The Proof Theory of Common Knowledge

Michel Marti and Thomas Studer

Abstract Common knowledge of a proposition A can be characterized by the following infinitary conjunction: everybody knows A and everybody knows that everybody knows A and everybody knows that everybody knows that everybody knows A and so on. We present a survey of deductive systems for the logic of common knowledge. In particular, we present two different Hilbert-style axiomatizations and two infinitary cut-free sequent systems. Further we discuss the problem of syntactic cut-elimination for common knowledge. The paper concludes with a list of open problems.

Keywords Common knowledge, multi-agent systems, proof theory, infinitary deductive systems, cut-elimination

1 Introduction

Modal logic is a standard framework for reasoning about knowledge and belief (Hintikka, 1962). A necessity for this arises, for example, in the study of distributed multi-agent systems, say computers connected over a network. In this setting, agent i knowing some proposition P in a state s can be understood as P holding in all states that agent i can reach from s in one step. Hence agent i's knowledge may be modeled using a modal operator $\Box_i$.

Through arbitrary nestings of $\Box$-operators epistemic situations of considerable complexity may be modeled. However, there are certain situations of particular interest that the basic language of modal logic cannot talk about. One such example is *common knowledge* of a proposition P, which can roughly be viewed as the in-

Michel Marti
University of Bern, Neubrückstrasse 10, 3012 Bern, Switzerland, e-mail: mmarti@inf.unibe.ch

Thomas Studer
University of Bern, Neubrückstrasse 10, 3012 Bern, Switzerland, e-mail: tstuder@inf.unibe.ch

finitary conjunction *everybody knows that P and everybody knows that everybody knows that P and so on*.

Thus we extend the basic language with a new operator C where a formula $\mathsf{C}P$ means that *P is common knowledge*. We find that C is a normal modal operator, i.e., we have:

$$\mathsf{C}(A \to B) \to (\mathsf{C}A \to \mathsf{C}B). \tag{1}$$

We let the formula $\mathsf{E}A$ stand for *everbody knows that A*, i.e., if we consider h agents,

$$\mathsf{E}A := \Box_1 A \wedge \cdots \wedge \Box_h A.$$

It can be shown that common knowledge also satisfies the following induction principle:

$$A \wedge \mathsf{C}(A \to \mathsf{E}A) \to \mathsf{C}A. \tag{2}$$

Hintikka's work on epistemic logic is direct precursor to logics of common knowledge, although he did not consider fixpoint constructions (Hintikka, 1962). It was Lewis (1969) who carried out the classic study of the notion of common knowledge where part of his work, as he acknowledges, has been inspired by Schelling (1960). Aumann in his seminal paper (Aumann, 1976) gives the first mathematically rigorous formulation of common knowledge, which uses a set-theoretic setting. A definition of common knowledge in terms of epistemic logic has been given by Schiffer (1972). Halpern and Moses (1990) adopt this approach and introduce the *logic of common knowledge*, which is based on classical multi-modal logic. In particular, they show that the syntactic and set-theoretic approaches to common knowledge are logically equivalent, see (5) below. Another possibility to formalize common knowledge is in Barwise's situation semantics (Barwise, 1988, 1989) where common knowledge is given by a greatest fixed point construction. It turns out that in situation semantics the definitions of common knowledge as infinite conjunction and as greatest fixed point differ whereas in multi-modal logic they coincide. The textbooks by Fagin et al. (1995) and by Meyer and van der Hoek (1995) present and investigate many applications of the logic of common knowledge.

The problem of coordinated attack is a standard example to illustrate the mechanism of common knowledge. Let us briefly recall this classical problem where we follow the presentation given in (Fagin et al., 1995) and (Bucheli et al., 2011).

Suppose two divisions of an army, located in different places, are about to attack their enemy. They have some means of communication but they may be unreliable (i.e. messages may get lost), and the only way to secure a victory is to attack simultaneously. The problem now is: how should generals G and H, who command the two divisions, coordinate their attack? Of course, general G could send a message with the time of attack to general H. We use the proposition *del* to denote the fact that the message with the time of attack has been delivered. Thus general H upon receiving the message, knows the time of attack, i.e., $\Box_H del$. However, since communication is unreliable, general G considers it possible that his message has not been delivered, i.e., $\neg\Box_G\Box_H del$. But if general H sends an acknowledgment, he in turn cannot be

sure whether the acknowledgment has been delivered, i.e., $\neg\Box_H\Box_G\Box_H del$. Hence yet another acknowledgment is needed, and so on.

We now show that common knowledge of *del* is a necessary condition for the attack. Indeed, it is reasonable to assume it to be common knowledge between the generals that they should only attack simultaneously or not attack at all, i.e., that they attack only if both know that they attack, i.e.,

$$\mathsf{C}(att \to \mathsf{E}\, att).$$

Thus by (2) we obtain

$$att \to \mathsf{C}\, att. \tag{3}$$

A further reasonable assumption is that it is common knowledge that neither general attacks unless the message with the time of attack has been delivered, i.e.,

$$\mathsf{C}(att \to del).$$

Thus by (1) we obtain

$$\mathsf{C}\, att \to \mathsf{C}\, del. \tag{4}$$

Taking (3) and (4) together we obtain

$$att \to \mathsf{C}\, del,$$

which means that the generals attack only if it is common knowledge that the message has been delivered.

However, common knowledge of *del* cannot be achieved and consequently no attack will take place, no matter how many messages and acknowledgments are sent by the generals, even if all the messages are successfully delivered. The reason is, of course, that the sender of the last message always considers the possibility that his last message has not been delivered. Fagin et al. (1995) formally carry out this argument in detail.

In this paper, we study deductive systems for the logic of common knowledge. After defining the language and semantics of common knowledge, we present two Hilbert-style axiomatizations: one that is based on a greatest fixed point rule and one that is based on an induction axiom. Then we study two cut-free sequent systems for common knowledge. The first system includes an ω-rule to capture the greatest fixed point property of common knowledge whereas the second system features proofs with infinite branches equipped with a global soundness condition. In the last part of the paper we show how syntactic cut-elimination for the logic of common knowledge can be achieved by using nested sequents and deep inference.

We only consider systems with traditional common knowledge as introduced in (Halpern and Moses, 1990), that is we assume that common knowledge satisfies the induction principle (2). Lewis (1969) originally introduced a form of common knowledge that does not have this property. McCarthy studied that version of common knowledge under the name *any fool knows* (McCarty et al., 1978). Nowadays

it is often called *generic common knowledge* and investigated, e.g., by Antonakos (2007, 2016) and Artemov (2006).

Another variant of the logic of common knowledge is obtained by replacing the base logic with an intuitionistic modal logic. Recently, Jäger and Marti (2015) followed this approach and introduced a system for intuitionistic common knowledge.

We restrict this survey to work which is directly related to the proof theory of the logic of common knowledge. However, there is a lot of work on sequent calculi for LTL and PDL, which is very closely related since they are all fixpoint logics, e.g., Gudzhinskas (1982) and Paech (1989). Similarly, there is a lot of work on tableaux calculi for these logics, e.g., Goré (2014).

2 Language and Semantics

2.1 Language

Definition 1 (Formula). We consider a language with h agents for some natural number $h > 0$. Let Prop be a countable set of atomic propositions. The *formulas* of our language are inductively defined by:

1. if $P \in \mathsf{Prop}$, then P and its negation $\overline{P}$ are formulas,
2. if A and B are formulas, so are $(A \wedge B)$ and $(A \vee B)$,
3. if A is a formula, so are $\Box_i A$ and $\Diamond_i A$ for $1 \leq i \leq h$,
4. if A is a formula, so are $\mathsf{C}A$ and $\tilde{\mathsf{C}}A$.

In case there is no danger of confusion, we will omit parentheses in formulas.

