Two Ways to Common Knowledge

Samuel Bucheli[1,2] Roman Kuznets[1,2] Thomas Studer[2]

Institut für Informatik und angewandte Mathematik
Universität Bern
Bern, Switzerland

Abstract

It is not clear what a system for evidence-based common knowledge should look like if common knowledge is treated as a greatest fixed point. This paper is a preliminary step towards such a system. We argue that the standard induction rule is not well suited to axiomatize evidence-based common knowledge. As an alternative, we study two different deductive systems for the logic of common knowledge. The first system makes use of an induction axiom whereas the second one is based on co-inductive proof theory. We show the soundness and completeness for both systems.

Keywords: Justification logics, common knowledge, proof theory

1 Introduction

Justification logics [6] are epistemic logics that explicitly include justifications for an agent's knowledge. Historically, Artemov [3,4] developed the first of these logics, the Logic of Proofs, to solve the problem of a provability semantics for S4. Fitting's model construction [11] provides a natural epistemic semantics for the Logic of Proofs, which can be generalized to the whole family of justification logics. It augments Kripke models with a function that specifies admissible evidence for each formula at a given state.

Instead of the simple A *is known*, justification logics formalize t *is a justification for* A. Thus, these logics feature evidence-based knowledge and enable us to reason about the evidence. This novel approach has many applications. For instance, it makes it possible to tackle the logical omniscience problem [7] and to deal with certain forms of self-referentiality [12].

The notion of common knowledge is essential in the area of multi-agent systems, where coordination among a set of agents is a central issue. The textbooks [10,14] provide excellent introductions to epistemic logics in general and common knowledge in particular. Informally, common knowledge of a proposition A is defined as

[1] Supported by Swiss National Science Foundation grant 200021–117699.
[2] Emails: {bucheli, kuznets, tstuder}@iam.unibe.ch

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.com/locate/entcs

the infinitary conjunction *everybody knows A and everybody knows that everybody knows A and so on*. This is equivalent to saying that common knowledge of A is the greatest fixed point of $\lambda X.(\textit{everybody knows } A \textit{ and everybody knows } X)$. The standard approach to axiomatizing this property is by means of a co-closure axiom (see Definition 2.1) and the following induction rule (see, for instance, [10]):

$$\frac{A \to \mathsf{E}(A \wedge B)}{A \to \mathsf{C}B} \quad (\mathsf{I\text{-}R1})$$

A justified common knowledge operator was introduced by Artemov in [5]. However, his operator does not capture the greatest solution of the corresponding fixed point equation. The relation between the classical and the justified versions of common knowledge is studied in [2].

Our long-term goal is to come up with an evidence-based version of common knowledge where common knowledge is treated as a greatest fixed point. However, using a rule akin to (I-R1) in a justification logic makes it difficult to show that the resulting logic enjoys internalization, the property that states that the logic internalizes its own notion of proof, which is central to the Realization Theorem.

We believe that in order to achieve our aim it is necessary to consider alternative formalizations of common knowledge. In this paper, we will examine two such approaches. The first is based on induction whereas the second employs co-induction. The first system we study includes an induction axiom instead of the rule (I-R1). This axiom was proposed in [14], where a semantic completeness proof is given. We investigate the proof-theoretic relationship between this axiom and (I-R1) thereby providing an alternative completeness proof.

Common knowledge is equivalent to an infinitary conjunction. Therefore, it seems plausible that a justification term for common knowledge is an infinitely long term, i.e., a co-inductive term. To support this approach, we introduce a co-inductive system S for common knowledge. In this formal system, proofs may have infinite branches. Such systems have previously been studied, for example, for the μ-calculus [15,18] and the linear time μ-calculus [9]. The underlying idea of this approach is based on the fundamental semantic theorem of the modal μ-calculus [8] (due to Streett and Emerson [17]). A similar result was also developed in [16].

Our completeness proof for the infinitary system S is performed along the lines of [15] utilizing the determinacy of certain infinite games. Alternatively, we could use the completeness of the common knowledge system with an ω-rule [1]. The transformation from ω-rules to infinite branches then would yield the completeness of S (see [18] for this approach in the context of the μ-calculus).

The paper is organized as follows. In the next section, we introduce the language and semantics for the logic of common knowledge. We recall the deductive system $\mathsf{H_R}$ from [10], which is based on (I-R1). In Section 3, we present the system $\mathsf{H_{Ax}}$, which includes the induction axiom from [14]. We then study a proof-theoretic reduction of $\mathsf{H_R}$ to $\mathsf{H_{Ax}}$, thus providing the completeness of $\mathsf{H_{Ax}}$. The system S that features proofs with infinite branches is introduced in Section 4. We establish the soundness and completeness of S by employing techniques from the proof of the fundamental semantic theorem and results about infinite games.

2 Preliminaries

2.1 Language and Semantics

We consider a language with h agents for some $h > 0$. This language will be fixed throughout the paper, and h will always denote the number of agents. Propositions P and their negations $\overline{P}$ are atoms. Formulae are denoted by A, B, C. They are given by the following grammar

$$A ::= P \mid \overline{P} \mid A \wedge A \mid A \vee A \mid \Box_i A \mid \Diamond_i A \mid \mathsf{C}A \mid \tilde{\mathsf{C}}A \ ,$$

where $1 \leq i \leq h$. The formula $\Box_i A$ is read as *agent i knows A*, and the formula $\mathsf{C}A$ is read as *A is common knowledge*. The connectives $\Box_i$ and C have $\Diamond_i$ and $\tilde{\mathsf{C}}$ as their respective duals. The negation $\neg A$ of a formula A is defined in the usual way by using De Morgan's laws, the law of double negation, and the duality laws for modal operators. We also define $A \to B := \neg A \vee B$ and $A \leftrightarrow B := (A \to B) \wedge (B \to A)$. The formula $\mathsf{E}A$ is an abbreviation for *everybody knows A*:

$$\mathsf{E}A := \Box_1 A \wedge \cdots \wedge \Box_h A \quad \text{and} \quad \tilde{\mathsf{E}}A := \Diamond_1 A \vee \cdots \vee \Diamond_h A \ .$$

A *Kripke structure* $\mathcal{M}$ is a tuple $(S, R_1, \ldots, R_h, \pi)$, where S is a non-empty set of states, each R_i is a binary relation on S, and π is a valuation function that assigns to each atomic formula a set of states such that $\pi\left(\overline{P}\right) = S \setminus \pi(P)$.

Given a Kripke structure $\mathcal{M} = (S, R_1 \ldots, R_h, \pi)$ and states $v, w \in S$, we say that *w is reachable from v in n steps* ($\mathsf{reach}(v, w, n)$) if there exist states $s_0, \ldots, s_n$ such that $s_0 = v$, $s_n = w$, and for all $0 \leq j \leq n-1$ there exists $1 \leq i \leq h$ with $R_i(s_j, s_{j+1})$. We say *w is reachable from v* if there exists an n with $\mathsf{reach}(v, w, n)$.

