Proof-Theoretic Contributions to Modal Fixed Point Logics

Habilitationsschrift

Thomas Studer

Institut für Informatik und
angewandte Mathematik
Universität Bern

2009

Preface

Synopsis

This thesis provides an overview of my work on the proof theory for modal fixed point logics. In particular, it summarizes the main results of the following papers.

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

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

3. K. Brünnler and T. Studer. Syntactic cut-elimination for common knowledge. *Annals of Pure and Applied Logic*, to appear.

4. T. Studer. Common knowledge does not have the Beth property. *Information Processing Letters*, to appear.

5. D. Steiner and T. Studer. Total public announcements. In S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science, LFCS 2007*, pages 498–511. Springer, 2007.

6. G. Jäger, M. Kretz, and T. Studer. Cut-free axiomatizations for stratified modal fixed point logic. In H. Schlingloff, editor, *Proceedings of the 4th Workshop Methods for Modalities*, pages 125–143. 2005.

7. G. Jäger, M. Kretz, and T. Studer. Canonical completeness for infinitary μ. *Journal of Logic and Algebraic Programming*, 76(2):270–292, 2008.

8. T. Studer. On the proof theory of the modal mu-calculus. *Studia Logica*, 89:343–363, 2008.

Acknowledgements

I am deeply grateful to Gerhard Jäger for introducing me to logic and theoretical computer science. His steady support and his enthusiasm have greatly influenced this work an my personal scientific development.

There are numerous people I had scientific discussions with and they all contributed to my work. Any attempt to list them all would be incomplete. Let me only mention my friends from the Bern logic group for lots of help and stimulating discussions as well as for the great atmosphere they have shared with me. In particular, I would like to thank Kai Brünnler, Gerhard Jäger, This Kretz, and David Steiner who co-authored some of the papers covered in this thesis.

Last but not least, I am very thankful to my family for all the understanding and support.

Erlach, February 2009, Thomas Studer

Chapter 1

Modal Logic

1.1 Introduction

Modal logic as the formal study of modalities goes back to Lewis [52] who introduced modal operators in order to solve the paradoxes of material implication and to obtain logics of necessity and possibility. In modern terms, his key idea was that we can take a formula A, prefix it with a $\Box$ or $\Diamond$ symbol, and we obtain new formulae $\Box A$ (meaning that A is necessary) and $\Diamond A$ (meaning that A is possible), respectively.

Since then, many different modal operators were proposed and used in many different contexts. For instance, epistemic logic introduces modalities like *it is known that* and temporal logic arises with modalities like *eventually*. Looking at modal logic from a more abstract point of view, one noticed that it provides a general framework to study relational structures which occur naturally in various areas. For instance modal logic plays a very prominent role in theoretical computer science. Automated verification of hardware and software, knowledge-based programming, and intelligent distributed computing all rely on the theoretical background of modal logic. See [17, 18, 24] for excellent overviews on recent developments in modal logic.

For many applications it is necessary to extend the basic language of modal logic by additional operators. Assume, for instance, that in some temporal logic we have a modal operator T such that $\mathsf{T}A$ means *tomorrow A holds.* With this logic it is possible to talk about the future. We can express things like *in n days A holds* - where n is a given natural number - by n-times nesting the T operator. However, there are no quantifiers available. Thus we cannot say *for every n, in n days A holds* which means that we cannot say

$$\textit{A holds on every day.} \tag{1.1}$$

If we would work with an infinitary language, then (1.1) could be expressed by the infinitary conjunction

$$A \wedge \mathsf{T}A \wedge \mathsf{TT}A \wedge \mathsf{TTT}A \wedge \cdots . \tag{1.2}$$

In order to express (1.1) by a finite statement, we can either (1) extend our language by a special modal operator saying *on every day it holds that* or (2) introduce means to build least and greatest fixed points. For the second solution, we observe that the greatest fixed point of the operator given by $\lambda X.A \wedge \mathsf{T}X$ is semantically equivalent to (1.2). The general extension of modal logic by least and greatest fixed point operators is known as the *modal μ-calculus*. It has been introduced by Kozen [46] in order to state and prove properties of programs.

The *logic of common knowledge* is a variant of epistemic logic with an extra modality C. The formula $\mathsf{C}A$ then means that A *is common knowledge*. The equivalent of the formula $\mathsf{C}A$ in the modal μ-calculus is the greatest fixed point of

$$\lambda X.\text{everybody knows that } A \text{ and everybody knows that } X. \tag{1.3}$$

We are interested in the proof theory of modal fixed point logics. That means we are concerned with the study of proofs as formal objects. In general, the principal tasks of proof theory are the following: First, to formulate systems of logic and characterize what follows from certain axioms, and second, to study the structure of formal proofs (for instance to find normal forms and to establish syntactic facts about proofs). In particular, these tasks include the quest for deductive systems that have certain desired structural properties as well as completeness proofs for those systems. Moreover, it also includes the study of embeddings or, more general, of the syntactic relationship between several systems.

There are already many issues about the proof theory of modal logics without fixed point extensions. As Wansing [86] observed, standard sequent systems for modal logic typically fail to be modular and do not satisfy most of the properties usually demanded on sequent calculi. Some recent approaches to solve these problems include the internalization of the Kripke semantics into the inference system [57] or the use of deep sequents [20]. However, our interest is on fixed point extension of modal logic and not on the consequences of different frame conditions for deductive systems. Therefore we will not study these problems here but focus on the effect of adding fixed point operators to modal logic.

This thesis is organized as follows. In the next section we start with introducing the language and semantics of the basic modal logic. Then we will present Hilbert and Tait style deductive systems for it. Chapter 2 is devoted to the study of common knowledge. First we present the logic of common knowledge and we recall a Hilbert style system as well as an infinitary Tait style system for common knowledge. Our contributions include:

1. the introduction of the first finitary, sound and complete, cut-free deductive system for common knowledge,

2. the study of deduction chains for common knowledge which is a syntactic and in a certain sense constructive method for proving completeness of a deductive system,

3. a syntactic cut-elimination procedure for common knowledge which also provides an upper bound on the depth of cut-free proofs,

4. a proof that the logic of common knowledge lacks interpolation,

5. an axiomatization for public announcements and common knowledge where, in contrast to the classical setting, the announcement operators are total.

In Chapter 3 we study infinitary deductive systems for the modal μ-calculus. Our contributions include:

1. the study of a cut-free infinitary system for the so-called stratified fragment of the μ-calculus,

2. a canonical completeness proof for an infinitary system for the modal μ-calculus which is the only available proof working with standard methods from modal logic; all other proofs make use of sophisticated game or automata theoretic means,

3. an embedding of a system with an ω-rule into a system with global induction which results in a new proof of the finite model property of the modal μ-calculus.

Chapter 4 concludes this thesis.

1.2 Basic Modal Logic

Language. Let $\mathcal{L}$ denote the basic language of propositional (multi-)modal logic.

Definition 1 (Language $\mathcal{L}$)**.** Let

$$\Phi = \{\mathsf{p}, \sim\!\mathsf{p}, \mathsf{q}, \sim\!\mathsf{q}, \mathsf{r}, \sim\!\mathsf{r}, \ldots\}$$

be a countable set of atomic propositions, $\mathsf{T} = \{\top, \bot\}$ a set containing symbols for truth and falsehood and $\mathsf{M} = \{1, \ldots, h\}$ a set of indices. Define the formulae of the language $\mathcal{L}$ inductively as follows:

1. If P is an element of Φ, then P is a formula of $\mathcal{L}$.
2. If A and B are formulae of $\mathcal{L}$, then so are $(A \wedge B)$ and $(A \vee B)$.
3. If A is a formula of $\mathcal{L}$ and $i \in \mathsf{M}$, then $\Box_i A$ and $\Diamond_i A$ are also formulae of $\mathcal{L}$.

