt{P}_{a,\geqslant s}\beta$, for every $s \in [0,1]_{\mathbb{Q}}$.
18. $\vdash \mathtt{P}_{\geqslant s}\alpha \to \mathtt{P}_{\geqslant r}\alpha$, for $s \geqslant r$, for every $s \in [0,1]_{\mathbb{Q}}$.
19. $\vdash \mathtt{P}_{a,\geqslant s}\alpha \to \mathtt{P}_{a,\geqslant r}\alpha$, for $s \geqslant r$.
20. $\vdash \mathtt{P}_{\leqslant s}\alpha \to \mathtt{P}_{\leqslant r}\alpha$, for $r \geqslant s$.
21. $\vdash \mathtt{P}_{a,\leqslant s}\alpha \to \mathtt{P}_{a,\leqslant r}\alpha$, for $r \geqslant s$.

PROOF. Proofs of the statements (1) – (10) can be found in standard textbooks (e.g. [21, 24]), for the statements (14)–(21) in [32], and for (11) in [28].

(12) Using propositional reasoning, we have that:

$$\vdash (\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \quad \vee \quad (\neg\bullet(\alpha \wedge \neg\alpha) \wedge (\beta \vee (\alpha \wedge \bullet(\alpha \mathrm{S} \beta)))) \leftrightarrow$$
$$(\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \quad \vee \quad (\neg\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge \bullet(\alpha \mathrm{S} \beta))$$

and since $\vdash [(\gamma \wedge \delta) \vee (\neg\gamma \wedge \delta)] \leftrightarrow \delta$ also:

$$\vdash (\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \quad \vee \quad (\neg\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge \bullet(\alpha \mathrm{S} \beta)) \leftrightarrow$$
$$\beta \quad \vee \quad (\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge \bullet(\alpha \mathrm{S} \beta))$$

The right side of the last formula is Axiom A$\mathrm{S}\bullet$, thus

$$\vdash (\bullet(\alpha \wedge \neg\alpha) \wedge \beta) \vee (\neg\bullet(\alpha \wedge \neg\alpha) \wedge (\beta \vee (\alpha \wedge \bullet(\alpha \mathrm{S} \beta)))).$$

(13) If $j = 0$, the statement is

$$\beta \vdash \alpha \mathrm{S} \beta$$

which follows from Axiom A$\mathrm{S}\bullet$. So, let $j > 0$ and

$$\begin{aligned}\gamma = \quad (\quad & \neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha) \wedge (\bullet\beta \vee [(\neg\bullet^2(\alpha \wedge \neg\alpha) \wedge \bullet\alpha) \wedge (\bullet^2\beta \vee \\ [\quad & \ldots \wedge (\bullet^{j-1}\beta \vee [(\neg\bullet^j(\alpha \wedge \neg\alpha) \wedge \bullet^{j-1}\alpha) \wedge (\bullet^j\beta \vee \\ [\quad & \neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta)])]) \ldots])]).\end{aligned}$$

Using propositional reasoning it can be obtained:

$\bullet^j\beta \vdash \bullet^j\beta \vee [\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta)]$
$\bullet^j\beta, \neg\bullet^j(\alpha \wedge \neg\alpha), \bullet^{j-1}\alpha \vdash \neg\bullet^j(\alpha \wedge \neg\alpha) \wedge \bullet^{j-1}\alpha \wedge (\bullet^j\beta \vee [\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta)])$
$\bullet^j\beta, \bigwedge_{k=1}^{j} \neg\bullet^k(\alpha \wedge \neg\alpha), \bigwedge_{l=0}^{j-1} \bullet^l\alpha \vdash \gamma.$

Next, using Lemma 5.2 we can transform γ in the following way:

- $\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \vdash \bullet^j\neg\bullet(\alpha \wedge \neg\alpha)$, by Lemma 5.4
- $\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta) \vdash \bullet^j[\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge \bullet(\alpha \mathrm{S} \beta)]$, by Axiom A$\bullet\wedge$
- $\bullet^j\beta \vee [\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta)] \vdash \bullet^j(\beta \vee [\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge \bullet(\alpha \mathrm{S} \beta)])$, by Lemma 5.6
- $\bullet^j\beta \vee [\neg\bullet^{j+1}(\alpha \wedge \neg\alpha) \wedge \bullet^j\alpha \wedge \bullet^{j+1}(\alpha \mathrm{S} \beta)] \vdash \bullet^j(\alpha \mathrm{S} \beta)$, using Axiom A$\mathrm{S}\bullet$

In this way,

$$\gamma \vdash \gamma',$$

where

$$\begin{aligned}\gamma' = \quad (\quad & \neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha) \wedge (\bullet\beta \vee [(\neg\bullet^2(\alpha \wedge \neg\alpha) \wedge \bullet\alpha) \wedge (\bullet^2\beta \vee \\ [\quad & \ldots \wedge (\bullet^{j-1}\beta \vee [(\neg\bullet^j(\alpha \wedge \neg\alpha) \wedge \bullet^{j-1}\alpha) \wedge \bullet^j(\alpha \mathrm{S} \beta)])]) \ldots])]),\end{aligned}$$

and the degree of $\bullet$ in front of $\alpha \mathrm{S} \beta$ in γ' is j. We can continue in the same way and obtain

$\gamma \vdash \neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge (\alpha \mathrm{S} \beta)$,
$\gamma \vdash \beta \vee [\neg\bullet(\alpha \wedge \neg\alpha) \wedge \alpha \wedge (\alpha \mathrm{S} \beta)]$ and
$\gamma \vdash \alpha \mathrm{S} \beta$, using Axiom A$\mathrm{S}\bullet$.

Thus, we have

$$\bullet^j\beta, \bigwedge_{k=1}^{j} \neg\bullet^k(\alpha \wedge \neg\alpha), \bigwedge_{l=0}^{j-1} \bullet^l\alpha \vdash \gamma;$$

$\gamma \vdash \alpha \mathtt{S} \beta$; and, finally,
$\bullet^j \beta, \bigwedge_{k=1}^{j} \neg \bullet^k (\alpha \wedge \neg\alpha), \bigwedge_{l=0}^{j-1} \bullet^l \alpha \vdash \alpha \mathtt{S} \beta$. □

THEOREM 14 (Witnesses' theorem).
Let $\mathbf{T}$ be a consistent set of formulas. Then,

1. If $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta))\}$ is not consistent, then there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i_0-1} \bigcirc^l \alpha) \wedge \bigcirc^{i_0} \beta))\}$$
is consistent.
2. If $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta))\}$ is not consistent, then there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i_0-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{i_0} \neg\bullet^l (\alpha \wedge \neg\alpha)) \wedge \bullet^{i_0} \beta))\}$$
is consistent.
3. If $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{C}\alpha)\}$ is not consistent, then there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}((\mathtt{E})^{i_0}\alpha)\}$$
is consistent.
4. If $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{\geqslant r}\alpha)\}$ is not consistent, then there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{\geqslant r - \frac{1}{i_0}}\alpha)\}$$
is consistent.
5. If $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r}\alpha)\}$ is not consistent, then there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha)\}$$
is consistent.

PROOF. We consider the statement (5). The other statements can be proved in a similar way and are left to the reader. So, let $\mathbf{T}$ be a consistent set of formulas such that

- $\mathbf{T} \cup \{\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r}\alpha)\}$ is not consistent; and
- for every $i_0 \in \mathbb{N}$, $\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha)\}$ is not consistent.