Let $\mathcal{M} = (S, R_1 \ldots, R_h, \pi)$ be a Kripke structure and $v \in S$ be a state. We define the *satisfaction relation* $\mathcal{M}, v \models A$ inductively on the structure of the formula A:

$$
\begin{array}{ll}
\mathcal{M}, v \models P & \text{if } v \in \pi(P), \\
\mathcal{M}, v \models \overline{P} & \text{if } v \in \pi\left(\overline{P}\right), \\
\mathcal{M}, v \models A \wedge B & \text{if } \mathcal{M}, v \models A \text{ and } \mathcal{M}, v \models B, \\
\mathcal{M}, v \models A \vee B & \text{if } \mathcal{M}, v \models A \text{ or } \mathcal{M}, v \models B, \\
\mathcal{M}, v \models \Box_i A & \text{if } \mathcal{M}, w \models A \text{ for all } w \text{ such that } R_i(v, w), \\
\mathcal{M}, v \models \Diamond_i A & \text{if } \mathcal{M}, w \models A \text{ for some } w \text{ with } R_i(v, w), \\
\mathcal{M}, v \models \mathsf{C}A & \text{if } \mathcal{M}, w \models A \text{ for all } w \text{ such that } (\exists n \geq 1)\mathsf{reach}(v, w, n), \\
\mathcal{M}, v \models \tilde{\mathsf{C}}A & \text{if } \mathcal{M}, w \models A \text{ for some } w \text{ with } (\exists n \geq 1)\mathsf{reach}(v, w, n).
\end{array}
$$

We write $\mathcal{M} \models A$ if $\mathcal{M}, v \models A$ for all $v \in S$. A formula A is called *valid* if $\mathcal{M} \models A$ for all Kripke structures $\mathcal{M}$. A formula A is called *satisfiable* if $\mathcal{M}, v \models A$ for some Kripke structure $\mathcal{M}$ and some state v.

2.2 Deductive System

Let us briefly recall the definition of the system for common knowledge that makes use of the induction rule.

Definition 2.1 [The system $\mathsf{H_R}$] The Hilbert calculus $\mathsf{H_R}$ for the logic of common knowledge is defined by the following axioms and inference rules:

Propositional axioms: All instances of propositional tautologies

Modus ponens: For all formulae A and B,

$$\frac{A \quad A \to B}{B} \quad (\mathsf{MP})$$

Modal axioms: For all formulae A and B and all indices $1 \leq i \leq h$,

$$\Box_i(A \to B) \to (\Box_i A \to \Box_i B) \quad (\mathsf{K})$$

Necessitation rule: For all formulae A and all indices $1 \leq i \leq h$,

$$\frac{A}{\Box_i A} \quad (\mathsf{Nec})$$

Co-closure axiom: For all formulae A,

$$\mathsf{C}A \to \mathsf{E}(A \wedge \mathsf{C}A) \quad (\mathsf{Co\text{-}Cl})$$

Induction rule: For all formulae A and B,

$$\frac{B \to \mathsf{E}(A \wedge B)}{B \to \mathsf{C}A} \quad (\mathsf{I\text{-}R1})$$

We have the following standard result, see [10].

Theorem 2.2 (Soundness and completeness of $\mathsf{H_R}$) *For any formula A,*

$$\mathsf{H_R} \vdash A \quad \textit{if and only if} \quad A \textit{ is valid.}$$

3 The Inductive Way

3.1 Deductive System

We now introduce a deductive system for common knowledge where the induction rule is replaced by an induction axiom. To obtain a complete system, we also need to include a normality axiom and a necessitation rule for the common knowledge operator.

Definition 3.1 [The system $\mathsf{H_{Ax}}$] The Hilbert calculus $\mathsf{H_{Ax}}$ consists of the axioms and rules of $\mathsf{H_R}$ whereby $(\mathsf{I\text{-}R1})$ is replaced by the following axioms and rule:

C-modal axiom: For all formulae A and B,

$$\mathsf{C}(A \to B) \to (\mathsf{C}A \to \mathsf{C}B) \quad (\mathsf{C\text{-}K})$$

C-necessitation rule: For all formulae A,

$$\frac{A}{\mathsf{C}A} \quad (\mathsf{C\text{-}Nec})$$

Induction axiom: For all formulae A,

$$\mathsf{E}A \wedge \mathsf{C}(A \to \mathsf{E}A) \to \mathsf{C}A \quad (\mathsf{I\text{-}Ax})$$

In [14], an induction axiom is introduced as $A \wedge \mathsf{C}(A \to \mathsf{E}A) \to \mathsf{C}A$. However, in our setting, the axiom from [14] would not be sound since we do not define common knowledge to be reflexive.

3.2 Soundness

The soundness of H_{Ax} is easily obtained.

Theorem 3.2 (Soundness) *For any formula A, if $\mathsf{H}_{\mathsf{Ax}} \vdash A$, then A is valid.*

Proof. As usual, by induction on the length of the derivation of $\mathsf{H}_{\mathsf{Ax}} \vdash A$. We only show the case where A is the induction axiom. Let $\mathcal{M}$ be a Kripke structure. We show by induction on n that for all $n \geq 1$, if $\mathcal{M}, v \models \mathsf{E}A \wedge \mathsf{C}(A \to \mathsf{E}A)$, then for all states w with $\mathsf{reach}(v, w, n)$, we have $\mathcal{M}, w \models A$. If $n = 1$, then $\mathcal{M}, v \models \mathsf{E}A$ guarantees $\mathcal{M}, w \models A$. For $n = m + 1$, $m \geq 1$, let w be such that $\mathsf{reach}(v, w, n)$. Then there exists v' such that

(i) $\mathsf{reach}(v, v', m)$ and

(ii) $\mathsf{reach}(v', w, 1)$.

From (i) and $\mathcal{M}, v \models \mathsf{C}(A \to \mathsf{E}A)$ we obtain $\mathcal{M}, v' \models A \to \mathsf{E}A$. By the induction hypothesis, we get $\mathcal{M}, v' \models A$. Therefore, $\mathcal{M}, v' \models \mathsf{E}A$. Thus, by (ii), we get $\mathcal{M}, w \models A$. □

3.3 Completeness

In order to establish the completeness of H_{Ax}, we have to introduce an intermediate system $\mathsf{H}_{\mathsf{int}}$. We first reduce H_{R} to $\mathsf{H}_{\mathsf{int}}$ and then reduce $\mathsf{H}_{\mathsf{int}}$ to H_{Ax}. These reductions reveal the proof-theoretic relationship between the induction axiom and the induction rule. Moreover, it follows that the completeness of H_{R} implies the completeness of H_{Ax}.