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

Note that formulae are a priori in negation normal form. The negation $\neg A$ of a formula A is defined as usual by reflecting De Morgan's laws, the law of double negation, and the duality laws for modal operators. For formulae A and B, we can now introduce implication and equivalence as usual by $A \to B := \neg A \vee B$ and $A \leftrightarrow B := (A \to B) \wedge (B \to A)$.

Semantics. We employ standard Kripke semantics for modal logics to give meaning to formulae.

Definition 2 (Kripke structure)**.** A Kripke structure $\mathsf{K} = (S, R, \pi)$ is a triple where S is a non–empty set, $R : \mathsf{M} \to \mathcal{P}(S \times S)$ and $\pi : \Phi \to \mathcal{P}(S)$ is a function such that $\pi(\sim\!\mathsf{p}) = S \setminus \pi(\mathsf{p})$ for all $\sim\!\mathsf{p} \in \Phi$. We call S the set of states of K. The function R assigns an accessibility relation to each $i \in \mathsf{M}$ where we write R_i for the relation $R(i)$.

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

Definition 3 (Denotation)**.** Let $\mathsf{K} = (S, R, \pi)$ be a Kripke structure. For every $A \in \mathcal{L}$ we define the set $\|A\|_{\mathsf{K}} \subseteq S$ inductively as follows:

$$\|P\|_{\mathsf{K}} := \pi(P) \text{ for all } P \in \Phi, \quad \|\top\|_{\mathsf{K}} := S, \quad \|\bot\|_{\mathsf{K}} := \emptyset,$$

$$\|B \wedge C\|_{\mathsf{K}} := \|B\|_{\mathsf{K}} \cap \|C\|_{\mathsf{K}}, \quad \|B \vee C\|_{\mathsf{K}} := \|B\|_{\mathsf{K}} \cup \|C\|_{\mathsf{K}},$$

$$\|\Box_i B\|_{\mathsf{K}} := \{w \in S : v \in \|B\|_{\mathsf{K}} \text{ for all } v \text{ such that } wR_iv\},$$

$$\|\Diamond_i B\|_{\mathsf{K}} := \{w \in S : v \in \|B\|_{\mathsf{K}} \text{ for some } v \text{ such that } wR_iv\}.$$

We call a formula A *satisfiable* if there is a Kripke structure K such that $\|A\|_{\mathsf{K}}$ is non-empty. For a Kripke structure $\mathsf{K} = (S, R, \pi)$ we write $\mathsf{K} \models A$ if $\|A\|_{\mathsf{K}} = S$. Moreover, we write $\mathsf{K}, s \models A$ if $s \in \|A\|_{\mathsf{K}}$. The formula A is called *valid* if for every Kripke structure K we have $\mathsf{K} \models A$. Let Γ be a set of formulae. We write $\Gamma \models A$ if for all Kripke structures K such that $\mathsf{K} \models B$ for each $B \in \Gamma$, we also have $\mathsf{K} \models A$.

In the context of modeling knowledge, one often is interested in Kripke structures in which all accessibility relations are required to be equivalence relations. The corresponding logic is called $\mathsf{S5}$. Its semantics is given as follows. We will write $\mathcal{K}^{eq}$ for the class of all Kripke structures (S, R, π) where each accessibility relation R_i is an equivalence relation. The formula A is $\mathsf{S5}$-*valid*, if and only if $\mathsf{K} \models A$ for all $\mathsf{K} \in \mathcal{K}^{eq}$. Further, we say that A is $\mathsf{S5}$-*satisfiable*, if and only if there is a $\mathsf{K} \in \mathcal{K}^{eq}$ such that $\|A\|_{\mathsf{K}}$ is non-empty.

Deductive Systems.

Definition 4 (The system $\mathsf{H}_{\mathsf{Mod}}$)**.** The Hilbert calculus $\mathsf{H}_{\mathsf{Mod}}$ for modal logic is defined by the following axioms and inference rules:

Propositional axioms: Every instance of a propositional tautology

Modal axioms: For all formulae A and B and all indices i from M

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

Rules: For all formulae A and B and all indices i from M

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

We have the following standard completeness result.

Theorem 5 (Soundness and completeness of $\mathsf{H}_{\mathsf{Mod}}$)**.** *For any formula A of $\mathcal{L}$ we have that*

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

We can obtain a deductive system for the logic $\mathsf{S5}$ by extending $\mathsf{H}_{\mathsf{Mod}}$ as follows.

Definition 6 (The system H_{S5})**.** The system H_{S5} is defined by extending $\mathsf{H}_{\mathsf{Mod}}$ with the following axioms.

Additional Modal axioms: For all formulae A and all indices i from M

$$\begin{array}{ll} \Box_i A \to A & (\mathsf{T}) \\ \Box_i A \to \Box_i \Box_i A & (\mathsf{4}) \\ \neg\Box_i A \to \Box_i \neg\Box_i A & (\mathsf{5}) \end{array}$$

Again, we have the following standard completeness result.

Theorem 7 (Soundness and completeness of H_{S5})**.** *For any formula A of $\mathcal{L}$ we have that*

$$A \textit{ is } \mathsf{S5}\textit{-valid if and only if } \mathsf{H}_{\mathsf{S5}} \vdash A.$$

For proof-theoretic purposes, Hilbert systems often are not suitable since (MP) does not have the subformula property. That means in instances of (MP) there occurs a formula B in the premise which is not a subformula of the conclusion A. A simple consequence of this is, for instance, that there is no systematic proof search procedure possible in a Hilbert system.

Let us now look at a system that enjoys the subformula property. $\mathsf{T}_{\mathsf{Mod}}$ is a Tait style system [73, 80] for modal logic, that means a one-sided Gentzen calculus which derives finite sets $\Gamma, \Delta, \Sigma, \ldots$ of formulae. These sets are called *sequents* and they are interpreted disjunctively. We use the following shorthand: if Γ is the set $\{A_1, \ldots, A_n\}$, then $\Diamond_i\Gamma := \{\Diamond_i A_1, \ldots, \Diamond_i A_n\}$.

Definition 8 (The system $\mathsf{T}_{\mathsf{Mod}}$)**.** The system $\mathsf{T}_{\mathsf{Mod}}$ is defined by the following axioms and inference rules:

Axioms: For all sequents Γ and all p in Φ

$$\Gamma, \mathsf{p}, \sim\mathsf{p} \quad (\mathsf{ID1}) \qquad\qquad \Gamma, \top \quad (\mathsf{ID2})$$

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

$$\frac{\Gamma, A, B}{\Gamma, A \lor B}\ (\lor) \qquad\qquad \frac{\Gamma, A \qquad \Gamma, B}{\Gamma, A \land B}\ (\land)$$

Modal rules: For all sequents Γ and Σ and formulae A and all indices i from M

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

Again, we have the following standard completeness result.

Theorem 9 (Soundness and completeness of $\mathsf{T}_{\mathsf{Mod}}$)**.** *For any formula A of $\mathcal{L}$ we have that*

$$A \textit{ is valid if and only if } \mathsf{T}_{\mathsf{Mod}} \vdash A.$$

In the sequel we will also consider extensions of sequent systems by the rule (cut) which is given by

$$\frac{\Gamma, A \qquad \Gamma, \neg A}{\Gamma} \quad (\mathsf{cut})$$

for all sequents Γ and formulae A. Note that semantic cut-elimination is an immediate consequence of the completeness of $\mathsf{T}_{\mathsf{Mod}}$.

Corollary 10 (Semantic cut-elimination for $\mathsf{T}_{\mathsf{Mod}}$)**.** *For any formula A of $\mathcal{L}$ we have that*

$$\mathsf{T}_{\mathsf{Mod}} + (\mathsf{cut}) \vdash A \quad \Longrightarrow \quad \mathsf{T}_{\mathsf{Mod}} \vdash A.$$

Note that unlike in the case of Hilbert systems, there is no straightforward way to extend $\mathsf{T}_{\mathsf{Mod}}$ in order to obtain a Tait style system for S5.