Then,

$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha)\} \vdash (\gamma \wedge \neg\gamma)$, for every $i_0 \in \mathbb{N}$;
$\mathbf{T} \vdash \neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha) \to (\gamma \wedge \neg\gamma)$, by Deduction theorem, for every $i_0 \in \mathbb{N}$;
$\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha)$, for every $i_0 \in \mathbb{N}$;
$\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r}\alpha)$, by RA,

which contradicts the assumption about consistency of $\mathbf{T}$. Hence, there is $i_0 \in \mathbb{N}$ such that
$$\mathbf{T} \cup \{\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{i_0}}\alpha)\}$$
is consistent. □

LEMMA 6

Let $\mathbf{T}$ be a maximal consistent set of formulas. Then,

1. For every formula α, exactly one of α and $\neg\alpha$ is in $\mathbf{T}$.
2. $\mathbf{T}$ is deductively closed.
3. $\alpha \wedge \beta \in \mathbf{T}$ iff $\alpha \in \mathbf{T}$ and $\beta \in \mathbf{T}$.
4. If $\{\alpha, \alpha \to \beta\} \subseteq \mathbf{T}$, then $\beta \in \mathbf{T}$.
5. If $\{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l\alpha) \wedge \bigcirc^i\beta)) : i \in \mathbb{N}\} \subset \mathbf{T}$, then $\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta)) \in \mathbf{T}$.
6. If $\{\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \CIRCLE^l\alpha) \wedge (\bigwedge_{l=0}^{i} \neg\CIRCLE^l(\alpha \wedge \neg\alpha)) \wedge \CIRCLE^i\beta)) : i \in \mathbb{N}\} \subset \mathbf{T}$, then $\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta)) \in \mathbf{T}$.
7. If $\{\Phi_{k,\mathbf{B},\mathbf{X}}((\mathtt{E})^i\alpha) : i \in \mathbb{N}\} \subset \mathbf{T}$, then $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{C}\alpha) \in \mathbf{T}$.
8. If $r = \sup\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\alpha \in \mathbf{T}\}$, and $r \in [0,1]_{\mathbb{Q}}$, then $\mathtt{P}_{\geqslant r}\alpha \in \mathbf{T}$.
9. If $r = \sup\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\alpha \in \mathbf{T}\}$, then for every $s \in [0,1]_{\mathbb{Q}}$ such that $r > s$, $\mathtt{P}_{\geqslant s}\alpha \in \mathbf{T}$.
10. If $r = \sup\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{a,\geqslant s}\alpha \in \mathbf{T}\}$, and $r \in [0,1]_{\mathbb{Q}}$, then $\mathtt{P}_{a,\geqslant r}\alpha \in \mathbf{T}$.
11. If $r = \sup\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{a,\geqslant s}\alpha \in \mathbf{T}\}$, then for every $s \in [0,1]_{\mathbb{Q}}$ such that $r > s$, $\mathtt{P}_{a,\geqslant s}\alpha \in \mathbf{T}$.
12. There is a positive $i \in \mathbb{N}$ such that for every $\alpha \in \mathbf{For}$, $\CIRCLE^i(\alpha \wedge \neg\alpha) \in \mathbf{T}$, and for every $j \in \mathbb{N}$, $j < i$, $\CIRCLE^j(\alpha \wedge \neg\alpha) \notin \mathbf{T}$.
13. If for every $\alpha \in \mathbf{For}$, $\CIRCLE(\alpha \wedge \neg\alpha) \notin \mathbf{T}$, then $\mathbf{T}^{-\CIRCLE}$ is maximal consistent.
14. $\mathbf{T}^{-\bigcirc}$ is maximal consistent.
15. If for every $\alpha \in \mathbf{For}$, $\CIRCLE(\alpha \wedge \neg\alpha) \notin \mathbf{T}$, then $\mathbf{T} = (\mathbf{T}^{-\CIRCLE})^{-\bigcirc}$.
16. If $\mathtt{K}_a\alpha \notin \mathbf{T}$, then $\mathbf{T}^{-\mathtt{K}_a} \cup \{\neg\alpha\}$ is consistent.

PROOF. Let $\mathbf{T}$ be a maximal consistent set.
(1)–(4) The proofs are standard.
(5) It holds $\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1} \bigcirc^l\alpha) \wedge \bigcirc^i\beta))$ for every $i \in \mathbb{N}$, and by Rule R$\mathtt{U}$, $\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha\mathtt{U}\beta))$. Since $\mathbf{T}$ is deductively closed, $\Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha\mathtt{U}\beta)) \in \mathbf{T}$.
(6)–(7) can be proved using the same idea as in (5).
(8) If $r \in \{s \in [0,1]_{\mathbb{Q}} \mid \mathtt{P}_{\geqslant s}\alpha \in \mathbf{T}\}$, then the statement trivially holds. So, let us assume that $r \in [0,1]_{\mathbb{Q}}$ and $r \notin \{s \in [0,1]_{\mathbb{Q}} \mid \mathtt{P}_{\geqslant s}\alpha \in \mathbf{T}\}$. Then from

$\mathbf{T} \vdash \mathtt{P}_{\geqslant s}\alpha$ for every $s \in [0,1]_{\mathbb{Q}}$ such that $s < r$
$\mathbf{T} \vdash \Phi_{0,\alpha\vee\neg\alpha,\mathbf{X}}(\mathtt{P}_{\geqslant s}\alpha)$ for every $s \in [0,1]_{\mathbb{Q}}$ such that $s < r$
$\mathbf{T} \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{\geqslant r}\alpha)$, by Rule RGA, and
$\mathbf{T} \vdash \mathtt{P}_{\geqslant r}\alpha$,

since $\mathbf{T}$ is deductively closed, it follows that $\mathtt{P}_{\geqslant r}\alpha \in \mathbf{T}$.
(9) It follows by the properties of the supremum, and Lemma 5.18.
(10) and (11) can be proved in the same way as (8) and (9).
(12) First, note that if for any $\alpha \in \mathbf{For}$, $\CIRCLE^i(\alpha \wedge \neg\alpha) \in \mathbf{T}$, then for every $\beta \in \mathbf{For}$, $\CIRCLE^i(\beta \wedge \neg\beta) \in \mathbf{T}$:

$\mathbf{T} \vdash (\alpha \wedge \neg\alpha) \to (\beta \wedge \neg\beta)$
$\mathbf{T} \vdash \CIRCLE^i((\alpha \wedge \neg\alpha) \to (\beta \wedge \neg\beta))$, by R$\CIRCLE$N
$\mathbf{T} \vdash \CIRCLE^i(\beta \wedge \neg\beta)$, by A$\CIRCLE\!\to$ and MP,

and since $\mathbf{T}$ is deductively closed, $\CIRCLE^i(\beta \wedge \neg\beta) \in \mathbf{T}$. Thus, if for any $\alpha \in \mathbf{For}$ there is $i \in \mathbb{N}$ such that $\CIRCLE^i(\alpha \wedge \neg\alpha) \in \mathbf{T}$, there is also the minimal i which satisfies the statement.

Next, assume that for every $\alpha \in \mathbf{For}$ and for every positive $i \in \mathbb{N}$, $\CIRCLE^i(\alpha \wedge \neg\alpha) \notin \mathbf{T}$. Since $\mathbf{T}$ is maximal consistent, it means that for every $\alpha \in \mathbf{For}$, $\neg\CIRCLE^i(\alpha \wedge \neg\alpha) \in \mathbf{T}$. To make the following more readable, let

- β denote $\bullet(\alpha \wedge \neg\alpha)$ and
- $\gamma = \beta \rightarrow \beta$.