Definition 3.3 [The system $\mathsf{H}_{\mathsf{int}}$] $\mathsf{H}_{\mathsf{int}}$ consists of the axioms and rules of H_{R} whereby $(\mathsf{I\text{-}R1})$ is replaced by the following axiom and rule:

C-distributivity: For all formulae A and B,

$$\mathsf{C}(A \wedge B) \to (\mathsf{C}A \wedge \mathsf{C}B) \quad (\mathsf{C\text{-}Dis})$$

Induction rule 2: For all formulae A,

$$\frac{A \to \mathsf{E}A}{\mathsf{E}A \to \mathsf{C}A} \quad (\mathsf{I\text{-}R2})$$

Lemma 3.4 *For each formula A, we have that $\mathsf{H}_{\mathsf{R}} \vdash A$ implies $\mathsf{H}_{\mathsf{int}} \vdash A$.*

Proof. It is sufficient to show that $(\mathsf{I\text{-}R1})$ is derivable in $\mathsf{H}_{\mathsf{int}}$. Assume

$$\mathsf{H}_{\mathsf{int}} \vdash B \to \mathsf{E}(A \wedge B) \ . \quad (1)$$

Then $\mathsf{H_{int}} \vdash A \wedge B \to \mathsf{E}(A \wedge B)$. By (I-R2), we obtain that

$$\mathsf{H_{int}} \vdash \mathsf{E}(A \wedge B) \to \mathsf{C}(A \wedge B) \ .$$

Using (C-Dis), we get $\mathsf{H_{int}} \vdash \mathsf{E}(A \wedge B) \to \mathsf{C}A$. Finally, (1) yields $\mathsf{H_{int}} \vdash B \to \mathsf{C}A$, which completes the proof. □

Lemma 3.5 *For each formula A, we have that $\mathsf{H_{int}} \vdash A$ implies $\mathsf{H_{Ax}} \vdash A$.*

Proof. We first show that (C-Dis) is derivable in $\mathsf{H_{Ax}}$. The following formula is an instance of (C-K):

$$\mathsf{H_{Ax}} \vdash \mathsf{C}(A \wedge B \to B) \to (\mathsf{C}(A \wedge B) \to \mathsf{C}B) \ . \tag{2}$$

$\mathsf{H_{Ax}} \vdash A \wedge B \to B$ is a propositional axiom. By (C-Nec), $\mathsf{H_{Ax}} \vdash \mathsf{C}(A \wedge B \to B)$. By (2), we have $\mathsf{H_{Ax}} \vdash \mathsf{C}(A \wedge B) \to \mathsf{C}B$. A similar argument yields $\mathsf{H_{Ax}} \vdash \mathsf{C}(A \wedge B) \to \mathsf{C}A$. The last two statements together imply that (C-Dis) is derivable in $\mathsf{H_{Ax}}$.

It remains to show that (I-R2) is derivable in $\mathsf{H_{Ax}}$. Assume that $\mathsf{H_{Ax}} \vdash A \to \mathsf{E}A$. By (C-Nec), we get $\mathsf{H_{Ax}} \vdash \mathsf{C}(A \to \mathsf{E}A)$. Thus, the derivability of (I-R2) follows from (I-Ax). □

The two lemmas, together with the completeness of $\mathsf{H_R}$, give us the completeness of $\mathsf{H_{Ax}}$.

Corollary 3.6 (Completeness of $\mathsf{H_{Ax}}$) *For all formulae A, if A is valid, then $\mathsf{H_{Ax}} \vdash A$.*

4 The Co-Inductive Way

4.1 Deductive System

We now introduce the infinitary system S for common knowledge. In this formal system, proofs are finitely branching trees that may have infinitely long branches while all finite branches must still end in an axiom. In order to obtain a sound deductive system, we have to impose a global constraint on such infinite branches. Roughly, we require that on every infinite branch in a proof, there be a greatest fixed point unfolded infinitely often.

We consider sequents to be finite sets of formulae and denote them by Γ, Δ, Σ. For a sequent $\Delta = \{A_1, \ldots, A_n\}$, we denote the sequent $\{\Diamond_i A_1, \ldots, \Diamond_i A_n\}$ by $\Diamond_i \Delta$ and the sequent $\{\tilde{\mathsf{E}} A_1, \ldots, \tilde{\mathsf{E}} A_n\}$ by $\tilde{\mathsf{E}}\Delta$. In addition, $\mathcal{M}, v \models \Delta$ is understood as $\mathcal{M}, v \models A_1 \vee \cdots \vee A_n$.

Definition 4.1 A *preproof* for a sequent Γ is a possibly infinite tree whose root is labeled with Γ and which is built according to the following axioms and rules:

Axioms: For all sequents Γ and all propositions P,

$$\Gamma, P, \overline{P} \quad (\mathsf{ax})$$

Propositional rules: For all sequents Γ and all formulae A and B,

$$\frac{\Gamma, A, B}{\Gamma, A \vee B}\ (\vee) \qquad\qquad \frac{\Gamma, A \qquad \Gamma, B}{\Gamma, A \wedge B}\ (\wedge)$$

Modal rules: For all sequents Γ and Σ, all formulae A, and all indices $1 \leq i \leq h$,

$$\frac{\Gamma, A}{\Diamond_i \Gamma, \Box_i A, \Sigma}\ (\Box)$$

Fixed point rules: For all sequents Γ and all formulae A,

$$\frac{\Gamma, \tilde{\mathsf{E}}A \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}A}{\Gamma, \tilde{\mathsf{C}}A}\ (\tilde{\mathsf{C}}) \qquad\qquad \frac{\Gamma, \mathsf{E}A \wedge \mathsf{E}\mathsf{C}A}{\Gamma, \mathsf{C}A}\ (\mathsf{C})$$

We now introduce the notion of a thread in a branch of a proof tree.

Definition 4.2 The *principal formula* of a rule is the formula that is explicitly displayed in the conclusion of the rule. The *active formulae* of a rule are those formulae that are explicitly displayed in the premise(s) of the rule. The formulae in Γ and Σ are called the *side formulae* of a rule.

Definition 4.3 Consider a proof tree for some sequent. For all rule applications r that occur in this proof tree, we define a *connection relation* $\mathsf{Con}(r)$ on formulae as follows:

(i) In the case when r is not an application of $(\Box)$, we define $(A, B) \in \mathsf{Con}(r)$ if $A = B$ and A is a side formula of r or if A is the principal formula and B is an active formula of r.

(ii) In the case when r is an application of $(\Box)$, we define $(\Box_i A, A) \in \mathsf{Con}(r)$ if $\Box_i A$ is the principal formula of r and we define $(\Diamond_i B, B) \in \mathsf{Con}(r)$ if $\Diamond_i B \in \Diamond_i \Gamma$.

Definition 4.4 Consider a finite or infinite branch $\Gamma_0, \Gamma_1, \ldots$ in a proof tree. Let r_i be the rule application where Γ_i is the conclusion and Γ_{i+1} is a premise. A *thread* in this branch is a sequence of formulae $A_0, A_1, \ldots$ such that $(A_i, A_{i+1}) \in \mathsf{Con}(r_i)$ and $A_i \in \Gamma_i$ for every i. Note that a thread in an infinite branch may be finite or infinite.