Chapter 2

Common Knowledge

2.1 Introduction

Modal logic may be employed to reason about knowledge. A necessity for this arises for example when modeling systems of distributed agents, say computers connected over a network. In this setting, an agent knowing some proposition A in a state s is usually understood as A holding in all states reachable from s in one step and thus each agent's knowledge may be modeled using a respective box operator. Furthermore, through arbitrary nesting of boxes epistemic situations of considerable complexity become expressible. However, it is well known that there are certain situations of particular interest which the basic language of modal logic cannot talk about. One such example is *common knowledge* of a proposition A, which can roughly be viewed as the infinitary conjunction *all agents know* A *and all agents know that all agents know* A *and so on*.

Common knowledge is of particular interest in connection with coordination among a set of agents. For example, it is common knowledge that red traffic lights mean *stop* and green ones mean *go*. Thus most drivers feel safe when they pass green lights. Now suppose that this fact is not common knowledge. In that case each driver still knows that she can pass when the lights are green and has to stop when the lights are red. However, she does not know that the other drivers know the rule and therefore she will not feel safe any more. Thus a safe driver will always stop (even when the lights are green) unless there are no other cars at the crossing since she considers it possible that another driver might jump a red light. Of course, for this simple example it is enough to only consider knowledge about other people's knowledge but this need not be iterated ad infinitum. However, there are situations where an arbitrary number of iterations of the knowledge operator has to be taken into account. Thus common knowledge is important for coordination and simultaneous actions in multi-agent systems. In fact, one can even prove that common knowledge is a prerequisite for simultaneous actions, see [32].

The classic study of the notion of common knowledge has been carried out by Lewis [53]. As he acknowledges, part of his work is inspired by Schelling [67]. Aumann in his seminal paper [8] provides the first mathematically rigorous formulation of common knowledge using set theory. A definition of common knowledge in terms of epistemic logic has been given by Schiffer [68]. Halpern and Moses [38] 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 developing common knowledge are logically equivalent, see (2.1) below. Another possibility to formalize common knowledge is in Barwise's situation semantics [13, 14] where common knowledge is given by a greatest fixed point construction. It comes out that in the situation semantics the definitions of common knowledge as infinite conjunction and as greatest fixed point differ whereas in multi-modal logic they coincide. Many applications of common knowledge in computer science are investigated in the textbooks by Fagin et al. [32] as well as Meyer and van der Hoek [56].

Note that there is also Artemov's notion of *justified common knowledge* [7] which is based on the logic of proofs [6]. The main model theoretic difference between common knowledge and justified common knowledge is the following: the former captures the greatest solution of the fixed point equation of common knowledge (1.3) whereas the latter considers all of its solutions. See [5] for a detailed account on the relationship of these approaches to common knowledge.

So far most of the work on common knowledge has been performed from a model theoretic point of view. Notable exceptions are Alberucci and Jäger [2, 3] who pioneered proof-theoretic investigations on common knowledge. They introduce several sequent systems for common knowledge and present first results with respect to cut-elimination. We will continue this line of research.

Language. $\mathcal{L}_{\mathsf{CK}}$ is the language of (multi-)modal logic extended by the common knowledge operator C and its dual $\tilde{\mathsf{C}}$.

Definition 11 (Language $\mathcal{L}_{\mathsf{CK}}$)**.** Define the formulae of the language $\mathcal{L}_{\mathsf{CK}}$ inductively like the language $\mathcal{L}$ with the additional clause:

4. If A is a formula of $\mathcal{L}_{\mathsf{CK}}$, then so are $\mathsf{C}A$ and $\tilde{\mathsf{C}}A$.

We define the following abbreviations:

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

for $\{1, \ldots, h\} = \mathsf{M}$. Thus $\mathsf{E}A$ stands for *everybody knows* A. We will also need iterated applications of these operators:

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

Definition 12. We define the *length* $\mathsf{ln}(A)$ of a formula A as follows:

1. $\mathsf{ln}(\mathsf{p}) := \mathsf{ln}({\sim}\mathsf{p}) := \mathsf{ln}(\top) := \mathsf{ln}(\bot) := 1$
2. $\mathsf{ln}(A \wedge B) := \mathsf{ln}(A \vee B) := \mathsf{ln}(A) + \mathsf{ln}(B)$
3. $\mathsf{ln}(\Box_i A) := \mathsf{ln}(\Diamond_i A) := \mathsf{ln}(A) + 1$
4. $\mathsf{ln}(\mathsf{C}A) := \mathsf{ln}(\tilde{\mathsf{C}}A) := \mathsf{ln}(A) \cdot h + h + 1$

Semantics. We extend the standard Kripke semantics for modal logics to give meaning to $\mathcal{L}_{\mathsf{CK}}$ formulae as follows.

Definition 13 (Denotation)**.** Let $\mathsf{K} = (S, R, \pi)$ be a Kripke structure. For every $A \in \mathcal{L}_{\mathsf{CK}}$ we define the set $\|A\|_{\mathsf{K}} \subseteq S$ by adding the following clauses to Definition 3.

$$\|\mathsf{C}A\|_{\mathsf{K}} := \bigcap \{\|\mathsf{E}^m A\|_{\mathsf{K}} : m \geq 1\}$$
$$\|\tilde{\mathsf{C}}A\|_{\mathsf{K}} := \bigcup \{\|\tilde{\mathsf{E}}^m A\|_{\mathsf{K}} : m \geq 1\}$$

The notions of validity and satisfiability of $\mathcal{L}_{\mathsf{CK}}$ formulae are defined accordingly.

Our semantics of the operator C reflects the so-called iterative approach to common knowledge where $\mathsf{C}A$ is treated to be equivalent to the infinite conjunction $\mathsf{E}^1 A \wedge \mathsf{E}^2 A \wedge \mathsf{E}^3 A \wedge \cdots$. Alternatively, we could interpret common knowledge as greatest fixed point since

$$\|\mathsf{C}A\|_{\mathsf{K}} = \bigcup \{X \subseteq S : X = \|\mathsf{E}A \wedge \mathsf{E}\mathsf{q}\|_{\mathsf{K}[\mathsf{q}:=X]}\} \tag{2.1}$$

where q is an atomic proposition that does not occur in A and $\mathsf{K}[\mathsf{q} := X]$ is like K except that the valuation function maps q to X. A proof of (2.1) can be found for example in [32].

A crucial property for the logics we consider is the small model property. Again, a proof can be found for instance in [32].

Theorem 14 (Small Model Property)**.** *If an $\mathcal{L}_{\mathsf{CK}}$ formula A is satisfiable, then there is a Kripke structure K with at most $2^{\mathsf{ln}(A)}$ states such that $\|A\|_{\mathsf{K}} \neq \emptyset$.*

Deductive Systems. The traditional way to formalize common knowledge is to use a Hilbert style axiom system. Such a system has a co-closure axiom, which states that common knowledge is a post-fixed point, and an induction rule which states that this post-fixed point is the greatest fixed point.

Definition 15 (The system H_{CK})**.** The system H_{CK} is defined by extending $\mathsf{H}_{\mathsf{Mod}}$ with the following axioms and rules:

Co-closure axiom: For all formulae A

$$\mathsf{C}A \to \mathsf{E}(A \land \mathsf{C}A) \quad (\mathsf{C})$$

Induction rule: For all formulae A and B

$$\frac{A \to \mathsf{E}(A \land B)}{A \to \mathsf{C}B} \quad (\mathsf{IND})$$

Soundness and completeness of H_{CK} can be shown by standard methods [32].

Theorem 16 (Soundness and completeness of H_{CK})**.** *For any formula A of $\mathcal{L}_{\mathsf{CK}}$ we have that*

$$A \textit{ is valid if and only if } \mathsf{H}_{\mathsf{CK}} \vdash A.$$

The approach of using an induction rule does not work well for designing a Gentzen style sequent calculus for common knowledge. Alberucci and Jäger [3] show that a particular cut-free sequent system designed in this way is not complete. To obtain a complete cut-free system they replace the induction rule by an infinitary ω-rule which results in the following deductive system.