Then,

$\mathbf{T} \vdash \neg\bullet^i(\alpha \wedge \neg\alpha)$, for every positive $i \in \mathbb{N}$, i.e.,
$\mathbf{T} \vdash \neg\bullet^i\beta$, for every positive $i \in \mathbb{N}$
$\mathbf{T} \vdash \neg(\bigwedge_{l=0}^{i-1}\bullet^l\gamma) \vee \neg(\bigwedge_{l=0}^{i}\neg\bullet^l(\gamma \wedge \neg\gamma)) \vee \neg\bullet^i\beta$, for every positive $i \in \mathbb{N}$
$\mathbf{T} \vdash \Phi_{0,\{\delta\vee\neg\delta\},\mathbf{X}}(\neg((\bigwedge_{l=0}^{i-1}\bullet^l\gamma) \wedge (\bigwedge_{l=0}^{i}\neg\bullet^l(\gamma \wedge \neg\gamma)) \wedge \bullet^i\beta)$, for every positive $i \in \mathbb{N}$, and any δ
$\mathbf{T} \vdash \Phi_{0,\{\delta\vee\neg\delta\},\mathbf{X}}(\neg(\gamma \mathtt{S} \beta))$, by R$\mathtt{S}$ for any δ
$\mathbf{T} \vdash \neg(\gamma \mathtt{S} \beta)$
$\mathbf{T} \vdash \neg((\beta \rightarrow \beta)\mathtt{S}\beta)$
$\mathbf{T} \vdash \neg\mathtt{P}\beta$, by the definition of $\mathtt{P}$, i.e.,
$\mathbf{T} \vdash \neg\mathtt{P}\bullet(\alpha \wedge \neg\alpha)$,

which contradicts consistency of $\mathbf{T}$, since $\mathtt{P}\bullet(\alpha \wedge \neg\alpha)$ is the axiom A$\mathtt{P}\bullet$. Thus, there is a unique $i \in \mathbb{N}$ which satisfies the statement.

(13) If $\mathbf{T}^{-\bullet} = \{\alpha : \bullet\alpha \in \mathbf{T}\}$ is not consistent, then

$\mathbf{T}^{-\bullet} \vdash \alpha \wedge \neg\alpha$, for every formula α;
$\bullet\mathbf{T}^{-\bullet} \vdash \bullet(\alpha \wedge \neg\alpha)$, by Theorem 5.2; and
$\mathbf{T} \vdash \bullet(\alpha \wedge \neg\alpha)$, since $\bullet\mathbf{T}^{-\bullet} = \{\bullet\beta : \beta \in \mathbf{T}^{-\bullet}\} = \{\bullet\beta : \bullet\beta \in \mathbf{T}\} \subset \mathbf{T}$,

which contradicts consistency of $\mathbf{T}$, since by the assumption $\mathbf{T}$ does not contain formulas of the form $\bullet(\alpha \wedge \neg\alpha)$. If $\mathbf{T}^{-\bullet}$ is not maximal, then there is $\alpha \in \mathbf{For}$ such that $\alpha \notin \mathbf{T}^{-\bullet}$ and $\alpha \notin \mathbf{T}^{-\bullet}$. It means that

- $\bullet\alpha \notin \mathbf{T}$;
- $\bullet\neg\alpha \notin \mathbf{T}$; and
- $\neg\bullet\alpha \notin \mathbf{T}$, using Axiom A$\bullet\neg$;

which contradicts maximality of $\mathbf{T}$. Thus, $\mathbf{T}^{-\bullet}$ is maximal consistent.

(14) can be proved using the same ideas as (13).

(15) Since for every $\gamma \in \mathbf{For}$, $\bullet(\gamma \wedge \neg\gamma) \notin \mathbf{T}$, the following hold:

- $\bigcirc\bullet\alpha \in \mathbf{T}$ iff $\bullet\bigcirc\alpha \in \mathbf{T}$, by the axioms A$\bigcirc\bullet$C$_1$ and A$\bigcirc\bullet$C$_2$ and
- $\bullet\bigcirc\alpha \in \mathbf{T}$ iff $\alpha \in \mathbf{T}$, by Axiom A$\bigcirc\bullet$.

So $\alpha \in \mathbf{T}$ iff $\bullet\bigcirc\alpha \in \mathbf{T}$ iff $\bigcirc\alpha \in \mathbf{T}^{-\bullet} = \{\delta : \bullet\delta \in \mathbf{T}\}$ iff $\alpha \in (\mathbf{T}^{-\bullet})^{-\bigcirc} = \{\delta : \bigcirc\delta \in \mathbf{T}^{-\bullet}\}$. It means that $\mathbf{T} = (\mathbf{T}^{-\bullet})^{-\bigcirc}$.

(16) If $\mathbf{T}^{-\mathtt{K}_a} \cup \{\neg\alpha\}$ if it is not consistent, then $\mathbf{T}^{-\mathtt{K}_a} \cup \{\neg\alpha\} \vdash \gamma \wedge \neg\gamma$ and$\mathbf{T}^{-\mathtt{K}_a} \vdash \alpha$. Then, by Theorem 5.3, $\mathtt{K}_a\mathbf{T}^{-\mathtt{K}_a} \vdash \mathtt{K}_a\beta$. Since $\mathbf{T}$ is maximal consistent and deductively closed, and $\mathbf{T} \supset \mathtt{K}_a\mathbf{T}^{-\mathtt{K}_a}$, it implies a contradiction. □

A.3 Canonical model

THEOREM 6 (Lindenbaum's theorem).

Every $\mathtt{Ax}_{\mathbf{PTEL}}$-consistent set of formulas $\mathbf{T}$ can be extended to a maximal $\mathtt{Ax}_{\mathbf{PTEL}}$-consistent set $\mathbf{T}^*$.

PROOF. The proof will be based on the following ideas:

- a procedure for extending $\mathbf{T}$ will be described so that in each step a consistent superset of $\mathbf{T}$ is obtained (by adding new formulas to supersets of $\mathbf{T}$);
- the procedure guarantees that, if a formula which is the negation of a conclusion of an infinitary rule is added to a superset of $\mathbf{T}$, then a witness (the negation of a premise of the rule) is also added to the superset;
- it will be shown that the union of all those extensions:
  - contains exactly one of α, $\neg\alpha$ for every $\alpha \in \mathbf{For}$, and
  - is a deductively closed sets,

  so that the union is a maximal consistent extension of $\mathbf{T}$.

Let $\{\alpha_i : i \in \mathbb{N}\}$ be a list of all **For**-formulas. We define a sequence of theories $\{\mathbf{T}_i : i \in \mathbb{N}\}$ and a theory $\mathbf{T}^*$ as follows:

1. $\mathbf{T}_0 = \mathbf{T}$.
2. For every $i \in \mathbb{N}$:
   a. If $\mathbf{T}_i \cup \{\alpha_i\}$ is consistent, then $\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\alpha_i\}$.
   b. If $\mathbf{T}_i \cup \{\alpha_i\}$ is inconsistent, then
      i. If $\alpha_i = \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{U} \beta))$, then
      $$\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i, \neg\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{j-1} \bigcirc^l \alpha) \wedge \bigcirc^j \beta))\}$$
      for some $j \in \mathbb{N}$ so that $\mathbf{T}_{i+1}$ is consistent.
      ii. If $\alpha_i = \Phi_{k,\mathbf{B},\mathbf{X}}(\neg(\alpha \mathtt{S} \beta))$, then
      $$\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i, \neg\Phi_{k,\mathbf{B},\mathbf{X}}(\neg((\bigwedge_{l=0}^{j-1} \bullet^l \alpha) \wedge (\bigwedge_{l=0}^{j} \neg\bullet^l(\alpha \wedge \neg\alpha)) \wedge \bullet^j \beta))\}$$
      for some $j \in \mathbb{N}$ so that $\mathbf{T}_{i+1}$ is consistent.
      iii. If $\alpha_i = \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{C}\alpha)$, then
      $$\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i, \neg\Phi_{k,\mathbf{B},\mathbf{X}}((\mathtt{E})^j \alpha)\}$$
      for some $j \in \mathbb{N}$ so that $\mathbf{T}_{i+1}$ is consistent.
      iv. If $\alpha_i = \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{\geqslant r}\alpha)$, then
      $$\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i, \neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{\geqslant r - \frac{1}{j}}\alpha)\}$$
      for some $j \in \mathbb{N}$ so that $\mathbf{T}_{i+1}$ is consistent.
      v. If $\alpha_i = \Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r}\alpha)$, then
      $$\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i, \neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathtt{P}_{a,\geqslant r - \frac{1}{j}}\alpha)\}$$
      for some $j \in \mathbb{N}$ so that $\mathbf{T}_{i+1}$ is consistent.
      vi. Otherwise, $\mathbf{T}_{i+1} = \mathbf{T}_i \cup \{\neg\alpha_i\}$.
3. $\mathbf{T}^* = \cup_{i \in \mathbb{N}} \mathbf{T}_i$.