The formula $\Box_i A$ is read as *agent i knows that 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 dual operators. Note that formulas are a priori in negation normal form. The negation $\neg A$ of a formula A is defined as usual using de Morgan's laws, the law of double negation, and the duality laws for modal operators. For formulas A and B we introduce implication as usual by $A \to B := \neg A \vee B$.

We define the following abbreviations:

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

Thus $\mathsf{E}A$ stands for *everybody knows that A*. We will also need iterated applications of these operators:

$$\mathsf{E}^1 A := \mathsf{E}A \quad \text{and} \quad \mathsf{E}^{n+1} A := \mathsf{E}\mathsf{E}^n A,$$
$$\tilde{\mathsf{E}}^1 A := \tilde{\mathsf{E}}A \quad \text{and} \quad \tilde{\mathsf{E}}^{n+1} A := \tilde{\mathsf{E}}\tilde{\mathsf{E}}^n A.$$

Definition 2 (Length of a formula). We define the *length* $\mathsf{ln}(A)$ of a formula A inductively by:

1. $\mathsf{ln}(P) := \mathsf{ln}(\overline{P}) := 1$ for $P \in \mathsf{Prop}$,
2. $\mathsf{ln}(B \wedge C) := \mathsf{ln}(B \vee C) := \mathsf{ln}(B) + \mathsf{ln}(C)$,
3. $\mathsf{ln}(\Box_i B) := \mathsf{ln}(\Diamond_i B) := \mathsf{ln}(B) + 1$,
4. $\mathsf{ln}(\mathsf{C}B) := \mathsf{ln}(\tilde{\mathsf{C}}B) := \mathsf{ln}(B) \cdot h + h + 1$.

Definition 3 (Rank of a formula). We define the *rank* $\mathsf{rk}(A)$ of a formula A inductively by:

1. $\mathsf{rk}(P) := \mathsf{rk}(\overline{P}) := 0$,
2. $\mathsf{rk}(A \wedge B) := \mathsf{rk}(A \vee B) := \max(\mathsf{rk}(A), \mathsf{rk}(B)) + 1$,
3. $\mathsf{rk}(\Box_i A) := \mathsf{rk}(\Diamond_i A) := \mathsf{rk}(A) + 1$,
4. $\mathsf{rk}(\mathsf{C}A) := \mathsf{rk}(\tilde{\mathsf{C}}A) := \omega + \mathsf{rk}(A)$.

The length of a formula is a natural number whereas the rank of a formula may be a transfinite ordinal. We find $\mathsf{rk}(\mathsf{C}A) > \mathsf{rk}(\mathsf{E}^m A)$ for any natural number m.

2.2 Semantics

We employ standard Kripke semantics for modal logics to give meaning to formulas. We use $\mathscr{P}(X)$ to denote the power set of a set X.

Definition 4 (Kripke Structure). A *Kripke structure* $\mathsf{K} = (S, R_1, \ldots, R_h, \pi)$ is a tuple where

1. S is a non-empty set,
2. $R_i \subseteq S \times S$ for all $1 \leq i \leq h$,
3. $\pi : \mathsf{Prop} \to \mathscr{P}(S)$.

We call S the set of states, R_i an accessibility relation, and π the valuation function of the Kripke structure K.

Assume we are given a Kripke structure $\mathsf{K} = (S, R_1, \ldots, R_h, \pi)$ and a formula A. We define the set of states $\|A\|_{\mathsf{K}}$ of K at which A holds by induction on the structure of A.

Definition 5 (Denotation). Let $\mathsf{K} = (S, R_1, \ldots, R_h, \pi)$ be a Kripke structure and A be a formula. The set $\|A\|_{\mathsf{K}} \subseteq S$ is defined inductively by:

$$
\begin{aligned}
\|P\|_{\mathsf{K}} &:= \pi(P) \quad \text{for } P \in \mathsf{Prop} \\
\|\overline{P}\|_{\mathsf{K}} &:= S \setminus \pi(P) \quad \text{for } P \in \mathsf{Prop} \\
\|B \wedge C\|_{\mathsf{K}} &:= \|B\|_{\mathsf{K}} \cap \|C\|_{\mathsf{K}} \\
\|B \vee C\|_{\mathsf{K}} &:= \|B\|_{\mathsf{K}} \cup \|C\|_{\mathsf{K}} \\
\|\Box_i B\|_{\mathsf{K}} &:= \{w \in S \mid \text{for all } v \, \big(R_i(w,v) \text{ implies } v \in \|B\|_{\mathsf{K}}\big)\} \\
\|\Diamond_i B\|_{\mathsf{K}} &:= \{w \in S \mid \text{there exists } v \, \big(R_i(w,v) \text{ and } v \in \|B\|_{\mathsf{K}}\big)\} \\
\|\mathsf{C}B\|_{\mathsf{K}} &:= \bigcap \{\|\mathsf{E}^m A\|_{\mathsf{K}} \mid m \geq 1\} \\
\|\tilde{\mathsf{C}}B\|_{\mathsf{K}} &:= \bigcup \{\|\tilde{\mathsf{E}}^m A\|_{\mathsf{K}} \mid m \geq 1\}.
\end{aligned}
$$

Sometimes we write $\mathsf{K}, w \models A$ for $w \in \|A\|_{\mathsf{K}}$. We say that a formula A is *satisfiable* if there exists a Kripke structure K such that $\|A\|_{\mathsf{K}}$ is non-empty. For a Kripke structure $\mathsf{K} = (S, R_1, \ldots, R_h, \pi)$ and a formula A we write $\mathsf{K} \models A$ if $\|A\|_{\mathsf{K}} = S$. A formula A is called *valid* if for all Kripke structures K we have $\mathsf{K} \models A$.

Our semantics of the common knowledge operator reflects to so-called iterative approach where $\mathsf{C}A$ is treated to be equivalent to the infinite conjuction

$$\mathsf{E}^1 A \wedge \mathsf{E}^2 A \wedge \mathsf{E}^3 A \wedge \cdots.$$

Alternatively, we could interpret common knowledge as a greatest fixed point since for $\mathsf{K} = (S, R_1, \ldots, R_h, \pi)$ we have

$$\|\mathsf{C}A\|_{\mathsf{K}} = \bigcup \{X \subset S \mid X = \|\mathsf{E}A \wedge EP\|_{\mathsf{K}[P:=X]}\} \tag{5}$$

where P is an atomic proposition that does not occur in A and $\mathsf{K}[P := X]$ is a Kripke structure like K except that the valuation function maps P to X. A proof of (5) can be found in (Fagin et al., 1995).

The logic of common knowledge enjoys the small model property. Proofs are given, for instance, in (Fagin et al., 1995; Meyer and van der Hoek, 1995).

Theorem 1 (Small model property). *If a formula A is satisfiable , then there exists a Kripke structure K with at most $2^{\ln(A)}$ states such that $\|A\|_{\mathsf{K}} \neq \emptyset$.*

3 Hilbert-Style Systems

We have seen that there are several equivalent ways to define the semantics for common knowledge. There are also several ways to axiomatize common knowledge. In this section, we first present a deductive system that includes a greatest fixed point rule for common knowledge. Then we introduce a system that axiomatizes common knowledge via an induction principle.

3.1 Induction rule

Definition 6 (The system $\mathsf{H}_{\mathsf{I\text{-}R}}$). The Hilbert calculus $\mathsf{H}_{\mathsf{I\text{-}R}}$ for the logic of common knowledge is defined by the following axioms and inference rules:

Propositional axioms.