Definition 17 (The system $\mathsf{T}^{\omega}_{\mathsf{CK}}$)**.** The system $\mathsf{T}^{\omega}_{\mathsf{CK}}$ is defined from $\mathsf{T}_{\mathsf{Mod}}$ by changing the modal rules and adding the common knowledge rules as follows where $\tilde{\mathsf{C}}\{B_1, \ldots, B_n\} := \{\tilde{\mathsf{C}}B_1, \ldots, \tilde{\mathsf{C}}B_n\}$:

Modal rules: For all sequents Γ, Δ, Σ and formulae A and all indices i from M

$$\frac{\Gamma, A, \tilde{\mathsf{C}}\Delta}{\Diamond_i\Gamma, \Box_i A, \tilde{\mathsf{C}}\Delta, \Sigma} \quad (\Box_{\mathsf{C}})$$

Common knowledge rules: For all sequents Γ and formulae A

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

The rule (C) is a so-called ω-rule since it permits the derivation of $\mathsf{C}A$ from the infinitely many premises $\mathsf{E}^k A$ for all $k \geq 1$. We call $\mathsf{T}^{\omega}_{\mathsf{CK}}$ a semi-formal system since, as opposed to formal systems, it has basic inferences with infinitely many premises. Semi-formal systems are an important ingredient in the proof-theoretic analysis of subsystems of arithmetic and set-theory. The use of an ω-rule goes back to Hilbert who employed it to obtain certain completeness results for arithmetic [40], see [33] for a detailed discussion.

Alberucci and Jäger [3] provide a completeness proof for $\mathsf{T}^{\omega}_{\mathsf{CK}}$ by a canonical counter-model construction.

Theorem 18 (Soundness and completeness of $\mathsf{T}^{\omega}_{\mathsf{CK}}$)**.** *For any formula A of $\mathcal{L}_{\mathsf{CK}}$ we have that*

$$A \textit{ is valid if and only if } \mathsf{T}^{\omega}_{\mathsf{CK}} \vdash A.$$

2.2 Contributions

Our contributions to the logic of common knowledge are presented in the following papers:

1. Cut-free common knowledge [42]
2. Deduction chains for common knowledge [49]
3. Syntactic cut-elimination for common knowledge [22]
4. Common knowledge does not have the Beth property [79]
5. Total public announcements [76]

In the remainder of this chapter we will summarize the results of these contributions.

2.2.1 Cut-free common knowledge

As mentioned before cut-elimination seems not possible for finitary systems which are based on an induction rule. So it was on open problem whether there can be a finitary cut-free deductive system for common knowledge. In **Cut-free common knowledge [42]** we developed the first sound and complete cut-free system for common knowledge. Since then other such systems have been found. Abate, Goré and Widmann, for example, introduce a cut-free tableau system for common knowledge in [1]. Moreover, cut-free systems for certain modal fixed point logics can be obtained by representing focus games [50] as sequent calculi [21]. Using this approach, Wehbe presented a cut-free sequent system for relativized common knowledge [87].

Regarding $\mathsf{T}^{\omega}_{\mathsf{CK}}$, we see that it is only the rule (C) which is responsible for possibly infinite derivations. All proofs will be completely finite if we succeed in restricting the infinitely many premises of each application of (C) to a finite subset. Fortunately, this can be achieved by exploiting the small model property of the logic of common knowledge. A similar approach for PDL appears in Leivant [51].

We will now give a sketch of our approach to provide a finitary cut-free system for common knowledge. For any formula A and finite set $\Gamma = \{B_1, \ldots, B_n\}$ we define the bounding function

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

Definition 19 (The system $\mathsf{T}^{<\omega}_{\mathsf{CK}}$)**.** The system $\mathsf{T}^{<\omega}_{\mathsf{CK}}$ is defined from $\mathsf{T}^{\omega}_{\mathsf{CK}}$ by replacing the infinitary rule for common knowledge by the following:

Finitary common knowledge rule: For all sequents Γ and formulae A

$$\frac{\Gamma, \mathsf{E}^k A \quad \text{for } k = \mathsf{bd}(A, \Gamma)}{\Gamma, \mathsf{C}A} \quad (\mathsf{C}^{<\omega})$$

The completeness of $\mathsf{T}^{<\omega}_{\mathsf{CK}}$ immediately follows from the completeness of $\mathsf{T}^{\omega}_{\mathsf{CK}}$. To show the soundness we make use of the small model property as follows. Assume that the conclusion $\Gamma, \mathsf{C}A$ of an instance of $(\mathsf{C}^{<\omega})$ is not valid. By the small model property, there exists a counter model with at most $\mathsf{bd}(A, \Gamma)$ states. Using some basic facts about monotone operators we conclude that this also must be a counter model to $\Gamma, \mathsf{E}^k A$ where $k = \mathsf{bd}(A, \Gamma)$. Thus, the disjunction over $\Gamma, \mathsf{E}^k A$ is not valid. Therefore $(\mathsf{C}^{<\omega})$ preserves validity. The soundness of $\mathsf{T}^{<\omega}_{\mathsf{CK}}$ follows by induction on the length of derivations.

Theorem 20 (Soundness and completeness of $\mathsf{T}^{<\omega}_{\mathsf{CK}}$)**.** *For any formula A of $\mathcal{L}_{\mathsf{CK}}$ we have that*

$$A \text{ is valid if and only if } \mathsf{T}^{<\omega}_{\mathsf{CK}} \vdash A.$$

2.2.2 Deduction chains for common knowledge

In **Deduction chains for common knowledge** [49], we aim to deepen the proof-theoretic understanding of the logic of common knowledge by giving an alternative completeness proof for $\mathsf{T}^{\omega}_{\mathsf{CK}}$ using the method of deduction chains. Deduction chains represent a syntactic and in a certain sense constructive method for proving completeness of a formal system. Given a formula A, the deduction chains of A are built up by systematically decomposing A into its subformulae. In the case where A is a valid formula, the decomposition yields a (usually cut-free) proof of A. If A is not valid, the decomposition produces a counter model for A.

The method of deduction chains was first introduced by Schütte in [70, 72] and has been used mainly in the proof theory of systems of first and second order arithmetic. See for instance [44, 63] for applications of the method in this field. In [71] Schütte extended deduction chains to modal logic and we extend this approach again to accommodate fixed point constructs. The main additional difficulty is that the presence of fixed points requires a fully deterministic procedure for the decomposition of a given formula in order to guarantee fairness in the case of an infinite deduction chain.

The two main ingredients in the method of deduction chains are the following two lemmata. Since we are dealing with modal logic, a deduction chain consists of so-called sequence trees and not just sequences of formulae as in the non-modal case.

Lemma 21 (Principal semantic lemma)**.** *If there exists a deduction chain of a formula A which is infinite or ends in a non-axiomatic sequence tree, then there exists a counter model for A.*

Note that the proof of this lemma is constructive and returns such a counter model. It makes essential use of a fairness condition on the construction of deduction chains.

Lemma 22 (Principal syntactic lemma)**.** *If all deduction chains for a formula A end in axiomatic sequence trees, then there exists a proof of A in $\mathsf{T}^{\omega}_{\mathsf{CK}}$.*

The proof of this lemma is along the following lines.

1. Code each sequence tree R in the deduction tree (consisting of all deduction chains) of A as a set of formulae C^R.
2. Show that $\mathsf{T}^{\omega}_{\mathsf{CK}} \vdash C^L$ for each leaf L of the deduction tree.
3. Show by induction on the Kleene-Brouwer ordering of the deduction tree that $\mathsf{T}^{\omega}_{\mathsf{CK}} \vdash C^R$ if $\mathsf{T}^{\omega}_{\mathsf{CK}} \vdash C^{S_i}$ for all successors S_i of R.