Definition 4.5 Consider an infinite branch of a preproof for a sequent Γ. An infinite thread in this branch is called a C-*thread* if infinitely many of its formulae are the principal formulae of applications of (C).

Definition 4.6 An S-*proof* for a sequent Γ is a preproof for Γ such that every finite branch ends in an axiom and every infinite branch contains a C-thread. We write $\mathsf{S} \vdash \Gamma$ if there exists an S-proof for Γ.

We will illustrate how S-proofs work by deriving the induction axiom in S. In order to present this derivation in a compact form, we need to state some properties of the system. It should be noted that the proof of Lemma 4.7(ii) requires infinite derivations, e.g., in the case of $A = \mathsf{C}B$.

$$
\dfrac{\dfrac{(\mathsf{ax'})}{\neg A, A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A} \qquad \dfrac{\vdots}{\neg A, \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{C}A}}\ (\mathsf{C})}{\neg A, A \wedge \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{C}A}}\ (\wedge)
$$

$$
\dfrac{\dfrac{\dfrac{\neg A, A \wedge \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{C}A}}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A), \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{EC}A}}\ (\mathsf{E})}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A) \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{EC}A}}\ (\vee)}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{EC}A}}\ (\tilde{\mathsf{C}})
$$

$$
\dfrac{\dfrac{\dfrac{(\mathsf{ax'})}{\neg A, A}}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{E}A}\ (\mathsf{E}) \qquad \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{EC}A}}{\dfrac{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{E}A \wedge \mathsf{EC}A}}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \underline{\mathsf{C}A}}\ (\mathsf{C})}\ (\wedge)
$$

Fig. 1. A sample S-proof for the induction axiom (I-Ax) with a highlighted C-thread.

Lemma 4.7 (i) *For all formulae A and all sequents Γ and Σ, the following analog of the $(\Box)$-rule is derivable in* S*:*

$$\dfrac{\Gamma, A}{\tilde{\mathsf{E}}\Gamma, \mathsf{E}A, \Sigma}\ (\mathsf{E})$$

(ii) *For all formulae A and all sequents Γ, the following generalized form of axioms (ax) is derivable:*

$$\mathsf{S} \vdash \Gamma, A, \neg A \quad (\mathsf{ax'})$$

Example 4.8 Fig. 1 contains the bottom part of an infinite S-proof for the induction axiom (I-Ax) expressed in a sequent form as $\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A$. Two of the three topmost sequents shown are labeled (ax') and are derivable by Lemma 4.7(ii). The only infinite branch outside of (ax')-derivations has infinitely many repetitions of the sequent $\neg A, \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A$. To show that this preproof is indeed an S-proof, it is sufficient to find a C-thread in this branch. The thread that consists of the red underlined formulae is such a C-thread.

4.2 Soundness

The soundness proof essentially uses the idea that underlies the fundamental semantic theorem of the modal μ-calculus.

Let $\delta(A)$ be the maximal number of nested C operators in the formula A: for instance, $\delta(\mathsf{C}(\mathsf{C}P \vee \mathsf{C}Q)) = 2$. Given $m \geq 1$ and a sequence $\sigma = (\sigma_m, \dots, \sigma_1)$ of ordinals, for all formulae A such that $\delta(A) \leq m$, we define the satisfaction relation $\models^\sigma_{\mathsf{C}}$ in the same way as $\models$ except in the case of C, where we set $\mathcal{M}, v \models^\sigma_{\mathsf{C}} \mathsf{C}B$ if $\mathcal{M}, w \models^\sigma_{\mathsf{C}} B$ for all w for which there exists n with $\sigma_{\delta(\mathsf{C}B)} \geq n \geq 1$ and $\mathsf{reach}(v, w, n)$. We immediately obtain

$$\mathcal{M}, v \models_{\mathsf{C}}^{(\sigma_m, \dots, \sigma_{\delta(\mathsf{C}B)}+1, \dots, \sigma_1)} \mathsf{C}B \text{ iff } \mathcal{M}, v \models_{\mathsf{C}}^{(\sigma_m, \dots, \sigma_{\delta(\mathsf{C}B)}, \dots, \sigma_1)} \mathsf{E}B \wedge \mathsf{EC}B \ . \qquad (3)$$

It is sufficient to consider only ordinals $\leq \omega$, but ω itself as a possible element of a sequence σ is necessary to guarantee that for all formulae A,

$$\mathcal{M}, v \not\models A \text{ implies that there exists } \sigma \text{ such that } \mathcal{M}, v \not\models^\sigma_{\mathsf{C}} A \ . \qquad (4)$$

Lemma 4.9 *Let A be a formula, Δ be a sequent, σ be a sequence of ordinals, $\mathcal{M} = (S, R_1, \ldots, R_h, \pi)$ be a Kripke structure, $v \in S$ be a state, and $1 \leq i \leq h$. If $\mathcal{M}, v \not\models \Box_i A, \Diamond_i \Delta$ and $\mathcal{M}, v \not\models^\sigma_{\mathsf{C}} \Box_i A$, then there exists a state $w \in S$ with $R_i(v, w)$ such that $\mathcal{M}, w \not\models A, \Delta$ and $\mathcal{M}, w \not\models^\sigma_{\mathsf{C}} A$.*

Proof. Suppose for all $w \in S$ with $R_i(v, w)$, at least one of the claims $\mathcal{M}, w \models A, \Delta$ or $\mathcal{M}, w \models^\sigma_{\mathsf{C}} A$ holds. We distinguish the following two cases:

(i) $\mathcal{M}, w \models^\sigma_{\mathsf{C}} A$ holds for all $w \in S$ with $R_i(v, w)$. Then we have $\mathcal{M}, v \models^\sigma_{\mathsf{C}} \Box_i A$. Contradiction.

(ii) There is at least one $w \in S$ with $R_i(v, w)$ such that $\mathcal{M}, w \not\models^\sigma_{\mathsf{C}} A$. Then $\mathcal{M}, w \not\models A$. Hence, there must be a formula $B \in \Delta$ such that $\mathcal{M}, w \models B$. However, this means $\mathcal{M}, v \models \Diamond_i B$ and, therefore, $\mathcal{M}, v \models \Diamond_i \Delta$. Contradiction. □

Given two sequences σ and τ of the same length m, we say $\sigma < \tau$ if σ is smaller than τ with respect to the lexicographic ordering. Since we consider sequences of a fixed length, the relation $<$ is a well-ordering.