All instances of propositional tautologies

Modal axioms. For all formulas A and B and all $1 \leq i \leq h$,

$$\Box_i(A \to B) \to (\Box_i A \to \Box_i B)$$

Closure axioms. For all formulas A,

$$\mathsf{C}A \to \mathsf{E}(A \wedge \mathsf{C}A)$$

Modus ponens. For all formulas A and B,

$$\frac{A \quad A \to B}{B}$$

Necessitation. For all formulas A and all $1 \leq i \leq h$,

$$\frac{A}{\Box_i A}$$

Induction rule. For all formulas A and B,

$$\frac{B \to \mathsf{E}(A \wedge B)}{B \to \mathsf{C}A}$$

The induction rule states that if a formula B satisfies the closure axiom, i.e., $B \to \mathsf{E}(A \wedge B)$ is valid, then $B \to \mathsf{C}A$ is also valid. This can be read as *if B satisfies the closure axiom, then the extension of B is smaller than the extension of $\mathsf{C}A$*. Hence $\mathsf{C}A$ is the greatest formula satisfying the closure axiom.

Theorem 2 (Soundness and completeness of $\mathsf{H}_{\mathsf{I\text{-}R}}$). *For any formula A we have that*

$$A \text{ is valid} \quad \text{if and only if} \quad \mathsf{H}_{\mathsf{I\text{-}R}} \vdash A.$$

A proof is given in (Fagin et al., 1995).

3.2 Induction Axiom

Definition 7 (The system $\mathsf{H}_{\mathsf{I\text{-}A}}$). The Hilbert calculus $\mathsf{H}_{\mathsf{I\text{-}A}}$ for the logic of common knowledge consists of the axioms and rules of $\mathsf{H}_{\mathsf{I\text{-}R}}$ whereby the induction rule is replaced by the following axioms and rules:

C-modal axioms. For all formulas A and B,

$$\mathsf{C}(A \to B) \to (\mathsf{C}A \to \mathsf{C}B)$$

C-necessitation. For all formulas A,

$$\frac{A}{\mathsf{C}A}$$

Induction axioms. For all formulas A,

$$\mathsf{E}A \wedge \mathsf{C}(A \to \mathsf{E}A) \to \mathsf{C}A$$

In (Meyer and van der Hoek, 1995), the induction axiom is introduced as

$$A \wedge \mathsf{C}(A \to \mathsf{E}A) \to \mathsf{C}A,$$

see also (2). However, in our present setting this would not be sound since we do not define common knowledge to be reflexive.

The proof-theoretic relationship between the induction rule and the induction axiom is studied in (Bucheli et al., 2010) where it is shown that the induction rule of $\mathsf{H}_{\mathsf{I\text{-}R}}$ is derivable in $\mathsf{H}_{\mathsf{I\text{-}A}}$. Thus we have for all formulas A,

$$\mathsf{H}_{\mathsf{I\text{-}R}} \vdash A \quad \text{implies} \quad \mathsf{H}_{\mathsf{I\text{-}A}} \vdash A.$$

Therefore, completeness of $\mathsf{H}_{\mathsf{I\text{-}R}}$ implies completeness of $\mathsf{H}_{\mathsf{I\text{-}A}}$. Meyer and van der Hoek (1995) present a direct proof of completeness for $\mathsf{H}_{\mathsf{I\text{-}A}}$. Soundness of $\mathsf{H}_{\mathsf{I\text{-}A}}$ is established, e.g., in (Bucheli et al., 2010; Meyer and van der Hoek, 1995).

Theorem 3 (Soundness and completeness of $\mathsf{H}_{\mathsf{I\text{-}A}}$). *For any formula A we have that*

$$A \text{ is valid} \quad \text{if and only if} \quad \mathsf{H}_{\mathsf{I\text{-}A}} \vdash A.$$

4 Cut-Free Sequent Systems

In this section, we study deductive systems that derive *sequents*, that is finite sets of formulas. We use $\Gamma, \Delta, \ldots$ to denote sequents and for $\Gamma = \{A_1, \ldots, A_n\}$ set:

$$\Diamond_i \Gamma := \{\Diamond_i A_1, \ldots, \Diamond_i A_n\} \quad \text{and} \quad \tilde{\mathsf{C}}\Gamma := \{\tilde{\mathsf{C}}A_1, \ldots, \tilde{\mathsf{C}}A_n\}.$$

4.1 Infinitary rule

The pioneering work on the proof theory of common knowledge is (Alberucci and Jäger, 2005), which introduces Tait-style systems, i.e., systems deriving finite sets of formulas, for the logic of common knowledge. Alberucci and Jäger show that a system with an induction rule would not be complete without a cut rule. In order to obtain a cut-free sequent calculus for common knowledge, they introduce an ω-rule of the following form: if $\mathsf{E}^k A$ is derivable for every natural number k, then one may infer $\mathsf{C}A$. Based on this rule with infinitely many premises, they introduce the infinitary cut-free system G.

Definition 8 (The system G). The system G consists of the following axioms and rules:

$$\Gamma, P, \overline{P}$$

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

$$\frac{\Gamma, \tilde{\mathsf{C}}\Delta, A}{\Diamond_i \Gamma, \tilde{\mathsf{C}}\Delta, \Box_i A, \Sigma}$$

$$\frac{\Gamma, \mathsf{E}^k A \quad \text{for all } k \geq 1}{\Gamma, \mathsf{C}A} \qquad \frac{\Gamma, \Diamond A}{\Gamma, \tilde{\mathsf{C}}A}$$

Observe that the system G does not include a cut rule.

Definition 9 (The system $\mathsf{G}+(\mathsf{cut})$). The system $\mathsf{G}+(\mathsf{cut})$ is obtained from the system G by adding the cut rule

$$\frac{\Gamma, A \quad \Gamma, \neg A}{\Gamma}.$$

It is standard to embed $\mathsf{H}_{\mathsf{I\text{-}R}}$ into $\mathsf{G}+(\mathsf{cut})$, which yields completeness of $\mathsf{G}+(\mathsf{cut})$. We have the following result.

Theorem 4 (Soundness and completeness of $\mathsf{G}+(\mathsf{cut})$). *For any formula A we have that*

$$A \text{ is valid} \quad \text{if and only if} \quad \mathsf{G}+(\mathsf{cut}) \vdash A.$$

Alberucci and Jäger (2005) establish completeness of the cut-free system G by a canonical model construction.

Theorem 5 (Soundness and completeness of G). *For any formula A we have that*

$$A \text{ is valid} \quad \text{if and only if} \quad \mathsf{G} \vdash A.$$

There is an alternative completeness proof for G available. Kretz and Studer (2006) apply the method of deduction chains to the logic of common knowledge. This method systematically tries to build a proof tree of a given formula A and, in case that fails, constructs a countermodel for A from the proof search tree.

Derivations in G may have infinite depth only because of the ω-rule. If we succeed in restricting the number of premises of each application of the ω-rule to a finite subset, then all proofs will be finite. This can be achieved by exploiting the small model property of the logic of common knowledge, which leads to the system $\mathsf{G}^{<\omega}$ below (Jäger et al., 2007). A similar approach for PDL appears in (Leivant, 1981).

For a sequent $\Gamma = \{B_1, \ldots, B_n\}$ and a formula A we define the *bounding function* bd by

$$\mathsf{bd}(A, \Gamma) := 2^{\mathsf{ln}(\mathsf{C}A)+\mathsf{ln}(B_1)+\cdots\mathsf{ln}(B_n)}.$$

Definition 10 (The system $\mathsf{G}^{<\omega}$). The system $\mathsf{G}^{<\omega}$ is obtained from the system G by replacing the ω-rule with the *bounded ω-rule*

$$\frac{\Gamma, \mathsf{E}^1 A \quad \Gamma, \mathsf{E}^2 A \quad \cdots \quad \Gamma, \mathsf{E}^{\mathsf{bd}(A,\Gamma)} A}{\Gamma, \mathsf{C}A, \Sigma}$$

The addition of a (possibly empty) set Σ of side formulas in the conclusion of this rule is necessary for making it stable under weakening.