4. Finally, observe $C^R = A$ for the root R of the deduction tree.

Remark 23. *In order to prove step (3) of the above procedure, we need to observe that (in certain cases) the rules of* $\mathsf{T}^{\omega}_{\mathsf{CK}}$ *may also be applied deep inside* $\mathcal{L}_{\mathsf{CK}}$ *formulae.*

Corollary 24 (Completeness)**.** *If A is a valid formula of $\mathcal{L}_{\mathsf{CK}}$, then $\mathsf{T}^{\omega}_{\mathsf{CK}} \vdash A$.*

Proof. Assume that A is valid but not provable in $\mathsf{T}^{\omega}_{\mathsf{CK}}$. By contraposition of the principal syntactic lemma there would need to exist a deduction chain of A which is infinite or ends non-axiomatically. But in this case the principal semantic lemma would supply us with a counter model for A, contradicting our assumption. Thus A must be provable in $\mathsf{T}^{\omega}_{\mathsf{CK}}$ and indeed the principal syntactic lemma constructs such a proof. □

2.2.3 Syntactic cut-elimination for common knowledge

We have mentioned that there exist several cut-free deductive systems for common knowledge. However, we do not know of syntactic cut-elimination procedures for any of these systems, that is a procedure that transforms a proof which makes use of the rule (cut) to a proof without applications of (cut). Let us look at the problem of cut-elimination in the system $\mathsf{T}^{\omega}_{\mathsf{CK}}$. Consider the following proof:

$$\dfrac{(\Box)\,\dfrac{\begin{matrix}\pi_1\\ A,\Gamma,\tilde{\mathsf{C}}\neg B\end{matrix}}{\Box_i A,\Diamond_i\Gamma,\Sigma,\tilde{\mathsf{C}}\neg B} \qquad (\mathsf{C})\,\dfrac{\cdots\quad \begin{matrix}\pi_{2k}\\ \Box^k B,\Delta\end{matrix}\quad\cdots\quad {}_{1\le k<\omega}}{\mathsf{C}B,\Delta}}{\Box_i A,\Diamond_i\Gamma,\Sigma,\Delta}\,(\mathsf{cut})$$

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. The typical transformation would push the left rule instance below the cut, as follows:

$$(\Box)\,\dfrac{(\mathsf{cut})\,\dfrac{\begin{matrix}\pi_1\\ A,\Gamma,\tilde{\mathsf{C}}\neg B\end{matrix} \qquad (\mathsf{C})\,\dfrac{\cdots\quad \begin{matrix}\pi_{2k}\\ \Box^k B,\Delta\end{matrix}\quad\cdots\quad {}_{1\le k<\omega}}{\mathsf{C}B,\Delta}}{A,\Gamma,\Delta}}{\Box_i A,\Diamond_i\Gamma,\Sigma,\Diamond_i\Delta}$$

However, this transformation introduces the $\Diamond_i$ in $\Diamond_i\Delta$, and thus it does not yield a proof of the original conclusion. This is caused by the context restriction in the ($\Box$)-rule.

In **Syntactic cut-elimination for common knowledge [22]**, we present a syntactic cut-elimination procedure for an infinitary system of common knowledge. In this system we use deep sequents which are essentially trees and where rules apply anywhere deep inside of these trees. The general idea of applying rules deeply has been proposed several times in different forms and for different purposes. Schütte already used it in order to obtain systems without contraction and weakening, which he considered more elegant [69]. Guglielmi used it to give a proof-theoretic system for a certain substructural logic which cannot be captured in the sequent calculus. To do so, he developed the calculus of structures, a formalism which is centered around deep inference and abolishes the traditional format of sequent calculus proofs [37].

The calculus of structures then has also been developed for modal logic [77]. Based on these ideas, Brünnler introduced the notion of a deep sequent and gave a systematic set of sequent systems and a corresponding cut-elimination procedure for the modal logics between K and $\mathsf{S5}$ [20]. Kashima had used the same notion of sequent already in [45] in order to give cut-free sequent systems for some tense logics. Based on Kashima's ideas, Tanaka [81] introduced a system for predicate common knowledge logic. It essentially also uses what we call deep sequents. In fact, if one disregards the rather different notation and some choices in the formulation of rules, then one could say that our system is the propositional part of Tanaka's system. We already have observed that applying rules deeply is also important to adapt the method of deduction chains to common knowledge, see Remark 23.

There are cut-elimination procedures available for similar logics, for example by Pliuskevicius [61] for an infinitary system for linear time temporal logic. However, he does not need deep sequents. For linear time temporal logic it is enough to use indexed formulae of the form A_i which denote A at the i-th moment in time.

Deep sequents. A *deep sequent* is a finite multiset of formulae and boxed sequents. A *boxed sequent* is an expression $[\Gamma]_i$ where Γ is a deep sequent and $1 \leq i \leq h$. The letters $\Gamma, \Delta, \Lambda, \Pi, \Sigma$ now denote deep sequents and the word sequent now refers to deep sequent, except when it is clear from the context that a sequent is shallow, such as a sequent appearing in a derivation in $\mathsf{T}^{\omega}_{\mathsf{CK}}$. A sequent is always of the form

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

where the i_j denote agents and thus range from 1 to h. As usual, the comma denotes multiset union and there is no distinction between a singleton multiset and its element.
Fix an arbitrary linear order on formulae. Fix an arbitrary linear order on boxed sequents. The *corresponding formula* of a non-empty sequent Γ, denoted $\underline{\Gamma}_{\mathsf{F}}$, is defined as follows:

$$\underline{A_1, \dots, A_m, [\Delta_1]_{i_1}, \dots, [\Delta_n]_{i_n}}_{\mathsf{F}} = A_1 \vee \dots \vee A_m \vee \Box_{i_1} \underline{\Delta_1}_{\mathsf{F}} \vee \dots \vee \Box_{i_n} \underline{\Delta_n}_{\mathsf{F}} \ ,$$

where formulae and boxed sequents are listed according to the fixed orders. The *corresponding formula* of an empty sequent is $\bot$.

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

$$\Gamma\{\Delta\} = A, [[B], C, [D]] \quad .$$

Let us now introduce our system of deep sequents.

Definition 25 (The system $\mathsf{D}^{\omega}_{\mathsf{CK}}$)**.**

Propositional axioms and rules: For all contexts $\Gamma\{\}$, p in Φ , and all formulae A, B

$$\Gamma\{\mathsf{p}, \sim\mathsf{p}\} \qquad \Gamma\{\top\} \qquad \frac{\Gamma\{A\} \quad \Gamma\{B\}}{\Gamma\{A \wedge B\}}\ (\wedge) \qquad \frac{\Gamma\{A, B\}}{\Gamma\{A \vee B\}}\ (\vee)$$

Modal rules: For all contexts $\Gamma\{\}$, sequents Δ, formulae A, and all indices i from M

$$\frac{\Gamma\{[A]_i\}}{\Gamma\{\Box_i A\}}\ (\Box) \qquad \frac{\Gamma\{\Diamond_i A, [\Delta, A]_i\}}{\Gamma\{\Diamond_i A, [\Delta]_i\}}\ (\Diamond)$$

Fixed point rules: For all contexts $\Gamma\{\}$ and formulae A

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

We will also consider the structural rules *necessitation*, *weakening*, and *contraction*

$$\frac{\Gamma}{[\Gamma]_i}\ (\mathsf{nec}) \qquad \frac{\Gamma\{\emptyset\}}{\Gamma\{\Delta\}}\ (\mathsf{wk}) \qquad \frac{\Gamma\{\Delta, \Delta\}}{\Gamma\{\Delta\}}\ (\mathsf{ctr})$$

as well as the rule *cut*

$$\frac{\Gamma\{A\} \qquad \Gamma\{\neg A\}}{\Gamma\{\emptyset\}} \quad (\mathsf{cut}).$$

In an application of the rule (cut) the formula A is called the *cut formula*. Notice that the rules of system $\mathsf{D}^{\omega}_{\mathsf{CK}}$ are different from the corresponding rules in system $\mathsf{T}^{\omega}_{\mathsf{CK}}$ but have the same names. If we refer to a rule only by its name then it will be clear from the context which rule is meant. For example the cut in $\mathsf{T}^{\omega}_{\mathsf{CK}} + (\mathsf{cut})$ is the one associated to system $\mathsf{T}^{\omega}_{\mathsf{CK}}$ and the one in $\mathsf{D}^{\omega}_{\mathsf{CK}} + (\mathsf{cut})$ is the one associated with system $\mathsf{D}^{\omega}_{\mathsf{CK}}$.