First, we prove that all theories $\mathbf{T}_i$ are consistent. Note that this trivially holds for theories obtained by the steps 1, 2a and 2(b)vi of the above construction. Theorem 14 guarantees that the same holds for the steps 2(b)i–v.

Second, we show that $\mathbf{T}^*$ is a maximal consistent set of formulas. We start by noticing that the steps 2a and 2b of above construction guarantee that for every $\alpha \in \mathbf{For}$, at least one of α and $\neg\alpha$ belongs to $\mathbf{T}^*$. On the other hand, it is not possible that both α and $\neg\alpha$ are in $\mathbf{T}^*$. Otherwise, there would exist j and k such that α and $\neg\alpha$ are α_j, and α_k, respectively, from the above enumeration of all **For**-formulas, and for $i = \max\{j,k\}$, it would be $\alpha, \neg\alpha \in \mathbf{T}_{i+1}$, which contradicts consistency of $\mathbf{T}_{i+1}$.

In the last step, using transfinite induction on the length of a proof, we show that $\mathbf{T}^*$ is deductively closed. Let $\mathbf{T}^* \vdash \gamma$. Let γ be obtained from $\mathbf{T}^*$ by an application of one of the finitary rules. By the induction hypothesis, there is $l \in \mathbb{N}$ such that all premisses of the rule belong to $\mathbf{T}_l$. Let for some j and k, $\gamma = \alpha_j$ and $\neg\gamma = \alpha_k$ in the above enumeration of all **For**-formulas, and $i \geqslant \max\{j,k,l\}$. If $\neg\gamma \in \mathbf{T}_{i+1}$, then $\mathbf{T}_{i+1} \vdash \gamma$, and $\mathbf{T}_{i+1} \vdash \neg\gamma$, which contradicts consistency of $\mathbf{T}_{i+1}$. Finally, let γ be a consequence of one of the infinitary rules RU, RS, RC, RGA and RA. Let us consider Rule RA, while the other cases can be proved similarly. So, let $\gamma = \Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r}\alpha)$ be obtained by an application of Rule RA:

$\mathbf{T}^* \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{m}}\alpha)$, for every $m \in \mathbb{N}$, $m \geqslant \frac{1}{r}$, and

$\mathbf{T}^* \vdash \Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r}\alpha)$, by RA.

By the induction hypothesis, every $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{m}}\alpha) \in \mathbf{T}^*$. If $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r}\alpha) \notin \mathbf{T}^*$, let $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r}\alpha) = \alpha_i$ in the above enumeration of all **For**-formulas. By the step 2(b)v of the above construction, there is $j \in \mathbb{N}$ so that $\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) \in \mathbf{T}_{i+1}$. Let $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) = \alpha_k$ in the above enumeration of all **For**-formulas. By the induction hypothesis $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) \in \mathbf{T}^*$, so $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) \in \mathbf{T}_{k+1}$. Then we have

- $\neg\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) \in \mathbf{T}_{i+1}$ and
- $\Phi_{k,\mathbf{B},\mathbf{X}}(\mathrm{P}_{a,\geqslant r-\frac{1}{j}}\alpha) \in \mathbf{T}_{k+1}$,

which contradicts consistency of $\mathbf{T}_l$, where $l = \max\{i+1, k+1\}$.

Since $\mathbf{T}^*$ is deductively closed and does not contain all formulas, it is consistent. As it is noted above, for each $\alpha \in \mathbf{For}$ exactly one of α and $\neg\alpha$ belongs to $\mathbf{T}^*$. Thus, $\mathbf{T}^*$ is a maximal consistent set. □

LEMMA 7

Let the canonical model $\mathcal{M}^* = \langle \mathbf{R}^*, \mathcal{A}^*, \mathcal{K}^*, \mathcal{P}^* \rangle$ be defined as in Definition 8. Then for every possible world $(r^{\mathbf{S}}, n)$ and for every agent $a \in \mathbb{A}$:

1. $H^{*,(r^{\mathbf{S}},n)}$ is an algebra of sets;
2. $\mu^{*,(r^{\mathbf{S}},n)}$ is a finitely-additive probability measure;
3. $H_a^{*,(r^{\mathbf{S}},n)}$ is an algebra of sets; and
4. $\mu_a^{*,(r^{\mathbf{S}},n)}$ is a finitely-additive probability measure.

PROOF. To make this paper self contained we present the adapted proofs from [29, 32] for the statements (1) and (2), and the same ideas can be used for the statements (3) and (4).

(1) For every possible world $(r^{\mathbf{S}}, n)$, the family $H^{*,(r^{\mathbf{S}},n)}$ is an algebra of sets since

- by Definition 8, $\mathbf{R}^* = [\![\bullet(\alpha \wedge \neg\alpha)]\!]^{(r^{\mathbf{S}},n)}$, thus $\mathbf{R}^* \in H^{*,(r^{\mathbf{S}},n)}$;
- if $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} \in H^{*,(r^{\mathbf{S}},n)}$, then $[\![\neg\alpha]\!]^{(r^{\mathbf{S}},n)}$ is its complement which also belongs to $H^{*,(r^{\mathbf{S}},n)}$; and

- if $[\![\alpha_1]\!]^{(r^{\mathbf{S}},n)}, \ldots, [\![\alpha_l]\!]^{(r^{\mathbf{S}},n)} \in H^{*,(r^{\mathbf{S}},n)}$, then $[\![\alpha_1]\!]^{(r^{\mathbf{S}},n)} \cup \ldots \cup [\![\alpha_l]\!]^{(r^{\mathbf{S}},n)} = [\![\alpha_1 \vee \ldots \vee \alpha_l]\!]^{(r^{\mathbf{S}},n)}$ belongs to $H^{*,(r^{\mathbf{S}},n)}$.

(2) To prove this, we show that for every possible world $(r^{\mathbf{S}}, n)$, $\mu^{*,(r^{\mathbf{S}},n)}$ is a well-defined, nonnegative, bounded by 1 and finitely additive function.

From $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} = [\![\beta]\!]^{(r^{\mathbf{S}},n)}$ we have that $\vdash \alpha \leftrightarrow \beta$. By Lemma 5.15 it follows that $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) = \mu^{*,(r^{\mathbf{S}},n)}([\![\beta]\!]^{(r^{\mathbf{S}},n)})$. Thus, $\mu^{*,(r^{\mathbf{S}},n)}$ is well defined.

Axiom AGP1 guarantees that $P_{\geq 0}\alpha \in (r^{\mathbf{S}}, n)$, and $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) \geq 0$, for every $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} \in H^{*,(r^{\mathbf{S}},n)}$.