Of course, the completeness of $\mathsf{G}^{<\omega}$ immediately follows from the completeness of G. To obtain soundness of $\mathsf{G}^{<\omega}$, we make use of the small model property as follows (Jäger et al., 2007). Assume that the conclusion $\Gamma, \mathsf{C}A$ of an instance of the bounded ω-rule is not valid. By the small model property, there exists a counter-model with at most $\mathsf{bd}(A,\Gamma)$ many states. Using some basic facts about monotone operators we conclude that it must also be a counter-model to $\Gamma, \mathsf{E}^{\mathsf{bd}(A,\Gamma)}A$. Therefore, the bounded ω-rule preserves validity. The soundness of $\mathsf{G}^{<\omega}$ now follows as usual by induction on the length of derivations.

Theorem 6 (Soundness and completeness of $\mathsf{G}^{<\omega}$). *For any formula A we have that*

$$A \text{ is valid} \quad \text{if and only if} \quad \mathsf{G}^{<\omega} \vdash A.$$

4.2 Co-induction

Proofs in the system G are trees that are infinitely branching but each branch has finite length. Now we present the system G^{∞}, in which proof trees are only finitely branching but the branches may have infinite length. Niwinski and Walukiewicz (1996) introduced the first system of this kind for the modal μ-calculus. The system G^{∞} has been introduced by Bucheli et al. (2010).

Definition 11 (Preproof). 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:

$$\Gamma, P, \overline{P}\ (\mathrm{ax})$$

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

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

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

We now introduce the notion of a thread in a branch of a preproof.

Definition 12. The *principal formula* of a rule is the formula that is explicitly displayed in the conclusion of the rule. The *active formulas* of a rule are those formulas that are explicitly displayed in the premise(s) of the rule. The formulas in Γ and Σ are called *side formulas* of a rule.

Definition 13. Consider a given preproof for some sequent. For all rule applications r that occur in it, we define a connection relation $\mathsf{Con}(r)$ on formulas as follows:

1. 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.
2. 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 $(\Diamond_i A, A) \in \mathsf{Con}(r)$ if $\Diamond_i A \in \Diamond_i \Gamma$.

Definition 14. Consider a finite or infinite branch $\Gamma_0, \Gamma_1, \ldots$ in a given preproof. 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 formulas $A_0, A_1, \ldots$ 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 15. Consider an infinite branch of a given preproof for some sequent Γ. An infinite thread in this branch is called a C*-thread* if infinitely many of its formulas are the principal formula of an application of (C).

Definition 16 (G^∞-proof). A G^∞-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. As usual, we write $\mathsf{G}^\infty \vdash \Gamma$ if there exists a G^∞-proof of Γ.

We will illustrate how G^∞-proofs work by showing a derivation of the induction axiom in G^∞. To do so, we need the two results:

1. Generalized axioms are provable in G^∞:

$$\mathsf{G}^\infty \vdash \Gamma, A, \neg A$$

   Note that generalized axioms may require infinite proofs in G^∞, e.g., in the case of $A = \mathsf{C}B$.
2. The following analogue of the $(\Box)$-rule is derivable in G^∞:

$$\frac{\Gamma, A}{\tilde{\mathsf{E}}\Gamma, \mathsf{E}A, \Sigma}$$

Example 1. Figure 1 shows a G^∞-proof of the induction axiom expressed in sequence form as $\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A$. Note the two of the topmost nodes are labelled with generalized axioms. The only infinite branch (outside the derivations of the generalized axioms) 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 a proof, we need to exhibit a C-thread in this branch. The thread that consists of the rightmost formulas is such a thread.

The soundness proof essentially uses the idea that underlies the fundamental semantic theorem of the modal μ-calculus (Streett and Emerson, 1989).

We let $\delta(A)$ denote the maximal number of nested C-operators in the formula A. We have, e.g., $\delta(\mathsf{C}(\mathsf{C}P \vee \mathsf{C}Q)) = 2$. Given $m \geq 1$ and a sequence $\sigma = (\sigma_m, \ldots, \sigma_1)$ of ordinals with $\sigma_i \leq \omega$, for all formulas A such that $\delta(A) \leq m$ we define $\|A\|^\sigma_{\mathsf{K}}$ like $\|A\|_{\mathsf{K}}$ except in the case of C, where we set

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

Fig. 1 G^∞-proof of the induction axiom

$$\|\mathsf{C}B\|^\sigma_\mathsf{K} := \bigcap \{ \|\mathsf{E}^m A\|_\mathsf{K} \mid \sigma_{\delta(\mathsf{C}B)} \geq m \geq 1 \}.$$

We write $\mathsf{K}, v \models^\sigma A$ for $v \in \|A\|^\sigma_\mathsf{K}$. We immediately obtain the following simple facts:

$$\mathsf{K}, v \models^{(\sigma_m, \ldots, \sigma_{\delta(\mathsf{C}B)}+1, \ldots, \sigma_1)} \mathsf{C}B \quad \text{iff} \quad \mathsf{K}, v \models^{(\sigma_m, \ldots, \sigma_{\delta(\mathsf{C}B)}, \ldots, \sigma_1)} \mathsf{E}B \wedge \mathsf{E}\mathsf{C}B. \tag{6}$$

$$\mathsf{K}, v \not\models A \quad \text{implies that there exists } \sigma \text{ such that } \mathsf{K}, v \not\models^\sigma A. \tag{7}$$

Further we have the following lemma, which is shown in (Bucheli, 2012; Bucheli et al., 2010).

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

Given two sequences σ and τ of equal 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 7 (Soundness of G^∞). *For any formula A we have that*

$$\mathsf{G}^\infty \vdash A \quad \textit{implies} \quad A \textit{ is valid}.$$

Proof. Assume that A is not valid yet there is a G^∞-proof $\mathscr{T}$ for it. Then there is a Kripke structure K with a state s such that $s \notin \|A\|_\mathsf{K}$, which we will use to construct a branch $\Gamma_0, \Gamma_1, \ldots$ with the corresponding rule applications $r_0, r_1, \ldots$ in $\mathscr{T}$ and a sequence $s_0, s_1, \ldots$ of states in K such that

$$s_i \notin \| \bigvee \Gamma_i \|_\mathsf{K} \text{ and} \tag{8}$$

$$\text{if } (B, C) \in \mathsf{Con}(r_i), C \in \Gamma_{i+1}, \text{ and } s_i \notin \|B\|^\sigma_\mathsf{K}, \text{ then } s_{i+1} \notin \|C\|^\sigma_\mathsf{K}. \tag{9}$$

Let $\Gamma_0 := A$ and $s_0 := s$. Suppose 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 (8), Γ_i cannot be axiomatic and thus must have been inferred by some rule.

1. $r_i = (\Box)$. Let $\Box_k B \in \Gamma_i$ be the principal formula of r_i. Let σ be the least sequence such that $s_i \notin \|\Box_k B\|^\sigma_{\mathsf{K}}$. By Lemma 1 there exists a state s_{i+1} such that (8) and (9) hold. We let Γ_{i+1} be the unique premise of r_i.
2. $r_i = (\wedge)$. Let $B_1 \wedge B_2 \in \Gamma_i$ be the principal formula of r_i. Let σ be the least sequence such that $s_i \notin \|B_1 \wedge B_2\|^\sigma_{\mathsf{K}}$. Let Γ_{i+1} be the j-th premise of r_i such that $s_i \notin \|B_j\|^\sigma_{\mathsf{K}}$. Further set $s_{i+1} := s_i$. This construction guarantees (8) and (9).
3. In all other cases, r_i has a unique premise Δ. We set $s_{i+1} := s_i$ and $\Gamma_{i+1} := \Delta$. Again (8) and (9) hold.

We have constructed an infinite branch in $\mathscr{T}$. Since $\mathscr{T}$ is a G^∞-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 $s_j \notin \|A_j\|^{\sigma^j}_{\mathsf{K}}$. Note that this σ^j exists by (7). From (9) we obtain $\sigma^{j+1} \leq \sigma^j$ for all j. Moreover, because we are considering a C-thread, there are infinitely many applications of (C), which, by (6), implies that there are infinitely many j's with $\sigma^{j+1} < \sigma^j$. This contradicts the well-foundedness of $<$. $\Box$

Now we sketch the completeness proof for G^∞, which is based on game-theoretic results.