Cut rank and derivability. We define the *rank* $\mathsf{rk}(A)$ of a formula A as follows:

$$\begin{aligned}
&\mathsf{rk}(\mathsf{p}) := \mathsf{rk}(\sim\mathsf{p}) := \mathsf{rk}(\top) := \mathsf{rk}(\bot) := 0\\
&\mathsf{rk}(A \land B) := \mathsf{rk}(A \lor B) := \max(\mathsf{rk}(A), \mathsf{rk}(B)) + 1\\
&\mathsf{rk}(\Box_i A) := \mathsf{rk}(\Diamond_i A) := \mathsf{rk}(A) + 1\\
&\mathsf{rk}(\mathsf{C}A) := \mathsf{rk}(\tilde{\mathsf{C}}A) := \omega + \mathsf{rk}(A)
\end{aligned}$$

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

Admissibility and invertibility. An inference rule ρ is *depth- and cut-rank-preserving admissible* or, for short, *perfectly admissible* for a system $\mathcal{S}$ if for each instance of ρ with premises $\Gamma_1, \Gamma_2 \ldots$ and conclusion Δ, whenever $\mathcal{S} \mid\!\frac{\alpha}{\gamma}\, \Gamma_i$ for each premise Γ_i then $\mathcal{S} \mid\!\frac{\alpha}{\gamma}\, \Delta$. For each rule ρ there is its *inverse*, denoted by $\neg\rho$, which has the conclusion of ρ as its only premise and any premise of ρ as its conclusion. An inference rule ρ is *perfectly invertible* for a system $\mathcal{S}$ if $\neg\gamma$ is perfectly admissible for $\mathcal{S}$.

Lemma 26 (Admissibility of the structural rules and invertibility)**.**

1. *The rules necessitation, weakening and contraction are perfectly admissible for system* $\mathsf{D}^{\omega}_{\mathsf{CK}}$.

2. *All rules in* $\mathsf{D}^{\omega}_{\mathsf{CK}}$ *are perfectly invertible for* $\mathsf{D}^{\omega}_{\mathsf{CK}}$.

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 [72]. The *binary Veblen function* φ 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 [62, 63] and Schütte [72], 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 27 (Reduction Lemma)**.** *For every formula A with $\mathsf{rk}(A) = \gamma$ we have that*

$$\textit{if } \mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha_1}{\underset{\gamma}{\vdash}} \Gamma\{A\} \textit{ and } \mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha_2}{\underset{\gamma}{\vdash}} \Gamma\{\neg A\}, \textit{ then } \mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha_1 \# \alpha_2}{\underset{\gamma}{\vdash}} \Gamma\{\emptyset\}.$$

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

Lemma 28 (First Elimination Lemma)**.** *If $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{\gamma+1}{\vdash}} \Gamma$ then $\mathsf{D}^\omega_{\mathsf{CK}} \overset{2^\alpha}{\underset{\gamma}{\vdash}} \Gamma$.*

Lemma 29 (Second Elimination Lemma)**.** *If $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{\beta+\omega^\gamma}{\vdash}} \Gamma$ then $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\varphi_\gamma\alpha}{\underset{\beta}{\vdash}} \Gamma$.*

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 30 (Cut-elimination for the deep system)**.** *If $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{\omega\cdot n}{\vdash}} \Gamma$ then $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\varphi_1^n(\alpha)}{\underset{0}{\vdash}} \Gamma$.*

There are the followings embeddings of the shallow system into the deep system and vice versa.

Theorem 31 (Shallow into deep)**.** *If $\mathsf{T}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{\gamma}{\vdash}} \Gamma$ then $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\omega\cdot\alpha}{\underset{\gamma}{\vdash}} \Gamma$.*

Theorem 32 (Deep into shallow)**.** *If $\mathsf{D}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{0}{\vdash}} \Gamma$ then $\mathsf{T}^\omega_{\mathsf{CK}} \overset{\omega\cdot(\alpha+1)}{\underset{0}{\vdash}} \underline{\Gamma}_{\mathsf{F}}$.*

We can now state the cut-elimination theorem for the shallow system.

Theorem 33 (Cut-elimination for the shallow system)**.**
If $\mathsf{T}^\omega_{\mathsf{CK}} \overset{\alpha}{\underset{\omega\cdot n}{\vdash}} \Gamma$ then $\mathsf{T}^\omega_{\mathsf{CK}} \overset{\omega\cdot(\varphi_1^n(\omega\cdot\alpha)+1)}{\underset{0}{\vdash}} \Gamma$.

We will now embed H_{CK} into $\mathsf{D}^{\omega}_{\mathsf{CK}} + (\mathsf{cut})$, keeping track of the proof depth and thus, via cut elimination for $\mathsf{D}^{\omega}_{\mathsf{CK}}$, establish an upper bound for proofs in $\mathsf{D}^{\omega}_{\mathsf{CK}}$. Via the embedding of the deep into the shallow system, this bound also holds for the shallow system.

Theorem 34. *If* $\mathsf{H}_{\mathsf{CK}} \vdash A$ *then* $\mathsf{D}^{\omega}_{\mathsf{CK}} \vdash^{<\omega^2}_{\omega^2} A$.

Theorem 35 (Upper bounds)**.** *If A is a valid formula, then*

1. $\mathsf{D}^{\omega}_{\mathsf{CK}} \vdash^{<\varphi_2 0}_{0} A$*, and*
2. $\mathsf{T}^{\omega}_{\mathsf{CK}} \vdash^{<\varphi_2 0}_{0} A$.

The following figure summarizes the various embeddings we have established.

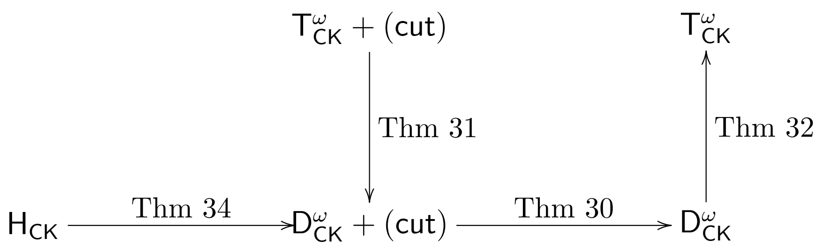

Figure 2.1: Overview of the various embeddings

We have looked at common knowledge based on the least normal modal logic. However, we believe that our approach is independent of the particular axiomatization of knowledge. The modal logic $\mathsf{S5}$ seems to be *the* system for knowledge. Contrary to shallow sequents, deep sequents can easily handle $\mathsf{S5}$, see [20]. So it is straightforward to design a system for $\mathsf{S5}$-based common knowledge. Generalizing contexts to allow two holes, the rule to add would be

$$\frac{\Gamma\{\Diamond A\}\{A\}}{\Gamma\{\Diamond A\}\{\emptyset\}} \quad (\mathsf{S5}).$$

2.2.4 Common knowledge does not have the Beth property

Craig interpolation and *Beth definability* have become traditional questions to ask of a logic system. They are important properties both at the theoretical and at the practical level. Let us only mention some areas of computer science where interpolation is applied: hardware/software specification, reasoning with large knowledge bases, type inference, theorem proving, and model checking.

It was an open question whether the logic of common knowledge has interpolation. We were able to show that this is not the case in **Common knowledge does not have the Beth property [79]**.