Since $\mathbf{R}^* = [\![\bullet(\alpha \wedge \neg\alpha)]\!]^{(r^{\mathbf{S}},n)}$ and by Axiom AGP$\bullet$, $\mathtt{P}_{\geqslant 1}\bullet(\alpha \wedge \neg\alpha) \in (r^{\mathbf{S}}, n)$, it follows that $\mu^{*,(r^{\mathbf{S}},n)}(\mathbf{R}^*) = 1$. Also, note that $[\![\bullet(\alpha \wedge \neg\alpha)]\!]^{(r^{\mathbf{S}},n)} = [\![\alpha \vee \neg\alpha]\!]^{(r^{\mathbf{S}},n)}$ and $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha \vee \neg\alpha]\!]^{(r^{\mathbf{S}},n)}) = 1$ On the other hand, $\emptyset = [\![\alpha \wedge \neg\alpha]\!]^{(r^{\mathbf{S}},n)}$ and $\mu^{*,(r^{\mathbf{S}},n)}(\emptyset) \geq 0$. From $\mathtt{P}_{\geqslant 1}(\alpha \vee \neg\alpha) \in (r^{\mathbf{S}}, n)$, by the definitions of $\mathtt{P}_{<s}$ and $\mathtt{P}_{\leqslant s}$ and Axiom AGP2, we have that $\neg\mathtt{P}_{<1}(\alpha \vee \neg\alpha) \in (r^{\mathbf{S}}, n)$, $\neg\mathtt{P}_{\leqslant r}(\alpha \vee \neg\alpha) \in (r^{\mathbf{S}}, n)$ for $r < 1$, and $\neg\mathtt{P}_{\geqslant 1-r}(\alpha \wedge \neg\alpha) \in (r^{\mathbf{S}}, n)$ for $r < 1$. Thus, $\sup_s\{\mathtt{P}_{\geqslant s}(\alpha \wedge \neg\alpha) \in (r^{\mathbf{S}}, n)\} = 0$, and $\mu^{*,(r^{\mathbf{S}},n)}(\emptyset) = 0$.

Let $r = \mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) = \sup_s\{\mathtt{P}_{\geqslant s}\alpha \in (r^{\mathbf{S}}, n)\}$. If $r = 1$, by Lemma 6.10 $\mathtt{P}_{\geqslant 1}\alpha \in (r^{\mathbf{S}}, n)$. It means that $(r^{\mathbf{S}}, n)$ contains $\neg\mathtt{P}_{>0}\neg\alpha$ (i.e., $\mathtt{P}_{\leqslant 0}\neg\alpha$, $\mathtt{P}_{\geqslant 1}\alpha$). By Axiom AGP2 there is no $s > 0$ such that $\mathtt{P}_{\geqslant s}\neg\alpha \in (r^{\mathbf{S}}, n)$. Thus, $\mu^{*,(r^{\mathbf{S}},n)}([\![\neg\alpha]\!]^{(r^{\mathbf{S}},n)})) = 0$. On the other hand, if $r < 1$, then, since $\neg\mathtt{P}_{\geqslant r'}\alpha = \mathtt{P}_{<r'}\alpha$, for every $r' > r$, $r' \in [0, 1]_{\mathbb{Q}}$, we have $\mathtt{P}_{<r'}\alpha \in (r^{\mathbf{S}}, n)$. It follows by Axiom AGP3 that $\mathtt{P}_{\leqslant r'}\alpha$, $\mathtt{P}_{\geqslant 1-r'}\neg\alpha \in (r^{\mathbf{S}}, n)$. If there is an $r'' < r$ such that $r'' \in [0, 1]_{\mathbb{Q}}$ and $\mathtt{P}_{\geqslant 1-r''}\neg\alpha \in (r^{\mathbf{S}}, n)$, then a contradiction $\neg\mathtt{P}_{>r''}\alpha \in (r^{\mathbf{S}}, n)$ follows. So, $\sup_s\{\mathtt{P}_{\geqslant s}(\neg\alpha) \in (r^{\mathbf{S}}, n)\} = 1 - \sup_s\{\mathtt{P}_{\geqslant s}\alpha \in (r^{\mathbf{S}}, n)\}$, and $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)})) = 1 - \mu^{*,(r^{\mathbf{S}},n)}([\![\neg\alpha]\!]^{(r^{\mathbf{S}},n)}))$.

Let $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} \cap [\![\beta]\!]^{(r^{\mathbf{S}},n)} = \emptyset$, $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) = r$ and $\mu^{*,(r^{\mathbf{S}},n)}([\![\beta]\!]^{(r^{\mathbf{S}},n)}) = s$. Since $[\![\beta]\!]^{(r^{\mathbf{S}},n)} \subset [\![\neg\alpha]\!]^{(r^{\mathbf{S}},n)}$, the previous statements imply that $r + s \leqslant r + (1 - r) = 1$. Let $r > 0$, and $s > 0$. By the well-known properties of the supremum, for all $r', s' \in [0, 1]_{\mathbb{Q}}$ such that $r' < r$ and $s' < s$, we have $\mathtt{P}_{\geqslant r'}\alpha$, $\mathtt{P}_{\geqslant s'}\beta \in (r^{\mathbf{S}}, n)$. Then, Axiom AGP5 implies that $\mathtt{P}_{\geqslant r'+s'}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)$. It means that $r+s \leqslant t_0 = \sup_t\{\mathtt{P}_{\geqslant t}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)\}$. If $r+s = 1$, then trivially holds that $r+s = t_0$ and $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)} \cup [\![\beta]\!]^{(r^{\mathbf{S}},n)}) = \mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) + \mu^{*,(r^{\mathbf{S}},n)}([\![\beta]\!]^{(r^{\mathbf{S}},n)})$. Otherwise, assume that $r+s < 1$ and $r+s < t_0$. Then for every $t' \in [0, 1]_{\mathbb{Q}} \cap (r+s, t_0)$, $\mathtt{P}_{\geqslant t'}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)$, and it is possible to choose $r'', s'' \in [0, 1]_{\mathbb{Q}}$ such that $r'' > r$, $s'' > s$, $r'' + s'' = t' \leqslant 1$, $\neg\mathtt{P}_{\geqslant r''}\alpha$, $\mathtt{P}_{<r''}\alpha \in (r^{\mathbf{S}}, n)$, and $\neg\mathtt{P}_{\geqslant s''}\beta$, $\mathtt{P}_{<s''}\beta \in (r^{\mathbf{S}}, n)$. It implies a contradiction since by Axiom AGP3, $\mathtt{P}_{\leqslant r''}\alpha \in (r^{\mathbf{S}}, n)$, by Axiom AGP5, $\mathtt{P}_{<r''+s''}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)$, $\neg\mathtt{P}_{\geqslant r''+s''}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)$, and $\neg\mathtt{P}_{\geqslant t'}(\alpha \vee \beta) \in (r^{\mathbf{S}}, n)$. Hence, $r + s = t_0$ and $\mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)} \cup [\![\beta]\!]^{(r^{\mathbf{S}},n)}) = \mu^{*,(r^{\mathbf{S}},n)}([\![\alpha]\!]^{(r^{\mathbf{S}},n)}) + \mu^{*,(r^{\mathbf{S}},n)}([\![\beta]\!]^{(r^{\mathbf{S}},n)})$. Otherwise, suppose that $r = 0$ or $s = 0$. Then we can reason as above, with the only exception that $r' = 0$ or $s' = 0$.

This proves that each $\mu^{*,(r^{\mathbf{S}},n)}$ is a finitely additive probability measure. □

THEOREM 7
The canonical model $\mathcal{M}^*$ is a $\mathtt{Mod}$-model.

PROOF. We have to prove that

- $\mathcal{A}^*$, $\mathcal{K}^*$ and $\mathcal{P}^*$ are properly defined; and
- for every α, $[\![\alpha]\!]^{(r^{\mathbf{S}},n)} = [\alpha]^{(r^{\mathbf{S}},n)}$, and $[\![\alpha]\!]_a^{(r^{\mathbf{S}},n)} = [\alpha]_a^{(r^{\mathbf{S}},n)}$.