Definition 17 (Saturated sequent). A sequent Γ is called *saturated* if all of the following hold:

1. if $A \wedge B \in \Gamma$, then $A \in \Gamma$ or $B \in \Gamma$,
2. if $A \vee B \in \Gamma$, then $A \in \Gamma$ and $B \in \Gamma$,
3. if $\mathsf{C}A \in \Gamma$, then $\mathsf{E}A \wedge \mathsf{E}\,\mathsf{C}A \in \Gamma$,
4. if $\tilde{\mathsf{C}}A \in \Gamma$, then $\mathsf{E}A \vee \tilde{\mathsf{E}}\,\tilde{\mathsf{C}}A \in \Gamma$.

Definition 18 ($\mathsf{G}^{\mathsf{Game}}$-tree). A $\mathsf{G}^{\mathsf{Game}}$-tree is built using the rules for G^∞-preproofs whereby the rule $(\Box)$ is replaced by the following rule.

Let $1 \leq m \leq h$, $H = \{h_1, \ldots, h_m\} \subseteq \{1, \ldots, h\}$, and $n_{h_1}, \ldots, n_{h_m}$ be positive integers. For all saturated sequents Σ that contain neither formulas that start with $\Diamond_j$ with $j \in H$ nor formulas that start with $\Box_i$ with $1 \leq i \leq h$, all sequents Γ_j with $j \in H$, and all formulas $A_{j,1}, \ldots, A_{j,n_j}$ with $j \in H$

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

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

A $\mathsf{G}^{\mathsf{Game}}$-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:

1. 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.

2. Apply $(\Box')$ backwards if possible.

Next we present a system $\mathsf{G}^{\mathsf{Dis}}$ 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 19 ($\mathsf{G}^{\mathsf{Dis}}$-tree). A $\mathsf{G}^{\mathsf{Dis}}$-tree is built using the rules for $\mathsf{G}^{\mathsf{Game}}$-trees where the rule $(\wedge)$ is replaced by the following two rules:

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

A $\mathsf{G}^{\mathsf{Dis}}$-tree is built in the same way as a $\mathsf{G}^{\mathsf{Game}}$-tree except that $(\wedge 1)$ and $(\wedge 2)$ are used instead of $(\wedge)$.

The notions of a thread and a C-thread are extended to $\mathsf{G}^{\mathsf{Game}}$- and $\mathsf{G}^{\mathsf{Dis}}$-trees. A $\tilde{\mathsf{C}}$-thread is a thread that contains infinitely many principal formulas 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 20. We say that a $\mathsf{G}^{\mathsf{Dis}}$-tree for a sequent Γ *disproves* Γ if

1. no branch ends with an axiom and
2. any infinite thread in any branch is a $\tilde{\mathsf{C}}$-thread.

A $\mathsf{G}^{\mathsf{Dis}}$-*disproof for* Γ is a $\mathsf{G}^{\mathsf{Dis}}$-tree that disproves Γ.

Now we are going to show that every sequent Γ has either a G^{∞}-tree that proves it or a $\mathsf{G}^{\mathsf{Dis}}$-tree that disproves it.

Let $\mathscr{T}$ be an $\mathsf{G}^{\mathsf{Game}}$-tree for Γ. We define an infinite game for two players on $\mathscr{T}$. Informally, player I will try to show that Γ is provable while player II will try to show that it is disprovable. The game is played as follows:

1. the game starts at the root of $\mathscr{T}$,
2. at any $(\Box')$-node, player I chooses one the the children,
3. at any $(\wedge)$-node, player II chooses one the the children,
4. at all other non-leaf nodes, the only child is chosen by default.

Such a game results in a path in $\mathscr{T}$. 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.

We immediately get the following theorem.

Theorem 8. *1. There is a winning strategy for player I if and only if there is a* G^{∞}*-proof for* Γ *contained in* $\mathscr{T}$.
2. There is a winning strategy for player II if and only if there is a $\mathsf{G}^{\mathsf{Dis}}$*-disproof for* Γ *contained in* $\mathscr{T}$.

With the help of Martin's theorem (Martin, 1975) we can show that this game is determined, i.e. one of the players has a winning strategy. For details of this argument see, e.g., (Niwinski and Walukiewicz, 1996). We obtain the following corollary.

Corollary 1. *Let $\mathscr{T}$ be a $\mathsf{G}^{\mathsf{Game}}$-tree for Γ. There exists either an G^{∞}-proof for Γ in $\mathscr{T}$ or an $\mathsf{G}^{\mathsf{Dis}}$-disproof for Γ in $\mathscr{T}$.*

It remains to note that from a given $\mathsf{G}^{\mathsf{Dis}}$-disproof for Γ one can construct a countermodel for Γ. In (Bucheli et al., 2010) the following lemma is established.

Lemma 2. *Consider a $\mathsf{G}^{\mathsf{Dis}}$-disproof $\mathscr{T}$ for $\Gamma = \{A\}$ for some formula A. There exists a Kripke structure $\mathsf{K}_{\mathscr{T}}$ with a set of worlds $S_{\mathscr{T}}$ such that $\|A\|_{\mathsf{K}_{\mathscr{T}}} \neq S_{\mathscr{T}}$.*

Theorem 9 (Completeness of G^{∞}). *For any formula A we have that*

$$A \text{ is valid} \quad \text{implies} \quad \mathsf{G}^{\infty} \vdash A.$$

Proof. We show the contrapositive. Assume that A is a formula that is not provable in G^{∞}. By Corollary 1 there exists a $\mathsf{G}^{\mathsf{Dis}}$-disproof for A. By Lemma 2 there exists a countermodel for A. Hence A is not valid. □

Although G^{∞}-proofs may be infinite objects, the system G^{∞} can be used to obtain an efficient decidability algorithm for the logic of common knowledge. The idea of this proof procedure is, very roughly, the following. Consider a formula A and the alphabet Ψ that consists of all sequents that may appear in a G^{∞}-proof of A. Thus a branch in a G^{∞}-preproof corresponds to an infinite word over Ψ. We define an automaton $\mathscr{A}$ on infinite words that accepts exactly those words that contain a C-thread. Further we define an automaton $\mathscr{B}$ on infinite trees that accepts exactly the G^{∞}-preproofs for the formula A. Then we construct a product automaton $\mathscr{A} \times \mathscr{B}$ that accepts exactly the G^{∞}-proofs for A. We find that the language of $\mathscr{A} \times \mathscr{B}$ is empty if and only if A is not provable. Since the emptiness problem for $\mathscr{A} \times \mathscr{B}$ is efficiently decidable we get a decision procedure for the logic of common knowledge. Details of this approach—in the context of the modal μ-calclus—are presented, e.g., in (Niwinski and Walukiewicz, 1996; Dax et al., 2006). An introduction to finite automata over infinite words and trees is given in (Grädel et al., 2002).

Another approach is to employ annotated sequents to keep track of possible C-threads. This makes it possible to finitize the system G^{∞}. The main idea is that during proof search, one can close a branch as axiomatic if—using the annotations—a cycle is detected that contains a C-thread. This method is based on focus games (Lange and Stirling, 2001) and has been employed to give finitary cut-free systems for temporal logics (Brünnler and Lange, 2008). Later Wehbe (2010) used it to present a system for common knowledge. However, in this context it is more natural to use relativized common knowledge (van Benthem et al., 2005), which corresponds to the temporal release-operator.

Abate et al. (2007) take a similar approach to obtain a decision procedure for common knowledge. They construct one-pass tableaux that also rely on annotations to find cyclic branches.