Theorem 4.10 (Soundness) *For all formulae A, if A is not valid, then $\mathsf{S} \nvdash A$.*

Proof. Suppose A is not valid yet there is an S-proof $\mathcal{T}$ for it. Then there is a Kripke structure $\mathcal{M}$ and a state s such that $\mathcal{M}, s \not\models A$, which will be used to construct a branch $\Gamma_0, \Gamma_1, \ldots$ with the corresponding inferences $r_0, r_1, \ldots$ in $\mathcal{T}$ and a sequence $s_0, s_1, \ldots$ of states in $\mathcal{M}$ such that

(a) $\mathcal{M}, s_i \not\models \Gamma_i$ and

(b) if $(B, C) \in \mathsf{Con}(r_i)$, $C \in \Gamma_{i+1}$, and $\mathcal{M}, s_i \not\models^\sigma_{\mathsf{C}} B$, then $\mathcal{M}, s_{i+1} \not\models^\sigma_{\mathsf{C}} C$.

Let $\Gamma_0 := A$ and $s_0 := s$. If Γ_i and s_i are given, we construct Γ_{i+1} and s_{i+1} according to the different cases for r_i. Note that because of (a) Γ_i cannot be axiomatic and thus must have been inferred by some rule.

(i) $r_i = (\Box)$: Let $\Box_i B \in \Gamma_i$ be the principal formula of r_i. Let σ be the least sequence such that $\mathcal{M}, s_i \not\models^\sigma_{\mathsf{C}} \Box_i B$. We apply Lemma 4.9 for this σ to find a state s_{i+1} such that (a) and (b) hold. We let Γ_{i+1} be the unique premise of r_i.

(ii) $r_i = (\wedge)$: Let $B_1 \wedge B_2 \in \Gamma_i$ be the principal formula of r_i. Let σ be the least sequence such that $\mathcal{M}, s_i \not\models^\sigma_{\mathsf{C}} B_1 \wedge B_2$. Let Γ_{i+1} be the j-th premise of r_i such that $\mathcal{M}, s_i \not\models^\sigma_{\mathsf{C}} B_j$. Further, set $s_{i+1} := s_i$. This construction guarantees (a) and (b).

(iii) In all other cases, r_i has a unique premise Δ. We set $s_{i+1} := s_i$ and $\Gamma_{i+1} := \Delta$. Again (a) and (b) hold.

We have constructed an infinite branch in $\mathcal{T}$. Since $\mathcal{T}$ is an S-proof, this branch must contain a C-thread $A_0, A_1, \ldots$. For each natural number j, we define σ^j to be the least sequence such that $\mathcal{M}, s_j \not\models^{\sigma^j}_{\mathsf{C}} A_j$. Note that σ^j exists by (4). It follows from (b) that $\sigma^{j+1} \leq \sigma^j$ for all j. Moreover, because we consider a C-thread, there are infinitely many applications of (C), which, according to (3), means that there are infinitely many j's with $\sigma^{j+1} < \sigma^j$. This contradicts the well-foundedness of $<$. □

4.3 Completeness

The completeness proof for the infinitary system S is based on [15], where a similar result is shown for the modal μ-calculus. For a given formula A, we define an infinite game such that player I has a winning strategy if and only if there is an S-proof for A and player II has a winning strategy if and only if there is a countermodel for A. It is possible to show that this game is *determined*, i.e., one of the players has a winning strategy. Hence, the completeness of S follows.

Definition 4.11 A sequent Γ is *saturated* if all of the following conditions hold:

(i) if $A \wedge B \in \Gamma$, then $A \in \Gamma$ or $B \in \Gamma$,

(ii) if $A \vee B \in \Gamma$, then $A \in \Gamma$ and $B \in \Gamma$,

(iii) if $\mathsf{C}A \in \Gamma$, then $\mathsf{E}A \wedge \mathsf{E}\mathsf{C}A \in \Gamma$, and

(iv) if $\tilde{\mathsf{C}}A \in \Gamma$, then $\tilde{\mathsf{E}}A \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}A \in \Gamma$.

Definition 4.12 The *system* $\mathsf{S}_{\mathsf{Game}}$ consists of the rules of S whereby $(\Box)$ is replaced by the following rules:
Alternative modal rules: Let $1 \leq m \leq h$, $H = \{h_1, \dots, h_m\} \subseteq \{1, \dots, h\}$, and $n_{h_1}, \dots, n_{h_m}$ be positive integers. For all saturated sequents Σ that contain neither formulae that start with $\Diamond_j$, $j \in H$, nor formulae that start with $\Box_i$, $1 \leq i \leq h$, all sequents Γ_j, $j \in H$, and all formulae $A_{j,1}, \dots, A_{j,n_j}$, $j \in H$,

$$\frac{\Gamma_{h_1}, A_{h_1,1} \quad \dots \quad \Gamma_{h_1}, A_{h_1,n_{h_1}} \quad \dots \quad \Gamma_{h_m}, A_{h_m,1} \quad \dots \quad \Gamma_{h_m}, A_{h_m,n_{h_m}}}{\Diamond_{h_1}\Gamma_{h_1}, \Box_{h_1}A_{h_1,1}, \dots, \Box_{h_1}A_{h_1,n_{h_1}}, \dots, \Diamond_{h_m}\Gamma_{h_m}, \Box_{h_m}A_{h_m,1}, \dots, \Box_{h_m}A_{h_m,n_{h_m}}, \Sigma} \ (\Box')$$

Note that this rule has $n_{h_1} + \dots + n_{h_m}$ many premises.

An $\mathsf{S}_{\mathsf{Game}}$-*tree for a sequent* Γ is built by iterating the following two steps until one reaches a saturated sequent which is either axiomatic or to which $(\Box')$ cannot be applied:

(i) Apply the rules $(\vee)$, $(\wedge)$, (C), and $(\tilde{\mathsf{C}})$ backwards until a saturated sequent is reached. While applying the rules, make sure that the conclusion always remains a subset of the premise.

(ii) Apply $(\Box')$ backwards, if possible.

We now introduce a system $\mathsf{S}_{\mathsf{Dis}}$ for establishing unprovability. Accordingly, its rules should not be read as sound, i.e., preserving validity, but rather as "dis-sound," i.e., preserving invalidity.

Definition 4.13 The *system* $\mathsf{S}_{\mathsf{Dis}}$ consists of the rules of $\mathsf{S}_{\mathsf{Game}}$ whereby $(\wedge)$ is replaced by the following two rules:

Alternative $(\wedge)$**:** For all sequents Γ and all formulae A and B,

$$\frac{\Gamma, A}{\Gamma, A \wedge B} \ (\wedge 1) \qquad\qquad \frac{\Gamma, B}{\Gamma, A \wedge B} \ (\wedge 2)$$

An $\mathsf{S}_{\mathsf{Dis}}$-*tree* is built in the same way as an $\mathsf{S}_{\mathsf{Game}}$-tree except that $(\wedge 1)$ and $(\wedge 2)$ are used instead of $(\wedge)$. Therefore, an $\mathsf{S}_{\mathsf{Dis}}$-tree for a sequent Γ is not unique.

$$\dfrac{\vdots}{\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P, P}\ (\mathsf{C})$$

$$\dfrac{\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P, P}{\Diamond_1\mathsf{C}P, \Diamond_1\tilde{\mathsf{C}}\mathsf{C}P, \Box_1 P, \Sigma}\ (\Box')$$

$$\vdots\ \ (*)$$

$$\dfrac{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P, \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P}{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P}\ (\vee)$$

$$\dfrac{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P}{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P}\ (\tilde{\mathsf{C}})$$

$$\dfrac{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P}{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P}\ (\wedge 1)$$

$$\dfrac{\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P}{\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P}\ (\mathsf{C})$$

Fig. 2. A sample $\mathsf{S}_{\mathsf{Dis}}$-disproof for $\tilde{\mathsf{C}}\overline{P} \to \tilde{\mathsf{C}}\mathsf{C}P$ with a highlighted $\tilde{\mathsf{C}}$-thread.