Concerning the first item, we note than by Definition 8, $a \in \mathcal{A}^*((r^{\mathbf{S}},n))$ iff $A_a \in r^{\mathbf{S}}(n)$, so $\mathcal{A}^*$ satisfies the condition from Definition 2. Regarding $\mathcal{K}^*$ note that if $a \notin \mathcal{A}^*((r^{\mathbf{S}},n))$, then $(r^{\mathbf{S}},n)\mathcal{K}^*_a(r',n')$ is false for all (r',n'). On the other hand, the axioms AKS and AKT guarantee that every $\mathcal{K}^*_a$ is symmetric and transitive. Furthermore, for every $(r^{\mathbf{S}},n)$, if $a \in \mathcal{A}^*((r^{\mathbf{S}},n))$ we have that $A_a \in \mathbf{S}_n$ and using Axiom AKR also that $\mathtt{K}_a\alpha \to \alpha \in \mathbf{S}_n$. It follows that $\mathbf{S}_n^{-\mathtt{K}_a} \subset \mathbf{S}_n$ and $(r^{\mathbf{S}},n)\mathcal{K}^*_a(r^{\mathbf{S}},n)$. Thus, $\mathcal{K}^*$ also satisfies the corresponding conditions from Definition 2. Finally, Lemma 7 guarantees that for every possible world $(r^{\mathbf{S}},n)$ and for every agent $a \in \mathbb{A}$, $H^{*,(r^{\mathbf{S}},n)}$ and $H_a^{*,(r^{\mathbf{S}},n)}$ are algebras of sets, while $\mu^{*,(r^{\mathbf{S}},n)}$ and $\mu_a^{*,(r^{\mathbf{S}},n)}$ are finitely-additive probability measures.

The second item means that we have to prove that belonging of formulas to a maximal consistent set has the same meaning as satisfiability of formulas in the corresponding possible world. Recall that

- $[\alpha]^{(r^{\mathbf{S}},n)}$ denotes $\{r^{\mathbf{S}'} \in \mathbf{R}^* : (r^{\mathbf{S}'},0) \models \alpha\}$;
- $[\![\alpha]\!]^{(r^{\mathbf{S}},n)}$ denotes $\{r^{\mathbf{S}} \in \mathbf{R}^* : \alpha \in \mathbf{S}_0\}$;
- $[\alpha]_a^{(r^{\mathbf{S}},n)}$ denotes $\{(r^{\mathbf{S'}},n') \in \mathbf{W}_a^{*,(r^{\mathbf{S}},n)} : (r^{\mathbf{S'}},n') \models \alpha\}$; and
- $[\![\alpha]\!]_a^{(r^{\mathbf{S}},n)}$ denotes $\{(r^{\mathbf{S'}},n') \in \mathbf{W}_a^{*,(r^{\mathbf{S}},n)} : \alpha \in \text{'}_{n'}\}$,

and that every $\mathbf{S}_n$ is maximal and consistent. We will use induction on complexity of α to prove the statements and analyze some of the cases (for propositional letters, and formulas of the forms $\bullet\beta$, $\beta\mathtt{S}\gamma$, $\mathtt{C}\beta$ and $\mathtt{P}_{\geqslant s}\beta$) leaving the rest to readers (for formulas of the forms $\neg\beta$, $\beta\wedge\gamma$, $\bigcirc\beta$, $\beta\mathtt{U}\gamma$, $\mathtt{K}_a\beta$ and $\mathtt{P}_{a,\geqslant s}\beta$).

Let $\alpha \in \mathbf{Var}$, e.g., $\alpha = p$. Then,

- $r^{\mathbf{S'}} \in [\![p]\!]^{(r^{\mathbf{S}},n)}$ iff $p \in \mathbf{S'}_0$ iff $p \in r^{\mathbf{S'}}(0)$ iff $(r^{\mathbf{S'}},0) \models p$ iff $r^{\mathbf{S'}} \in [p]^{(r^{\mathbf{S}},n)}$ and
- $(r^{\mathbf{S'}},n') \in [\![p]\!]_a^{(r^{\mathbf{S}},n)}$ iff $p \in \mathbf{S'}_{n'}$ iff $p \in r^{\mathbf{S'}}(n')$ iff $(r^{\mathbf{S'}},n') \models p$ iff $(r^{\mathbf{S'}},n') \in [p]_a^{(r^{\mathbf{S}},n)}$.

Thus, $[\![p]\!]^{(r^{\mathbf{S}},n)} = [p]^{(r^{\mathbf{S}},n)}$ and $[\![p]\!]_a^{(r^{\mathbf{S}},n)} = [p]_a^{(r^{\mathbf{S}},n)}$.

Assume $\alpha = \bullet\beta$. Let us consider the case of sets of the forms $[\![\bullet\beta]\!]^{(r^{\mathbf{S}},n)}$ and $[\bullet\beta]^{(r^{\mathbf{S}},n)}$. We want to show that $r^{\mathbf{S'}} \in [\![\bullet\beta]\!]^{(r^{\mathbf{S}},n)}$ iff $r^{\mathbf{S'}} \in [\bullet\beta]^{(r^{\mathbf{S}},n)}$. It follows from the facts:

- Definition 3 guarantees that $(r^{\mathbf{S'}},0) \models \bullet\beta$, i.e., every $r^{\mathbf{S'}} \in [\bullet\beta]^{(r^{\mathbf{S}},n)}$; and
- the construction of the canonical model $\mathcal{M}^*$ guarantees that $\bullet\beta \in \mathbf{S'}_0$, i.e., every $r^{\mathbf{S'}} \in [\![\bullet\beta]\!]^{(r^{\mathbf{S}},n)}$.

Next, let us consider the case of sets of the forms $[\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)}$ and $[\bullet\beta]_a^{(r^{\mathbf{S}},n)}$. We want to show that $(r^{\mathbf{S'}},n') \in [\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)}$ iff $(r^{\mathbf{S'}},n') \in [\bullet\beta]_a^{(r^{\mathbf{S}},n)}$. We distinguish two cases concerning n':

- Let $n' = 0$. If $(r^{\mathbf{S'}},0) \in [\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)}$, by the definition of the satisfiability relation, for every $\beta \in \mathbf{For}$, $(r^{\mathbf{S'}},0) \models \bullet\beta$, so $(r^{\mathbf{S'}},0) \in [\bullet\beta]_a^{(r^{\mathbf{S}},n)}$. For the other direction, let $(r^{\mathbf{S'}},0) \in [\bullet\beta]_a^{(r^{\mathbf{S}},n)}$. By the definition of $\mathcal{M}^*$, for every $\beta \in \mathbf{For}$, $\bullet\beta \in \mathbf{S'}_0$, thus $(r^{\mathbf{S'}},0) \in [\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)}$.
- Let $n' > 0$. Then,

  $(r^{\mathbf{S'}},n') \in [\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)}$, i.e., $\bullet\beta \in \mathbf{S'}_{n'}$ iff
  $\bigcirc\bullet\beta \in \mathbf{S'}_{n'-1}$ (by the definition of sequences of sets $\mathbf{S}_n$) iff
  $\beta \in \mathbf{S'}_{n'-1}$ (using Axiom A$\bigcirc\bullet$) iff
  $(r^{\mathbf{S'}},n'-1) \models \beta$ iff
  $(r^{\mathbf{S'}},n') \models \bullet\beta$ iff

$(r^{\mathbf{S'}}, n') \in [\bullet\beta]_a^{(r^{\mathbf{S}},n)}$.

Thus, $[\![\bullet\beta]\!]^{(r^{\mathbf{S}},n)} = [\bullet\beta]^{(r^{\mathbf{S}},n)}$, and $[\![\bullet\beta]\!]_a^{(r^{\mathbf{S}},n)} = [\bullet\beta]_a^{(r^{\mathbf{S}},n)}$.
Let $\alpha = \beta \mathtt{S} \gamma$.
Assume that $r^{\mathbf{S'}} \in [\![\beta \mathtt{S} \gamma]\!]^{(r^{\mathbf{S}},n)}$, i.e., $\beta \mathtt{S} \gamma \in \mathbf{S'}_0$. Then by Lemma 5.12 it follows that $\bullet(\beta \wedge \neg\beta) \in \mathbf{S'}_0$, and $\gamma \in \mathbf{S'}_0$. Using the induction hypothesis we have

- $(r^{\mathbf{S'}}, 0) \models \gamma$;
- $(r^{\mathbf{S'}}, 0) \models \beta \mathtt{S} \gamma$; and
- $r^{\mathbf{S'}} \in [\beta \mathtt{S} \gamma]^{(r^{\mathbf{S}},n)}$.