5 Syntactic Cut-Elimination

Syntactic cut-elimination refers to a procedure that, given a proof of a formula A containing instances of the cut-rule, effectively constructs a cut-free proof of A. Unfortunately, the usual cut-elimination procedure does not work in the context of common knowledge.

5.1 The Problem

By the completeness theorem we know that G is a cut-free deductive system for the logic of common knowledge. Yet, the usual syntactic cut-elimination procedure cannot be applied to G. Consider the following proof:

$$\dfrac{\dfrac{\dfrac{\vdots}{A,\Gamma,\tilde{\mathsf{C}}\neg B}}{\Box_i A,\Diamond_i\Gamma,\Sigma,\tilde{\mathsf{C}}\neg B} \qquad \dfrac{\cdots \qquad \dfrac{\vdots}{\Delta,E^k B} \qquad \cdots}{\Delta,\mathsf{C}B}}{\Box_i A,\Diamond_i\Gamma,\Sigma,\Delta}\,(\text{cut})$$

Here, the inference rule above the cut on the left does not apply to the cut-formula while the inference rule on the right does. In this situation, a typical cut-elimination procedure would push the left rule instance below the cut, which would yield the following:

$$\dfrac{\dfrac{\dfrac{\vdots}{A,\Gamma,\tilde{\mathsf{C}}\neg B} \qquad \dfrac{\cdots \qquad \dfrac{\vdots}{\Delta,E^k B} \qquad \cdots}{\Delta,\mathsf{C}B}}{A,\Gamma,\Delta}\,(\text{cut})}{\Box_i A,\Diamond_i\Gamma,\Sigma,\Diamond_i\Delta}$$

This transformation, however, introduces the $\Diamond_i$ in $\Diamond_i\Delta$. Therefore, we do not get a proof of the original conclusion. This behavior is caused by the context restriction in the rule introducing $\Box_i$. In the next section, we solve this problem by introducing a nested sequent system for the logic of common knowledge that does not require context restrictions. This system and the corresponding cut-elimination procedure have been introduced by Brünnler and Studer (2009). The idea of nested sequents goes back to Kashima (1994). Here we use the formulation of Brünnler (2006).

5.2 Deep Inference

A *nested sequent* is a finite multiset of formulas and boxed sequents. A *boxed sequent* is an expression of the form $[\Gamma]_i$ where Γ is a nested sequent and $1 \leq i \leq h$. In this section, we use the letters Γ, Δ, Σ to denote nested sequents. A nested sequent is always of the form

$$A_1, \ldots, A_m, [\Delta_1]_{i_1}, \ldots, [\Delta_n]_{i_n}$$

where $1 \leq i_j \leq h$. We fix an arbitrary linear order on formulas and on boxed sequents. The *corresponding formula* of a non-empty nested sequent Γ, denoted $\underline{\Gamma}_F$, is defined by

$$\underline{A_1, \ldots, A_m, [\Delta_1]_{i_1}, \ldots, [\Delta_n]_{i_n}}_F := A_1 \vee \cdots \vee A_m \vee \Box_{i_1} \underline{\Delta_1}_F \vee \cdots \vee \Box_{i_n} \underline{\Delta_n}_F$$

where formulas and boxed sequents are listed according to the fixed order.

A *sequent context* is a nested sequent with exactly one occurrence of the special symbol $\{\}$, called the *hole*, which does not occur inside formulas. Sequent contexts are denoted by $\Gamma\{\}$, $\Delta\{\}$ and so on. The sequent $\Gamma\{\Delta\}$ is obtained by replacing $\{\}$ inside $\Gamma\{\}$ with Δ. For instance, if $\Gamma\{\} = A, [[B]_1, \{\}]_2$ and $\Delta = C, [D]_3$, then $\Gamma\{\Delta\} = A, [[B]_1, C, [D]_3]_2$.

Definition 21 (The system D). The system D consists of the following axioms and rules:

$$\Gamma\{P, \overline{P}\} \qquad \frac{\Gamma\{A\} \quad \Gamma\{B\}}{\Gamma\{A \wedge B\}} \qquad \frac{\Gamma\{A, B\}}{\Gamma\{A \vee B\}}$$

$$\frac{\Gamma\{[A]_i\}}{\Gamma\{\Box_i A\}} \qquad \frac{\Gamma\{\Diamond_i A, [\Delta, A]_i\}}{\Gamma\{\Diamond_i A, [\Delta]_i\}}$$

$$\frac{\Gamma\{\mathsf{E}^k A\} \text{ for all } k \geq 1}{\Gamma\{\mathsf{C}A\}} \qquad \frac{\Gamma\{\tilde{\mathsf{C}}A, \tilde{\mathsf{E}}^k A\}}{\Gamma\{\tilde{\mathsf{C}}A\}}$$

Definition 22 (The system $\mathsf{D} + (\mathsf{cut})$). The system $\mathsf{D} + (\mathsf{cut})$ is obtained from the system D by adding the cut rule

$$\frac{\Gamma\{A\} \quad \Gamma\{\neg A\}}{\Gamma\{\emptyset\}}$$

The *cut rank* of an instance of the cut-rule is the rank of its cut formula A. For a system S that includes the cut-rule and ordinals α and γ and a sequent Γ we write $\mathsf{S} \vdash^{\alpha}_{\gamma} \Gamma$ to say that there is a proof of Γ in system S with depth bounded by α and where all instances of the cut-rule have cut rank strictly smaller than γ. In particular $\mathsf{S} \vdash^{\alpha}_{0} \Gamma$ implies that there is a cut-free proof of Γ in S. Moreover, we use $\mathsf{S} \vdash^{<\alpha}_{\gamma} \Gamma$ to state that there exists $\beta < \alpha$ such that $\mathsf{S} \vdash^{\beta}_{\gamma} \Gamma$.

We write $\alpha \# \beta$ for the *natural sum of* α *and* β which, in contrast to the ordinary ordinal sum, does not cancel additive components. For an introduction to ordinals, and a definition of the natural sum in particular, we refer to (Schütte, 1977). Since

our formulas may have transfinite rank, we also need the *binary Veblen function* φ, which is generated inductively as follows:

1. $\varphi_0\beta := \omega^\beta$,
2. if $\alpha > 0$, then $\varphi_\alpha\beta$ denotes the βth common fixed point of the functions $\lambda\xi.\varphi_\gamma\xi$ for $\gamma < \alpha$.

We obtain our cut-elimination result by applying the method of predicative cut-elimination, see (Pohlers, 1989, 1998; Schütte, 1977), which is a standard tool for the proof-theoretic analysis of systems of set theory and second order arithmetic. The so-called reduction lemma is the key lemma, which one has to prove in order to obtain predicative cut-elimination.

Lemma 3 (Reduction Lemma). *For each formula A with $\mathsf{rk}(A) = \gamma$ we have that*

$$\textit{if } \mathsf{D}+(\mathsf{cut}) \vdash^{\alpha_1}_{\gamma} \Gamma\{A\} \textit{ and } \mathsf{D}+(\mathsf{cut}) \vdash^{\alpha_2}_{\gamma} \Gamma\{\neg A\}, \textit{ then } \mathsf{D}+(\mathsf{cut}) \vdash^{\alpha_1 \# \alpha_2}_{\gamma} \Gamma\{\emptyset\}.$$

The following two elimination lemmata are standard consequences of the reduction lemma.

Lemma 4 (First Elimination Lemma).
If $\mathsf{D}+(\mathsf{cut}) \vdash^{\alpha}_{\gamma+1} \Gamma$, *then* $\mathsf{D}+(\mathsf{cut}) \vdash^{2^\alpha}_{\gamma} \Gamma$.

Lemma 5 (Second Elimination Lemma).
If $\mathsf{D}+(\mathsf{cut}) \vdash^{\alpha}_{\beta+\omega^\gamma} \Gamma$, *then* $\mathsf{D}+(\mathsf{cut}) \vdash^{\varphi_\gamma\alpha}_{\beta} \Gamma$.