The notions of a *thread* and a C-*thread* are extended to $\mathsf{S}_{\mathsf{Game}}$- and $\mathsf{S}_{\mathsf{Dis}}$-trees. A $\tilde{\mathsf{C}}$-*thread* is a thread that contains infinitely many principal formulae of applications of $(\tilde{\mathsf{C}})$. Note that any infinite thread is either a C- or a $\tilde{\mathsf{C}}$-thread but not both.

Definition 4.14 We say that an $\mathsf{S}_{\mathsf{Dis}}$-tree $\mathcal{T}$ for a sequent Γ *disproves* Γ if

(i) no branch ends with an axiom and

(ii) any infinite thread in any branch is a $\tilde{\mathsf{C}}$-thread.

Example 4.15 In order to disprove $\tilde{\mathsf{C}}\overline{P} \to \tilde{\mathsf{C}}\mathsf{C}P$, we construct an $\mathsf{S}_{\mathsf{Dis}}$-tree $\mathcal{T}$ for a corresponding sequent $\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P$ (see Fig. 2). In this tree, $\Diamond_1\mathsf{C}P, \Diamond_1\tilde{\mathsf{C}}\mathsf{C}P, \Box_1 P, \Sigma$ is a saturation of the sequent

$$\mathsf{C}P, \mathsf{E}P \wedge \mathsf{E}\mathsf{C}P, \mathsf{E}P, \tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P, \tilde{\mathsf{E}}\mathsf{C}P, \tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P\ . \qquad (5)$$

The saturation process is abbreviated as $(*)$. It involves exactly $2h-2$ applications of $(\vee)$ to saturate the disjunctions $\tilde{\mathsf{E}}\mathsf{C}P$ and $\tilde{\mathsf{E}}\tilde{\mathsf{C}}\mathsf{C}P$. In addition, the conjunction $\mathsf{E}P$ is saturated by at most $h-1$ applications of $(\wedge 1)$ and $(\wedge 2)$ in such a way that $\Box_1 P$ is the only resulting formula that starts with $\Box_i$. Most formulae that result from this saturation are disjunctions, conjunctions, or are already present in (5), with the exception of $\Diamond_1\mathsf{C}P, \dots, \Diamond_h\mathsf{C}P, \Diamond_1\tilde{\mathsf{C}}\mathsf{C}P, \dots, \Diamond_h\tilde{\mathsf{C}}\mathsf{C}P$, and $\Box_1 P$. Thus, Σ contains neither formulae that start with $\Box_i$ nor formulae that start with $\Diamond_1$, which enables us to apply $(\Box')$. The tree $\mathcal{T}$ extends upward indefinitely with infinitely many repetitions of the sequent $\mathsf{C}P, \tilde{\mathsf{C}}\mathsf{C}P, P$. This tree has only one branch, which is infinite. And this branch contains only one infinite thread, the one that consists of the red underlined formulae in Fig. 2. And this thread is indeed a $\tilde{\mathsf{C}}$-thread.

It may seem that this branch also contains a C-thread because there are infinitely many applications of (C) in the branch. However, the principal formulae of these (C)-rules do not belong to one thread. In particular, the thread that starts from $\mathsf{C}P$ in the root sequent does not pass through $\mathsf{C}P$ in the premise of the $(\Box')$-rule shown in Fig. 2. Instead, this thread passes through $\mathsf{E}P \wedge \mathsf{E}\mathsf{C}P$, $\mathsf{E}P$, ..., $\Box_1 P$, and P and eventually disappears after the next application of $(\Box')$.

Now we are going to show that any sequent Γ has either an S-tree that proves it or an $\mathsf{S_{Dis}}$-tree that disproves it.

Let $\mathcal{T}$ be an $\mathsf{S_{Game}}$-tree for Γ. We define an infinite game for two players on $\mathcal{T}$. Intuitively, player I will try to show that Γ is provable while player II will try to show the opposite. The game is played as follows:

(i) the game starts at the root of $\mathcal{T}$,

(ii) at any $(\Box')$ node, player I chooses one of the children,

(iii) at any $(\wedge)$ node, player II chooses one of the children,

(iv) at all other non-leaf nodes, the only child is chosen by default.

Such a game results in a path in $\mathcal{T}$. In the case of a finite path, player I wins if the path ends in an axiom; otherwise, player II wins. In the case of an infinite path, player I wins if the path contains a C-thread; otherwise, player II wins.

Theorem 4.16 (i) *There is a winning strategy for player I if and only if there is an* S*-proof for* Γ *contained in* $\mathcal{T}$*.*

(ii) *There is a winning strategy for player II if and only if there is an* $\mathsf{S_{Dis}}$*-disproof for* Γ *contained in* $\mathcal{T}$*.*

Proof. For the first claim, if there is an S-proof for Γ contained in $\mathcal{T}$, then the winning strategy for player I is to stay in the nodes that belong to this proof. For the other direction, consider a winning strategy for player I. It induces an S-proof for Γ as follows: the root of $\mathcal{T}$ is the root of the proof; if a node is included in the proof and player I has to perform the next move, then we select the child prescribed by the winning strategy; if it is player II's move, then we include all the children in our proof. The proof of the second claim is similar. $\Box$

With the help of Martin's theorem [13] we can show that this game is determined, i.e., one of the players has a winning strategy. For details of this argument, see [9,15]. We obtain the following as a corollary:

Theorem 4.17 *Let* $\mathcal{T}$ *be an* $\mathsf{S_{Game}}$*-tree for* Γ*. Then there exists either an* S*-proof for* Γ *in* $\mathcal{T}$ *or an* $\mathsf{S_{Dis}}$*-disproof for* Γ *in* $\mathcal{T}$*.*

It remains to show that from a given $\mathsf{S_{Dis}}$-disproof for Γ, we can construct a countermodel for Γ.