For the other direction, assume that $r^{\mathbf{S'}} \in [\beta \mathtt{S} \gamma]^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}}, 0) \models \beta \mathtt{S} \gamma$. Then,

- $(r^{\mathbf{S'}}, 0) \models \gamma$;
- by the induction hypothesis: $\gamma \in \mathbf{S'}_0$, $r^{\mathbf{S'}} \in [\![\gamma]\!]^{(r^{\mathbf{S}},n)}$; and
- since $\mathbf{S'}_0$ is maximal consistent, using Axiom A$\mathtt{S}\bullet$ it follows that $\beta \mathtt{S} \gamma \in \mathbf{S'}_0$ and $r^{\mathbf{S'}} \in [\![\beta \mathtt{S} \gamma]\!]^{(r^{\mathbf{S}},n)}$.

Assume that $(r^{\mathbf{S'}}, n') \in [\![\beta \mathtt{S} \gamma]\!]_a^{(r^{\mathbf{S}},n)}$, i.e., $\beta \mathtt{S} \gamma \in \mathbf{S'}_{n'}$. We distinguish two cases:

- Let $n' = 0$. Then also $\bullet(\beta \wedge \neg\beta) \in \mathbf{S'}_0$, and by Lemma 5.12, $\gamma \in \mathbf{S'}_0$ and using the induction hypothesis we have
  $(r^{\mathbf{S'}}, 0) \models \gamma$;
  $(r^{\mathbf{S'}}, 0) \models \beta \mathtt{S} \gamma$; and
  $(r^{\mathbf{S'}}, 0) \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$.
- Let $n' > 0$. Then, if $\gamma \in \mathbf{S'}_{n'}$, then using the induction hypothesis as above, we have that $(r^{\mathbf{S'}}, n') \models \gamma$, $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$, and thus $(r^{\mathbf{S'}}, n') \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$. Next, suppose that $\gamma \notin \mathbf{S'}_{n'}$. Using Lemma 5.12, and the the assumption $n' > 0$ we have
  - $\neg\bullet(\beta \wedge \neg\beta) \in \mathbf{S'}_{n'}$;
  - $\beta \wedge \bullet(\beta \mathtt{S} \gamma) \in \mathbf{S'}_{n'}$;
  - $\beta \in \mathbf{S'}_{n'}$;
  - $\bullet(\beta \mathtt{S} \gamma) \in \mathbf{S'}_{n'}$;
  - $\bigcirc\bullet(\beta \mathtt{S} \gamma) \in \mathbf{S'}_{n'-1}$, by the construction of sets S_i;
  - $\beta \mathtt{S} \gamma \in \mathbf{S'}_{n'-1}$, using Axiom A$\bigcirc\bullet$.
- Hence, if $\gamma \notin \mathbf{S'}_{n'}$, then $\beta \in \mathbf{S'}_{n'}$ and $\beta \mathtt{S} \gamma \in \mathbf{S'}_{n'-1}$. Since $\beta \in \mathbf{S'}_{n'}$, by the induction hypothesis we have $(r^{\mathbf{S'}}, n') \models \beta$. Now, if $n' - 1 = 0$, similarly as above $\gamma \in \mathbf{S'}_{n'-1}$, $(r^{\mathbf{S'}}, n' - 1) \models \gamma$, $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$, and $(r^{\mathbf{S'}}, n') \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$. On the other hand, if $n' - 1 > 0$, we can conclude as above:
  - if $\gamma \in \mathbf{S'}_{n'-1}$, then $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$, and $(r^{\mathbf{S'}}, n') \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$;
  - if $\gamma \notin \mathbf{S'}_{n'-1}$, then $(r^{\mathbf{S'}}, n' - 1) \models \beta$, and $\beta \mathtt{S} \gamma \in \mathbf{S'}_{n'-2}$.
- Finally, since n' is finite, in a finite number of steps we obtain that
  - for some integer $j \in (0, n')$, $(r^{\mathbf{S'}}, j) \models \gamma$ and for every integer $k \in (j, n']$, $(r^{\mathbf{S'}}, k) \models \beta$, which implies $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$; or
  - we will reach the possible world $(r^{\mathbf{S'}}, 0)$, and reasoning as above conclude that $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$.

- Thus, $(r^{\mathbf{S'}}, n') \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$. For the other direction, assume that $(r^{\mathbf{S'}}, n') \in [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}}, n') \models \beta \mathtt{S} \gamma$. Now,
  - If $n' = 0$, then $(r^{\mathbf{S'}}, 0) \models \gamma$, and by the induction hypothesis $\gamma \in \mathbf{S'}_0$, $(r^{\mathbf{S'}}, 0) \in [\![\gamma]\!]_a^{(r^{\mathbf{S}},n)}$. Since $\mathbf{S'}_0$ is maximal consistent, using Axiom A$\mathtt{S}\bullet$ it follows that $(r^{\mathbf{S'}}, 0) \in [\![\beta \mathtt{S} \gamma]\!]_a^{(r^{\mathbf{S}},n)}$.
  - If $n' > 0$, then there is an integer $j \in [0, n']$ such that $(r^{\mathbf{S'}}, j) \models \gamma$, and for every integer k, such that $j < k \leqslant n'$, $(r^{\mathbf{S'}}, k) \models \beta$. Using the induction hypothesis and by the construction of the canonical model, it follows that $\bullet^{n'-j}\gamma \in \mathbf{S'}_{n'}$, and that for every integer $k \in (j, n']$, $\bullet^{n'-k}\beta \in \mathbf{S'}_{n'}$. Then, using Lemma 5.13 we have that $\beta \mathtt{S} \gamma \in \mathbf{S'}_{n'}$, i.e., that $(r^{\mathbf{S'}}, n') \in [\![\beta \mathtt{S} \gamma]\!]_a^{(r^{\mathbf{S}},n)}$.

Thus, $[\![\beta \mathtt{S} \gamma]\!]^{(r^{\mathbf{S}},n)} = [\beta \mathtt{S} \gamma]^{(r^{\mathbf{S}},n)}$, and $[\![\beta \mathtt{S} \gamma]\!]_a^{(r^{\mathbf{S}},n)} = [\beta \mathtt{S} \gamma]_a^{(r^{\mathbf{S}},n)}$.

Let $\alpha = \mathtt{C}\beta$.

Assume that $r^{\mathbf{S'}} \in [\![\mathtt{C}\beta]\!]^{(r^{\mathbf{S}},n)}$, i.e., $\mathtt{C}\beta \in \mathbf{S'}_0$. Then $\mathtt{E}^m\beta \in \mathbf{S'}_0$, for every $m \in \mathbb{N}$, by Axiom A$\mathtt{CE}$. Since $\mathtt{E}^m$ is a conjunction of formulas of the form $\mathtt{K}_{a_m} \ldots \mathtt{K}_{a_1}\beta$, using the case for $\mathtt{K}_a\gamma$, we have that $(r^{\mathbf{S'}}, 0) \models \mathtt{E}^m\beta$, for every $m \in \mathbb{N}$, and $(r^{\mathbf{S'}}, 0) \models \mathtt{C}\beta$, by Definition 3. It follows that $r^{\mathbf{S'}} \in [\mathtt{C}\beta]^{(r^{\mathbf{S}},n)}$. For the other direction, assume $r^{\mathbf{S'}} \in [\mathtt{C}\beta]^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}}, 0) \models \mathtt{C}\beta$. Then for every $k \in \mathbb{N}$

- $(r^{\mathbf{S'}}, 0) \models \mathtt{E}^k\beta$, by the definition of the satisfiability relation; and
- by the induction hypothesis: $\mathtt{E}^k\beta \in \mathbf{S'}_0$.