The cut-elimination theorem follows by iterated application of the second elimination lemma. $\varphi_1^n(\alpha)$ denotes the n-times iteration of φ_1, that is an expression of the form $\varphi_1(\varphi_1(\ldots\varphi_1(\alpha)\ldots))$.

Theorem 10 (Cut-elimination for the deep system).
If $\mathsf{D}+(\mathsf{cut}) \vdash^{\alpha}_{\omega\cdot n} \Gamma$, *then* $\mathsf{D}+(\mathsf{cut}) \vdash^{\varphi_1^n(\alpha)}_{0} \Gamma$.

There are syntactic transformations of $\mathsf{G}+(\mathsf{cut})$ proofs to $\mathsf{D}+(\mathsf{cut})$ proofs and vice versa as stated in the following theorems:

Theorem 11 (Shallow into deep).
If $\mathsf{G}+(\mathsf{cut}) \vdash^{\alpha}_{\gamma} \Gamma$, *then* $\mathsf{D}+(\mathsf{cut}) \vdash^{\omega\cdot\alpha}_{\gamma} \Gamma$.

Theorem 12 (Deep into shallow).
If $\mathsf{D}+(\mathsf{cut}) \vdash^{\alpha}_{0} \Gamma$, *then* $\mathsf{G}+(\mathsf{cut}) \vdash^{\omega\cdot(\alpha+1)}_{0} \underline{\Gamma}_F$.

Note that the proof of this theorem in (Brünnler and Studer, 2009) contains a mistake. A correct version is given in (Brünnler and Studer, 2012).

Now we can put all these theorems together and obtain a syntactic cut-elimination theorem for the shallow system.

Theorem 13 (Cut-elimination for the shallow system).
If $\mathsf{G}+(\mathsf{cut}) \vdash^{\alpha}_{\omega\cdot n} \Gamma$, *then* $\mathsf{G}+(\mathsf{cut}) \vdash^{\omega\cdot(\varphi_1^n(\omega\cdot\alpha)+1)}_{0} \Gamma$.

We have already mentioned that $\mathsf{H}_{\text{I-R}}$ can be easily embedded in a sequent system with cut. Keeping track of the proof depth, we thus obtain—using cut-elimination—an upper bound for proofs in D. Via the embedding of the deep into the shallow system, this bound also holds for the shallow system.

Theorem 14. *If* $\mathsf{H}_{\text{I-R}} \vdash A$, *then* $\mathsf{D} + (\mathsf{cut}) \vdash^{<\omega^2}_{\omega^2} A$.

Theorem 15 (Upper bounds). *If A is a valid formula, then*

1. $\mathsf{D} + (\mathsf{cut}) \vdash^{<\varphi_2 0}_{0} A$, *and*
2. $\mathsf{G} + (\mathsf{cut}) \vdash^{<\varphi_2 0}_{0} A$.

Figure 2 summarizes the various embeddings that we have established.

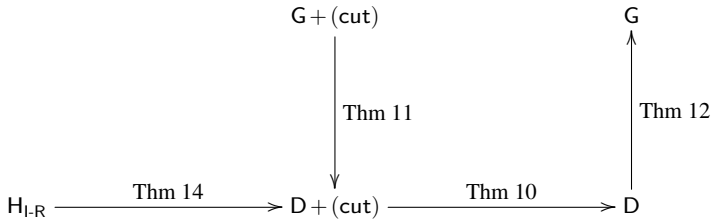

Fig. 2 Overview of the various embeddings

These results lead to several further questions. What is the 'mathematical' meaning of the upper bound on the depth of cut-free proofs? Is there a kind of boundedness lemma in modal logic similar to the one used in the analysis of set theories and second order arithmetic? Is $\varphi_2 0$ the best possible upper bound on the depth of proofs? What would be the equivalent of a well-ordering proof in modal logic? And finally, how could one syntactically eliminate cuts in a finitary system?

We have looked at common knowledge based on the least normal modal logic. However, we believe that the cut-elimination result for nested sequents is independent of the particular axiomatization of knowledge. The modal logic $\mathsf{S5}$, for instance, seems to be an important system for knowledge. Contrary to shallow sequents, deep sequents can easily handle $\mathsf{S5}$, see (Brünnler, 2006). So it is straightforward to design a system for $\mathsf{S5}$-based common knowledge.

Poggiolesi and Hill (2015) also present a calculus for common knowledge over $\mathsf{S5}$ that is based on a form of deep inference. They claim that their calculus also enjoys syntactic cut-elimination and that because their base logic is $\mathsf{S5}$, they can use some normal forms that make a finitization possible.

6 Conclusion

There is a great variety of deductive systems for the logic of common knowledge available. Yet, there are still several important open problems in this area.

Is there a nice and finitary deductive system for the logic of common knowledge? We have seen the system $\mathsf{G}^{<\omega}$, which is a finitary cut-free deductive system. However, the bounded ω-rule does not exhibit a nice behavior as its premises depend on the side formulas in Γ. Thus it is not possible to apply the usual proof-theoretic methods to $\mathsf{G}^{<\omega}$.

As mentioned before, we can design a cut-free and finitary systems using annotated sequents (Abate et al., 2007; Wehbe, 2010). However, again, the usual proof-theoretic methods cannot be applied to systems of this kind. For instance, already establishing weakening by syntactic methods is very complicated (Kokkinis and Studer, 2016).

An explanation why it is difficult to design a nice and cut-free system for common knowledge might be given by the fact that the logic of common knowledge does not enjoy interpolation (Studer, 2009). Often the existence of a nice cut-free system for a logic implies interpolation for that logic. Hence, by contraposition, we might say that the failure of interpolation 'implies' the non-existence of a nice cut-free system.

Is there a general syntactic cut-elimination method for modal fixed point logics? As we have shown, a direct syntactic cut-elimination procedure for G seems not possible. However, cut-elimination is possible in the system D using deep inference. This approach of using nested sequents works well for the logic of common knowledge but it cannot be generalized to arbitrary modal fixed point logics. Brünnler and Studer (2012) have shown that it is limited to the $\Box, \nu$-fragment of the modal μ-calculus, i.e., to a fragment where fixed points are reached after at most ω steps (Fontaine, 2008).

Thus we need another technique to obtain a general syntactic cut-elimination procedure. One approach could be to use systems with a Buchholz rule (Buchholz, 1981; Jäger and Studer, 2011). A first cut-elimination result in this context is given in (Mints and Studer, 2012).

Is there a realization procedure for common knowledge? Justification logics unfold the $\Box$-modality into justification terms, that is they feature formulas of the form $t : A$ meaning that an agent knows A for reason t, see, e.g., (Artemov, 2001; Kuznets and Studer, 2012, 2013). A *realization* is a mapping from the language of modal logic to the language of justification logic that replaces $\Box$-modalities by justification terms such that validity is preserved. Many modal logics are realizable in a corresponding justification logic. Antonakos (2013) showed that generic common knowledge is realizable in the logic of justified common knowledge as given by Artemov (2006).

Although there is a logic with justified traditional common knowledge (Bucheli et al., 2011), it is an open question whether the modal version can be realized in

the logic with justifications. The problem is that many realization proofs rely on cut-free sequent systems but it is not known how to treat the ω-rule of the system G in a realization procedure. We believe that the most promising approach to realizing common knowledge is to use a system like G^{∞}, which is also cut-free.

Acknowledgements We would like to thank Rajeev Goré for many helpful comments. This research is supported by the SNSF project 153169.

References

P. Abate, R. Goré, and F. Widmann. Cut-free single-pass tableaux for the logic of common knowledge. In *Workshop on Agents and Deduction at TABLEAUX 2007*, 2007.

L. Alberucci and G. Jäger. About cut elimination for logics of common knowledge. *Annals of Pure and Applied Logic*, 133:73–99, 2005.