Our proof that common knowledge does not have the Beth property is a variant of Maksimova's proof that temporal logics with 'the next' do not have the Beth property [54, 55]. See also [48] for a generalization of that proof to fragments of propositional dynamic logic. Let us write $A(P_1, \dots, P_n)$ to indicate that the formula A contains at most the displayed atomic propositions $P_1, \dots, P_n$ where we abbreviate such a sequence by $\vec{P}$. Then the *global Beth property* (B2) states that for any formula $A(\vec{P}, X)$ if

$$A(\vec{P}, X), A(\vec{P}, Y) \models X \leftrightarrow Y,$$

then there exists a formula $B(\vec{P})$ such that

$$A(\vec{P}, X) \models X \leftrightarrow B(\vec{P}).$$

The *Craig interpolation property* (CIP) states that if

$$A(\vec{P}, \vec{Q}) \rightarrow B(\vec{P}, \vec{R})$$

is valid, then there exists a formula $C(\vec{P})$ such that

$$A(\vec{P}, \vec{Q}) \rightarrow C(\vec{P}) \text{ and } C(\vec{P}) \rightarrow B(\vec{P}, \vec{R})$$

are valid. Gabbay and Maksimova [35] provide an extensive study of these and related concepts for modal and intuitionistic logics.

We define the following formulae where $\mathsf{C}^+ A := \mathsf{C}A \land A$ and P, X, Y are different atomic propositions.

$$\begin{aligned} A_1(P, X) &:= \mathsf{C}^+(\tilde{\mathsf{E}}X \leftrightarrow \sim\mathsf{X} \land \tilde{\mathsf{C}}\sim\mathsf{P}), \\ A_2(P, X) &:= \mathsf{C}^+(X \rightarrow \tilde{\mathsf{C}}\sim\mathsf{P}), \\ A_3(P) &:= \mathsf{C}^+\tilde{\mathsf{C}}\mathsf{C}P, \\ A_4(X) &:= \mathsf{C}^+(\mathsf{E}X \leftrightarrow \tilde{\mathsf{E}}X). \end{aligned}$$

Using these definitions, we set

$$A(P, X) := A_1(P, X) \land A_2(P, X) \land A_3(P) \land A_4(X).$$

Note that the formula $A(P, X) \land A(P, Y) \rightarrow (X \leftrightarrow Y)$ is valid. That means $A(P, X)$ defines X implicitly. We will show in the following that there cannot be an explicit definition of X. Hence, Beth definability does not hold for the logic of common knowledge.

Theorem 36. *The logic of common knowledge does not posses the global Beth property* (B2)*.*

Proof. Let $\mathcal{Z}$ be the Kripke model given by:

1. the domain of $\mathcal{Z}$ is the set of integers,
2. the accessibility relations R_i for $1 \leq i \leq h$ are given by $R_i(u, v)$ if and only if $v = u + 1$,
3. $\mathcal{Z}, u \models X$ if and only if u is odd and $u < 0$,
4. $\mathcal{Z}, u \models P$ if and only if $u \geq 0$.

We have $\mathcal{Z} \models A(P, X)$.
Let us call a formula B *L-stable in* $\mathcal{Z}$ if

$$\exists u \forall v \leq u(\mathcal{Z}, v \models B \Leftrightarrow \mathcal{Z}, u \models B).$$

By induction on the structure of formulae we easily see that every formula B which contains only P as a variable is L-stable in $\mathcal{Z}$. Therefore, for each formula B which contains only P as a variable, there exists a $u < 0$ such that $\mathcal{Z}, u \models B \Leftrightarrow \mathcal{Z}, u - 1 \models B$. However, by definition we have $\mathcal{Z}, u \models X \Leftrightarrow \mathcal{Z}, u - 1 \not\models X$. Hence B and X must have different truth values either at u or at $u - 1$. That means $\mathcal{Z} \not\models B \leftrightarrow X$. Because of $\mathcal{Z} \models A(P, X)$ this implies $A(P, X) \not\models X \leftrightarrow B(\vec{P})$. □

Theorem 37. *The logic of common knowledge lacks interpolation* (CIP)*.*

Proof. Let us introduce another (local) version (B1) of the Beth property: for any formula $A(\vec{P}, X)$ if

$$\models A(\vec{P}, X) \wedge A(\vec{P}, Y) \rightarrow (X \leftrightarrow Y),$$

then there exists a formula $B(\vec{P})$ such that

$$\models A(\vec{P}, X) \rightarrow (X \leftrightarrow B(\vec{P})).$$

The fact that $A(P, X) \wedge A(P, Y) \rightarrow (X \leftrightarrow Y)$ is valid and the model in the proof of the previous theorem show that (B1) does not hold for the logic of common knowledge. We conclude that the logic of common knowledge does not enjoy Craig interpolation (CIP) because (B1) can be derived from (CIP), see [26, 35]. □

2.2.5 Total public announcements

At the end of the eighties, Plaza published the famous article about logics of public communications [60]. In the sequel, the theory of knowledge change caused by incoming information has been further developed by many authors. We confine ourselves to mentioning just a few typical articles: Baltag et al. [11, 12], van Benthem et al. [15, 16], van Ditmarsch et al. [28, 29, 30], as well as Renne [65].

The language for logics of public announcements is the language of standard multi-modal logic augmented with announcement operators $[A]$ for every formula A. The expression $[A]B$ then stands for *after every announcement of A, it holds that B*. In the classical setting, only *truthful* announcements are considered in the sense that receiving a false announcement will lead to an inconsistent epistemic state. Formally, we have that

$$\neg[A]\bot \tag{2.2}$$

is not valid, see [29, Proposition 4.11].

We propose a system in which all announcements are considered, that means (2.2) holds. Therefore, in our system announcements need not be truthful; they can be true or false. As usual, a true announcement will lead to an update of an agent's epistemic state. However, a false announcement will not lead to an inconsistent epistemic state, it will automatically be ignored by the agent. That is, after a false announcement, an agent will have the same epistemic state as before the announcement. Because (2.2) holds in our system, we call it *consistency preserving*. The fact that announcements need not be truthful is of particular importance if not only the agents' knowledge but also their beliefs are considered. See Steiner's forthcoming PhD thesis [75] for a detailed treatment of this topic.

A property we keep from the classical setting is

$$\mathsf{p} \to [A]\mathsf{p}. \tag{2.3}$$

That means, an announcement does not change atomic facts. We call a system that satisfies (2.3) *atomic preserving*.

In **Total public announcements [76]**, we present axiomatizations for public announcements which satisfy both (2.2) and (2.3). We also propose a Kripke semantics for our systems and show soundness and completeness of our axiomatizations. For certain announcements, we show that agents can achieve common knowledge by receiving the announcement. We investigate total public announcements for $\mathsf{S5}$, for the logic of common knowledge as well as for so-called relativized common knowledge. In the sequel we present our results in the context of common knowledge.

Language and semantics.

Definition 38. Define the formulae of the language $\mathcal{L}_{\mathsf{A}}$ inductively like the language $\mathcal{L}_{\mathsf{CK}}$ with the additional clause:

5. If A and B are formulae of $\mathcal{L}_{\mathsf{A}}$, then so is $[A]B$.

The formula $[A]B$ means B *holds after the public announcement of* A. As usual, the formal semantics of an announcement is given in terms of deleting edges in a Kripke structure.

Definition 39 (Denotation)**.** Let $\mathsf{K} = (S, R, \pi)$ be a Kripke structure. For every $A \in \mathcal{L}_{\mathsf{A}}$ we define the set $\|A\|_{\mathsf{K}} \subset S$ by adding the following clause to Definition 13:

$$\|[C]B\|_{\mathsf{K}} := \{s \in S : \mathsf{K}^{C,s}, s \models B\}$$

where for given $C \in \mathcal{L}_{\mathsf{A}}$ and $s \in S$, the Kripke structure $\mathsf{K}^{C,s}$ is simultaneously defined by

$$\begin{array}{rcl} \mathsf{K}^{C,s} & := & (S, R_1^{C,s}, \ldots, R_n^{C,s}, V), \\ R_i^{C,s} & := & \begin{cases} R_i \cap \{(u,v) \in S^2 \mid \mathsf{K}, u \models C \text{ iff } \mathsf{K}, v \models C\} & \text{if } \mathsf{K}, s \models C, \\ R_i & \text{if } \mathsf{K}, s \not\models C. \end{cases} \end{array}$$

The notions of validity and satisfiability of $\mathcal{L}_{\mathsf{A}}$ formulae are defined accordingly. Again we write $\mathsf{K} \models A$ if $\|A\|_{\mathsf{K}} = S$.