Definition 4.18 Consider an $\mathsf{S_{Dis}}$-tree $\mathcal{T}$ that disproves a sequent Γ. The Kripke structure $\mathcal{M}^{\mathcal{T}} = (S^{\mathcal{T}}, R_1^{\mathcal{T}}, \dots, R_h^{\mathcal{T}}, \pi^{\mathcal{T}})$ *induced* by $\mathcal{T}$ is defined as follows:

(i) $S^{\mathcal{T}}$ consists of all occurrences of sequents in the conclusions of applications of $(\Box')$ in $\mathcal{T}$ as well as of all occurrences of sequents in the leaves of $\mathcal{T}$,

(ii) $R_i^{\mathcal{T}}(\Gamma, \Delta)$ holds if there is exactly one application of $(\Box')$ in between Γ and Δ and if there is a thread through Γ and Δ that contains $\Box_i A \in \Gamma$ and $A \in \Delta$ for some formula A,

(iii) $\pi^{\mathcal{T}}(P) := \{\Gamma \in S^{\mathcal{T}} : P \notin \Gamma\}$.

We can assign to each sequent Δ in $\mathcal{T}$ the corresponding state in $S^{\mathcal{T}}$ simply by finding the closest saturated descendant. We will denote this state by $\mathsf{sat}(\Delta)$.

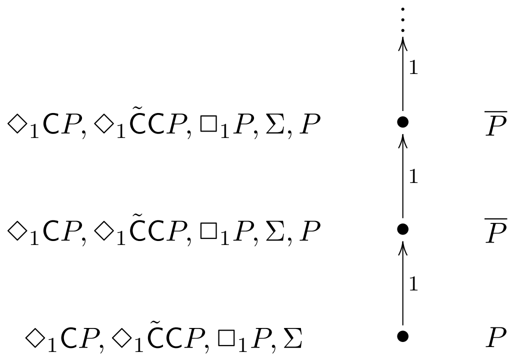

Fig. 3. The Kripke structure $\mathcal{M}^{\mathcal{T}}$ induced by the $\mathsf{S}_{\mathsf{Dis}}$-tree $\mathcal{T}$ from Example 4.15.

Example 4.19 The $\mathsf{S}_{\mathsf{Dis}}$-tree $\mathcal{T}$ constructed in Example 4.15 for $\tilde{\mathsf{C}}\overline{P} \to \tilde{\mathsf{C}}\mathsf{C}P$ induces a Kripke structure $\mathcal{M}^{\mathcal{T}}$ shown in Fig. 3. It is easy to see that

$$\mathcal{M}^{\mathcal{T}}, \quad \Diamond_1 \mathsf{C}P, \Diamond_1 \tilde{\mathsf{C}}\mathsf{C}P, \Box_1 P, \Sigma \quad \not\models \quad \tilde{\mathsf{C}}\overline{P} \to \tilde{\mathsf{C}}\mathsf{C}P \ .$$

Lemma 4.20 states that this is a general phenomenon: the root of the Kripke structure induced by a given $\mathsf{S}_{\mathsf{Dis}}$-tree falsifies the sequent at the root of the tree.

We define $\tilde{\delta}(A)$ to be the maximal number of nested $\tilde{\mathsf{C}}$ operators in A. Consider a Kripke structure $\mathcal{M}$, a state s, and a formula A. Let the $\tilde{\mathsf{C}}$-*signature* $\mathsf{sig}_{\tilde{\mathsf{C}}}(A, s)$ be the least sequence $\sigma = (\sigma_{\tilde{\delta}(A)}, \dots, \sigma_1)$ such that $\mathcal{M}, s \models^{\sigma}_{\tilde{\mathsf{C}}} A$. Here $\models^{\sigma}_{\tilde{\mathsf{C}}}$ is defined in the same way as $\models$ except in the case of $\tilde{\mathsf{C}}$, where we set $\mathcal{M}, v \models^{\sigma}_{\tilde{\mathsf{C}}} \tilde{\mathsf{C}}B$ if $\mathcal{M}, w \models^{\sigma}_{\tilde{\mathsf{C}}} B$ for some w for which there exists n with $\sigma_{\tilde{\delta}(\tilde{\mathsf{C}}B)} \geq n \geq 1$ and $\mathsf{reach}(v, w, n)$.

Lemma 4.20 *Consider an $\mathsf{S}_{\mathsf{Dis}}$-tree $\mathcal{T}$ that disproves the sequent $\Gamma = \{A\}$ for some formula A. Then $\mathcal{M}^{\mathcal{T}}, \mathsf{sat}(\Gamma) \not\models A$.*

Proof. Suppose that $\mathcal{M}^{\mathcal{T}}, \mathsf{sat}(\Gamma) \models A$. Then we can construct a C-thread in some branch of $\mathcal{T}$, which contradicts the assumption that $\mathcal{T}$ disproves A. We will simultaneously construct a branch $\Gamma_1, \Gamma_2, \dots$ and a thread $A_1, A_2, \dots$ in it such that

$$\mathcal{M}^{\mathcal{T}}, \mathsf{sat}(\Gamma_n) \models A_n \text{ for all } n. \tag{6}$$

We start with $\Gamma_1 := \Gamma$ and $A_1 := A$. Now assume that we have constructed the thread up to some element $A_n \in \Gamma_n$ with $\mathcal{M}^{\mathcal{T}}, \mathsf{sat}(\Gamma_n) \models A_n$. The next element is selected as follows:

(i) If a rule different from $(\Box')$ has been applied, then there is only one child of Γ_n and we let Γ_{n+1} be that child. We have $\mathsf{sat}(\Gamma_n) = \mathsf{sat}(\Gamma_{n+1})$ and distinguish the following cases:
  (a) A_n is not the principal formula. We set $A_{n+1} := A_n$.
  (b) $A_n = B \vee C$ is the principal formula. We set $A_{n+1} := B$ if

$$\mathsf{sig}_{\tilde{\mathsf{C}}}(B \vee C, \mathsf{sat}(\Gamma_n)) = \mathsf{sig}_{\tilde{\mathsf{C}}}(B, \mathsf{sat}(\Gamma_{n+1})) \ ;$$

  otherwise, we set $A_{n+1} := C$.

(c) $A_n = B \wedge C$ is the principal formula. We set $A_{n+1} := B$ if B occurs in Γ_{n+1}; otherwise, we set $A_{n+1} := C$.

(d) $A_n = \mathsf{C}B$ is the principal formula. Let $A_{n+1} := \mathsf{E}B \wedge \mathsf{E}\mathsf{C}B$.

(e) $A_n = \tilde{\mathsf{C}}B$ is the principal formula. Let $A_{n+1} := \tilde{\mathsf{E}}B \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}B$.

(ii) If ($\Box'$) has been applied, then we have $\mathsf{sat}(\Gamma_n) = \Gamma_n$. We distinguish the following cases:

(a) $A_n = \Box_i B$. There is a child where B is the active formula. Let Γ_{n+1} be that child and set $A_{n+1} := B$.