E. Antonakos. Justified and common knowledge: Limited conservativity. In S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science, LFCS 2007*, volume 4514 of *LNCS*, pages 1–11. Springer, 2007.

E. Antonakos. Explicit generic common knowledge. In S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science*, volume 7734 of *Lecture Notes in Computer Science*, pages 16–28. Springer, 2013.

E. Antonakos. Pairing traditional and generic common knowledge. In S. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science*, volume 9537 of *Lecture Notes in Computer Science*, pages 14–26. Springer, 2016.

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

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

R. Aumann. Agreeing to disagree. *Annals of Statistics*, 4(6):1236–1239, 1976.

J. Barwise. Three views of common knowledge. In M. Vardi, editor, *Proceedings of Theoretical Aspects of Reasoning About Knowledge*, pages 365–379. Morgan Kaufman, 1988.

J. Barwise. *The Situation in Logic*, volume 17 of *CSLI Lecture Notes*. 1989.

K. Brünnler. Deep sequent systems for modal logic. In G. Governatori, I. Hodkinson, and Y. Venema, editors, *Advances in Modal Logic*, volume 6, pages 107–119. College Publications, 2006.

K. Brünnler and M. Lange. Cut-free sequent systems for temporal logics. *Journal of Logic and Algebraic Programming*, 76:216–225, 2008.

K. Brünnler and T. Studer. Syntactic cut-elimination for common knowledge. *Annals of Pure and Applied Logic*, 160:82–95, 2009. doi: 10.1016/j.apal.2009.01.014.

K. Brünnler and T. Studer. Syntactic cut-elimination for a fragment of the modal mu-calculus. *Annals of Pure and Applied Logic*, 163(12):1838–1853, 2012.

S. Bucheli. *Justification Logics with Common Knowledge*. PhD thesis, Universität Bern, 2012.

S. Bucheli, R. Kuznets, and T. Studer. Two ways to common knowledge. In T. Bolander and T. Braüner, editors, *Proceedings of the 6th Workshop on Methods for Modalities (M4M–6 2009), Copenhagen, Denmark, 12–14 November 2009*, Electronic Notes in Theoretical Computer Science, pages 83–98. Elsevier, 2010. doi: 10.1016/j.entcs.2010.04.007.

S. Bucheli, R. Kuznets, and T. Studer. Justifications for common knowledge. *Journal of Applied Non-Classical Logics*, 21(1):35–60, 2011. doi: 10.3166/JANCL.21.35-60.

W. Buchholz. The $\Omega_{\mu+1}$-rule. In W. Buchholz, S. Feferman, W. Pohlers, and W. Sieg, editors, *Iterated Inductive Definitions and Subsystems of Analysis: Recent Proof Theoretic Studies*, volume 897 of *Lecture Notes in Mathematics*, pages 189–233. Springer, 1981. doi: 10.1007/BFb0091898.

C. Dax, M. Hofmann, and M. Lange. A proof system for the linear time μ-calculus. In *Proc. 26th Conf. on Foundations of Software Technology and Theoretical Computer Science, FSTTCS'06*, volume 4337 of *LNCS*, pages 274–285. Springer, 2006.

R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

G. Fontaine. Continuous fragment of the mu-calculus. In M. Kaminski and S. Martini, editors, *Computer Science Logic*, volume 5213 of *LNCS*, pages 139–153. Springer, 2008. doi: 10.1007/978-3-540-87531-4-12.

R. Goré. And-or tableaux for fixpoint logics with converse: LTL, CTL, PDL and CPDL. In S. Demri, D. Kapur, and C. Weidenbach, editors, *Automated Reasoning: 7th International Joint Conference, IJCAR 2014. Proceedings*, pages 26–45. Springer, 2014. doi: 10.1007/978-3-319-08587-6-3.

E. Grädel, W. Thomas, and T. Wilke, editors. *Automata Logics, and Infinite Games: A Guide to Current Research*. Springer, 2002. ISBN 3-540-00388-6.

E. Gudzhinskas. Syntactical proof of the elimination theorem for von Wrights temporal logic. *Math. Logika Primenen*, 2:113–130, 1982.

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

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

G. Jäger and M. Marti. Intuitionistic common knowledge or belief, 2015.

G. Jäger and T. Studer. A Buchholz rule for modal fixed point logics. *Logica Universalis*, 5:1–19, 2011. doi: 10.1007/s11787-010-0022-1.

G. Jäger, M. Kretz, and T. Studer. Cut-free common knowledge. *Journal Applied Logic*, 5(4):681–689, 2007.

R. Kashima. Cut-free sequent calculi for some tense logics. *Studia Logica*, 53(1): 119–136, 1994.

I. Kokkinis and T. Studer. Cyclic proofs for linear temporal logic. In D. Probst and P. Schuster, editors, *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, volume 6 of *Ontos Mathematical Logic*. De Gruyter, 2016.

M. Kretz and T. Studer. Deduction chains for common knowledge. *Journal of Applied Logic*, 4:331–357, 2006.

R. Kuznets and T. Studer. Justifications, ontology, and conservativity. In T. Bolander, T. Braüner, S. Ghilardi, and L. Moss, editors, *AiML 9*, pages 437–458. College Publications, 2012.

R. Kuznets and T. Studer. Update as evidence: Belief expansion. In S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science LFCS 13*, volume 7734 of *LNCS*, pages 266–279. Springer, 2013.

M. Lange and C. Stirling. Focus games for satisfiability and completeness of temporal logic. In *Proceedings of LICS*, 2001.

D. Leivant. A proof theoretic methodology for propositional dynamic logic. In *Proceedings of the International Colloquium on Formalization of Programming Concepts*, Springer LNCS, pages 356–373, 1981.

D. Lewis. *Convention: A Philosophical Study*. 1969.

D. Martin. Borel determinacy. *Annals of Mathematics*, 102:363–371, 1975.

J. McCarty, M. Sato, T. Hayashi, and S. Igarishi. On the model theory of knowledge. Technical Report STAN-CS-78-657, Stanford University, 1978.

J.-J. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge University Press, 1995.

G. Mints and T. Studer. Cut-elimination for the mu-calculus with one variable. In *Fixed Points in Computer Science 2012*, volume 77 of *EPTCS*, pages 47–54. Open Publishing Association, 2012.

D. Niwinski and I. Walukiewicz. Games for the mu-calculus. *Theoretical Computer Science*, 163(1&2):99–116, 1996.

B. Paech. Gentzen-systems for propositional temporal logics. In E. Börger, H. K. Büning, and M. M. Richter, editors, *CSL '88: 2nd Workshop on Computer Science Logic, Proceedings*, pages 240–253. Springer, 1989. doi: 10.1007/BFb0026305.

F. Poggiolesi and B. Hill. Common knowledge: a finitary calculus with a syntactic cut-elimination procedure. *Logique et Analyse*, 58(230):136–159, 2015.

W. Pohlers. *Proof Theory - An introduction*. Springer, 1989.

W. Pohlers. Subsystems of set theory and second order number theory. In S. Buss, editor, *Handbook of Proof Theory*, pages 209–335. Elsevier, 1998.

T. Schelling. *The Strategy of Conflict*. 1960.

S. Schiffer. *Meaning*. 1972.

K. Schütte. *Proof Theory*. Springer, 1977.

R. S. Streett and E. A. Emerson. An automata theoretic decision procedure for the propositional modal mu–calculus. *Information and Computation*, 81:249–264, 1989.

T. Studer. Common knowledge does not have the Beth property. *Information Processing Letters*, 109:611–614, 2009.

J. van Benthem, J. van Eijck, and B. Kooi. Common knowledge in update logics. In *Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge*, TARK '05, pages 253–261, 2005. ISBN 981-05-3412-4.

R. Wehbe. *Annotated Systems for Common Knowledge*. PhD thesis, Universität Bern, 2010.