Since $\mathbf{S'}_0$ is maximal consistent and deductively closed, for every $k \in \mathbb{N}$:

– $\mathbf{S'}_0 \vdash \mathtt{E}^k\beta$;
  $\mathbf{S'}_0 \vdash \Phi_{0,\{\beta\vee\neg\beta\},\mathbf{X}}(\mathtt{E}^k\beta)$;
  $\mathbf{S'}_0 \vdash \Phi_{0,\{\beta\vee\neg\beta\},\mathbf{X}}(\mathtt{C}\beta)$, by Rule R$\mathtt{C}$;
  $\mathbf{S'}_0 \vdash \mathtt{C}\beta$,

which means that $\mathtt{C}\beta \in \mathbf{S'}_0$, i.e., $r^{\mathbf{S'}} \in [\![\mathtt{C}\beta]\!]^{(r^{\mathbf{S}},n)}$.

Assume now that $(r^{\mathbf{S'}}, n') \in [\![\mathtt{C}\beta]\!]_a^{(r^{\mathbf{S}},n)}$, i.e., $\mathtt{C}\beta \in \mathbf{S'}_{n'}$. Then $\mathtt{E}^m\beta \in \mathbf{S'}_{n'}$, for every $m \in \mathbb{N}$, by Axiom A$\mathtt{CE}$. Since $\mathtt{E}^m$ is a conjunction of formulas of the form $\mathtt{K}_{a_m} \ldots \mathtt{K}_{a_1}\beta$, using the case for $\mathtt{K}_a\gamma$, we have that $(r^{\mathbf{S'}}, n') \models \mathtt{E}^m\beta$, for every $m \in \mathbb{N}$, and $(r^{\mathbf{S'}}, n') \models \mathtt{C}\beta$, by Definition 3. It follows that $(r^{\mathbf{S'}}, n') \in [\mathtt{C}\beta]_a^{(r^{\mathbf{S}},n)}$. For the other direction, assume $(r^{\mathbf{S'}}, n') \in [\mathtt{C}\beta]_a^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}}, n') \models \mathtt{C}\beta$. Then, for every $k \in \mathbb{N}$:

- $(r^{\mathbf{S'}}, n') \models \mathtt{E}^k\beta$, by the definition of the satisfiability relation; and
- by the induction hypothesis: $\mathtt{E}^k\beta \in \mathbf{S'}_{n'}$.

Since $\mathbf{S'}_{n'}$ is maximal consistent and deductively closed, for every $k \in \mathbb{N}$:

$\mathbf{S'}_{n'} \vdash \mathtt{E}^k\beta$;
$\mathbf{S'}_{n'} \vdash \Phi_{0,\{\beta\vee\neg\beta\},\mathbf{X}}(\mathtt{E}^k\beta)$;
$\mathbf{S'}_{n'} \vdash \Phi_{0,\{\beta\vee\neg\beta\},\mathbf{X}}(\mathtt{C}\beta)$, by Rule R$\mathtt{C}$;
$\mathbf{S'}_{n'} \vdash \mathtt{C}\beta$,

which means that $\mathtt{C}\beta \in \mathbf{S'}_{n'}$, i.e., $(r^{\mathbf{S'}}, n') \in [\![\mathtt{C}\beta]\!]_a^{(r^{\mathbf{S}},n)}$. Thus, $[\![\mathtt{C}\beta]\!]^{(r^{\mathbf{S}},n)} = [\mathtt{C}\beta]^{(r^{\mathbf{S}},n)}$ and $[\![\mathtt{C}\beta]\!]_a^{(r^{\mathbf{S}},n)} = [\mathtt{C}\beta]_a^{(r^{\mathbf{S}},n)}$.

Let $\alpha = \mathtt{P}_{\geqslant t}\beta$.

If $r^{\mathbf{S'}} \in [\![\mathtt{P}_{\geqslant t}\beta]\!]^{(r^{\mathbf{S}},n)}$, then $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_0$. It follows that $\sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_0\} \geqslant t$. Since $\mu^{*,(r^{\mathbf{S'}},0)}([\![\beta]\!]^{(r^{\mathbf{S'}},0)}) = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_0\}$, then $(r^{\mathbf{S'}},0) \models \mathtt{P}_{\geqslant t}\beta$, which means that $r^{\mathbf{S'}} \in [\mathtt{P}_{\geqslant t}\beta]^{(r^{\mathbf{S}},n)}$. For the other direction, let $r^{\mathbf{S'}} \in [\mathtt{P}_{\geqslant t}\beta]^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}},0) \models \mathtt{P}_{\geqslant t}\beta$. Then,

- $\mu^{*,(r^{\mathbf{S'}},0)}([\![\beta]\!]^{(r^{\mathbf{S'}},0)}) = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_0\} \geqslant t$;
- if $t = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_0\}$, then by Lemma 6.8, $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_0$; and
- if $t \leqslant \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_0\}$, then by Lemma 6.9, $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_0$.

In both cases, $r^{\mathbf{S'}} \in [\![\mathtt{P}_{\geqslant t}\beta]\!]^{(r^{\mathbf{S}},n)}$.

If $(r^{\mathbf{S'}},n') \in [\![\mathtt{P}_{\geqslant t}\beta]\!]_a^{(r^{\mathbf{S}},n)}$, then $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_{n'}$. It follows that $\sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_{n'}\} \geqslant t$. Since $\mu^{*,(r^{\mathbf{S'}},n')}([\![\beta]\!]^{(r^{\mathbf{S'}},n')}) = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_{n'}\}$, then $(r^{\mathbf{S'}},n') \models \mathtt{P}_{\geqslant t}\beta$, which means that $(r^{\mathbf{S'}},n') \in [\mathtt{P}_{\geqslant t}\beta]_a^{(r^{\mathbf{S}},n)}$. For the other direction, let $(r^{\mathbf{S'}},n') \in [\mathtt{P}_{\geqslant t}\beta]_a^{(r^{\mathbf{S}},n)}$, i.e., $(r^{\mathbf{S'}},n') \models \mathtt{P}_{\geqslant t}\beta$. Then,

- $\mu^{*,(r^{\mathbf{S'}},n')}([\![\beta]\!]^{(r^{\mathbf{S'}},n')}) = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_{n'}\} \geqslant t$;
- if $t = \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_{n'}\}$, then by Lemma 6.8, $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_{n'}$; and
- if $t \leqslant \sup_s\{s \in [0,1]_{\mathbb{Q}} : \mathtt{P}_{\geqslant s}\beta \in \mathbf{S'}_{n'}\}$, then by Lemma 6.9, $\mathtt{P}_{\geqslant t}\beta \in \mathbf{S'}_{n'}$.

In both cases $(r^{\mathbf{S'}},n') \in [\![\mathtt{P}_{\geqslant t}\beta]\!]_a^{(r^{\mathbf{S}},n)}$. Thus, $[\![\mathtt{P}_{\geqslant s}\beta]\!]^{(r^{\mathbf{S}},n)} = [\mathtt{P}_{\geqslant s}\beta]^{(r^{\mathbf{S}},n)}$, and $[\![\mathtt{P}_{\geqslant s}\beta]\!]_a^{(r^{\mathbf{S}},n)} = [\mathtt{P}_{\geqslant s}\beta]_a^{(r^{\mathbf{S}},n)}$. □

THEOREM 8 (Strong completeness for $\mathtt{Ax}_{\mathbf{PTEL}}$).
A set $\mathbf{T}$ of formulas is $\mathtt{Ax}_{\mathbf{PTEL}}$-consistent iff it is satisfiable.

PROOF. The ($\Leftarrow$)-direction follows from the soundness of the above axiomatic system. To prove the ($\Rightarrow$)-direction assume that $\mathbf{T}$ is consistent. Theorem 6 guarantees that $\mathbf{T}$ can be extended to a maximal consistent $\mathbf{T}^*$, while Theorem 7 shows that the canonical model $\mathcal{M}^*$ can be defined so that $\mathbf{T}$ is satisfiable in a possible world from $\mathcal{M}^*$. □

Received 26 August 2021