(b) $A_n = \Diamond_i B$. Because of $\mathcal{M}^{\mathcal{T}}, \mathsf{sat}(\Gamma_n) \models A_n$, there exists a state t such that $R_i^{\mathcal{T}}(\mathsf{sat}(\Gamma_n), t)$ and $\mathsf{sig}_{\tilde{\mathsf{C}}}(B, t) = \mathsf{sig}_{\tilde{\mathsf{C}}}(\Diamond_i B, \mathsf{sat}(\Gamma_n))$. The definition of $\mathcal{M}^{\mathcal{T}}$ implies that there is a child Γ' of Γ_n with $\mathsf{sat}(\Gamma') = t$. We set $\Gamma_{n+1} := \Gamma'$ and $A_{n+1} := B$.

(c) A_n is not of the form $\Box_i B$ or $\Diamond_i B$. Then there exists $A'_n \in \Gamma_n$ that is of this form such that $\mathcal{M}^{\mathcal{T}}, \Gamma_n \models A'_n$. We drop the thread constructed so far and continue instead with the thread from A to A'_n.

If the constructed thread were finite, then the last element Γ_n of the path would necessarily be a saturated sequent which would not contain formulae of the form $\Box_i B$. Then the definition of $\mathcal{M}^{\mathcal{T}}$ would imply that $\mathcal{M}^{\mathcal{T}}, \Gamma_n \not\models A_n$, which would contradict (6). Hence, the constructed thread is infinite. We can now use an argument about signatures similar to the one used in the soundness proof for S to show that the constructed thread cannot be a $\tilde{\mathsf{C}}$-thread. This contradicts the assumption that $\mathcal{T}$ disproves Γ. $\Box$

Theorem 4.21 (Completeness of S) *If A is a valid formula, then there exists an S-proof for it.*

Proof. Let A be a formula that is not provable in S. By Theorem 4.17, there exists an $\mathsf{S_{Dis}}$-tree that disproves A. Thus, by Lemma 4.20, there exists a countermodel for A. Hence, A is not valid. $\Box$

5 Conclusions

We have presented two systems $\mathsf{H_{Ax}}$ and S for common knowledge, which could be used to construct a justification counterpart for common knowledge. It appears that $\mathsf{H_{Ax}}$ is more suitable for this task than $\mathsf{H_R}$ as the latter has an additional rule, (I-R1), which may make it difficult to prove constructive necessitation, a property essential for justification logics. However, to establish a connection between the modal logic of common knowledge and its justification counterpart, the so-called Realization Theorem, a cut-free sequent calculus (akin to S) for the modal logic is ordinarily required. Furthermore, the system S might give us more insight into the nature of common knowledge evidence terms.

The idea of treating common knowledge evidence terms as co-inductive structures seems conceptually appealing but requires further investigation into the relationship between $\mathsf{H_{Ax}}$ and S. In particular, syntactic cut-elimination is vital for embedding $\mathsf{H_{Ax}}$ into S, which could shed a new light on how common knowledge emerges.

Acknowledgement

We thank the anonymous referees for encouraging and helpful comments.

References

[1] Alberucci, L. and G. Jäger, *About cut elimination for logics of common knowledge*, Annals of Pure and Applied Logic **133** (2005), pp. 73–99.
URL http://dx.doi.org/10.1016/j.apal.2004.10.004

[2] Antonakos, E., *Justified and common knowledge: Limited conservativity*, in: S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science, International Symposium, LFCS 2007, New York, NY, USA, June 4–7, 2007, Proceedings*, Lecture Notes in Computer Science **4514** (2007), pp. 1–11.
URL http://dx.doi.org/10.1007/978-3-540-72734-7_1

[3] Artemov, S. N., *Operational modal logic*, Technical Report MSI 95–29, Cornell University (1995).
URL http://www.cs.gc.cuny.edu/~sartemov/publications/MSI95-29.ps

[4] Artemov, S. N., *Explicit provability and constructive semantics*, Bulletin of Symbolic Logic **7** (2001), pp. 1–36.
URL http://www.jstor.org/stable/2687821

[5] Artemov, S. N., *Justified common knowledge*, Theoretical Computer Science **357** (2006), pp. 4–22.
URL http://dx.doi.org/10.1016/j.tcs.2006.03.009

[6] Artemov, S. N., *The logic of justification*, The Review of Symbolic Logic **1** (2008), pp. 477–513.
URL http://dx.doi.org/10.1017/S1755020308090060

[7] Artemov, S. N. and R. Kuznets, *Logical omniscience as a computational complexity problem*, in: A. Heifetz, editor, *Theoretical Aspects of Rationality and Knowledge, Proceedings of the Twelfth Conference (TARK 2009)*, 2009, pp. 14–23.
URL http://dx.doi.org/10.1145/1562814.1562821

[8] Bradfield, J. and C. Stirling, *Modal mu-calculi*, in: P. Blackburn, J. van Benthem and F. Wolter, editors, *Handbook of Modal Logic*, Studies in Logic and Practical Reasoning **3**, Elsevier, 2007 pp. 721–756.
URL http://dx.doi.org/10.1016/S1570-2464(07)80015-2

[9] Dax, C., M. Hofmann and M. Lange, *A proof system for the linear time μ-calculus*, in: S. Arun-Kumar and N. Garg, editors, *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science, 26th International Conference, Kolkata, India, December 13-15, 2006, Proceedings*, Lecture Notes in Computer Science **4337** (2006), pp. 273–284.
URL http://dx.doi.org/10.1007/11944836_26

[10] Fagin, R., J. Y. Halpern, Y. Moses and M. Y. Vardi, "Reasoning about Knowledge," MIT Press, 1995.

[11] Fitting, M., *The logic of proofs, semantically*, Annals of Pure and Applied Logic **132** (2005), pp. 1–25.
URL http://dx.doi.org/10.1016/j.apal.2004.04.009

[12] Kuznets, R., *Self-referential justifications in epistemic logic*, Theory of Computing Systems **Online First** (2009).
URL http://dx.doi.org/10.1007/s00224-009-9209-3

[13] Martin, D. A., *Borel determinacy*, Annals of Mathematics **102** (1975), pp. 363–371.
URL http://www.jstor.org/stable/1971035

[14] Meyer, J.-J. Ch. and W. van der Hoek, "Epistemic Logic for AI and Computer Science," Cambridge Tracts in Theoretical Computer Science **41**, Cambridge University Press, 1995.

[15] Niwiński, D. and I. Walukiewicz, *Games for the μ-calculus*, Theoretical Computer Science **163** (1996), pp. 99–116.
URL http://dx.doi.org/10.1016/0304-3975(95)00136-0

[16] Stirling, C. and D. Walker, *Local model checking in the modal mu-calculus*, Theoretical Computer Science **89** (1991), pp. 161–177.
URL http://dx.doi.org/10.1016/0304-3975(90)90110-4

[17] Streett, R. S. and E. A. Emerson, *An automata theoretic decision procedure for the propositional mu-calculus*, Information and Computation **81** (1989), pp. 249–264.
URL http://dx.doi.org/10.1016/0890-5401(89)90031-X

[18] Studer, T., *On the proof theory of the modal mu-calculus*, Studia Logica **89** (2008), pp. 343–363.
URL http://dx.doi.org/10.1007/s11225-008-9133-6