Note that if all R_i in K are equivalence relations, then $\mathsf{K}^{C,s}$ belongs to $\mathcal{K}^{eq}$. As before, we say an $\mathcal{L}_{\mathsf{A}}$ formula A is $\mathsf{S5}$-*valid*, if and only if $\mathsf{K} \models A$ for all $\mathsf{K} \in \mathcal{K}^{eq}$.

Deductive system.

Definition 40 (The system $\mathsf{H}_{\mathsf{S5}}^{\mathsf{C},\mathrm{PubAn}}$)**.** The system $\mathsf{H}_{\mathsf{S5}}^{\mathsf{C},\mathrm{PubAn}}$ is defined by extending H_{CK} with the axioms (T), (4), (5), and adding the following axioms and rules for announcements.

Announcements axioms and rules: For all p in Φ, all formulae A, B, C, and all indices i from M

$$\begin{array}{ll} [A]\mathsf{p} \leftrightarrow \mathsf{p} & (\mathsf{A1}) \\ [A](B \to C) \to ([A]B \to [A]C) & (\mathsf{A2}) \\ [A]\neg B \leftrightarrow \neg[A]B & (\mathsf{A3}) \\ A \to ([A]\Box_i B \leftrightarrow \Box_i(A \to [A]B)) & (\mathsf{A4}) \\ \neg A \to ([A]B \leftrightarrow B) & (\mathsf{A5}) \\ A \wedge [A]B \to ([A][B]C \leftrightarrow [A \wedge [A]B]C) & (\mathsf{A6}) \end{array}$$

$$\frac{A}{[B]A} \quad (\mathsf{NEC.2}) \qquad \frac{A \to [B]C \qquad A \wedge B \to \mathsf{E}(B \to A)}{A \wedge B \to [B]\mathsf{C}C} \quad (\mathsf{IND.2}).$$

Observe, that the public announcement operator is self-dual due to axiom ($\mathsf{A3}$). This means we do not have to distinct the statements 'B holds after *every* (truthful) public announcement of A' and 'B holds after *some* (truthful) public announcement of A'. In our setting, there is only one public announcement of a formula. It can be truthful or not.

The model change which is caused by a public announcement is a relativization to a submodel, see van Benthem and Ikegami [16]. Many logics are closed under relativizations. If this is the case for a given logic, then we can extend it by announcement operators and establish a translation from the logic with announcement operators into the logic without announcement operators. Completeness of the logic without announcement operators then implies completeness for the logic with announcement operators.

Van Benthem, van Eijck and Kooi [15] observed that the logic of common knowledge is not closed under relativizations. Therefore a reduction to the logic without announcement operators is not possible. Thus we have to employ the method of maximal consistent sets to show completeness. Our argument is the same as the one presented in [32] for the logic of common knowledge except that we have more cases in the truth lemma.

Theorem 41 (Soundness and completeness of $\mathsf{H}^{\mathsf{C},\mathrm{PubAn}}_{\mathsf{S5}}$)**.** *For any formula A of $\mathcal{L}_\mathsf{A}$ we have that*

$$A \textit{ is } \mathsf{S5}\textit{-valid if and only if } \mathsf{H}^{\mathsf{C},PubAn}_{\mathsf{S5}} \vdash A.$$

Immediate consequences of this completeness proof are the finite model property and the decidability of the satisfiability problem.

Next, we observe that agents can acquire common knowledge by receiving an announcement. To show this, we need the notion of an announcement resistant formula. An $\mathcal{L}_\mathsf{A}$ formula A is called *announcement resistant*, if

$$\mathsf{H}^{\mathsf{C},\mathrm{PubAn}}_{\mathsf{S5}} \vdash A \to [B]A$$

for every $\mathcal{L}_\mathsf{A}$ formula B. One can show that all propositional formulae as well as all provable $\mathcal{L}_\mathsf{A}$ formulae are announcement resistant. In addition, if A and B are announcement resistant, then so also are the formulae $A \wedge B$, $A \vee B$, $\Box_i A$, and $\mathsf{C}A$. We have the following theorem about acquiring common knowledge where $[A]^1 B := [A]B$ and $[A]^{k+1}B := [A][A]^k B$.

Theorem 42. *Let A be an announcement resistant $\mathcal{L}_\mathsf{A}$ formula. Then for all $k \geq 1$ we have*

$$\mathsf{H}^{\mathsf{C},PubAn}_{\mathsf{S5}} \vdash A \to [A]^k \mathsf{C}A.$$

Chapter 3

Modal μ-Calculus

3.1 Introduction

The logic of common knowledge is an extension of modal logic by one particular fixed point construction, see (2.1). Let us now consider the addition of general least and greatest fixed point operators to modal logic which results in the so-called modal μ-calculus.

The modal μ-calculus is a logic used extensively in certain areas of computer science. It has its origin in the area of logics for the specification and verification of properties of programs. Such logics have a long tradition in computer science and many systems have been studied in the literature. Let us only mention Propositional Dynamic Logic PDL [34, 64], Computational Tree Logic CTL [25], and Hennessy-Milner Logic HML [39] to name a few.

The use of fixed point operators in program logics goes back at least to De Bakker, Park and Scott, see for instance [9, 10, 59]. Then in 1983, Dexter Kozen [46] published a study of a logic that combined simple modalities (like in HML) with fixed point operators to provide a form of recursion. This logic, the modal μ-calculus, has a simple syntax, an easily given semantics, and yet the fixed points provide immense power. Most other modal logics can be seen as fragments of the μ-calculus. It also provides one of the strongest examples of the connections between modal and temporal logics, automata theory and the theory of games.

Language. $\mathcal{L}_\mu$ is the language of (multi-)modal logic extended by least and greatest fixed point operators. We also consider the language $\mathcal{L}_\mu^+$ which is $\mathcal{L}_\mu$ with additional formulae to explicitly represent the finite approximations $(\nu^k \mathsf{X})\mathcal{A}$ of a greatest fixed point $(\nu \mathsf{X})\mathcal{A}$.

Definition 43 (Language $\mathcal{L}_\mu$)**.** Let

$$\mathsf{V} = \{\mathsf{X}, {\sim}\mathsf{X}, \mathsf{Y}, {\sim}\mathsf{Y}, \mathsf{Z}, {\sim}\mathsf{Z}, \ldots\}$$

be a set containing countably many variables and their negations. Define the formulae of the language $\mathcal{L}_\mu$ inductively like the language $\mathcal{L}$ with the additional clauses:

4. If P is an element of V, then P is a formula of $\mathcal{L}_\mu$.
5. If A is a formula of $\mathcal{L}_\mu$ and the negated variable ${\sim}\mathsf{X}$ does not occur in A, then $(\mu\mathsf{X})A$ and $(\nu\mathsf{X})A$ are also formulae of $\mathcal{L}_\mu$.

If the negated variable ${\sim}\mathsf{X}$ does not occur in a formula A of $\mathcal{L}_\mu$, we say that A is X–positive or alternatively positive in X. Formulae which are positive in a certain variable determined by the context will henceforth be denoted by letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$. Furthermore, we will call a formula A of $\mathcal{L}_\mu$ closed, if it does not contain free variables.

Definition 44 (Language $\mathcal{L}_\mu^+$)**.** The formulae of the extended language $\mathcal{L}_\mu^+$ are defined by adding the following clause to the induction of Definition 43

6. If A is a formula of $\mathcal{L}_\mu^+$ and the negated variable ${\sim}\mathsf{X}$ does not occur in A, then $(\nu^k\mathsf{X})A$ is also a formula of $\mathcal{L}_\mu^+$ for every natural number $k > 0$.

We define X–positive and closed formulae of $\mathcal{L}_\mu^+$ analogously to those of $\mathcal{L}_\mu$.

We use $(\sigma\mathsf{X})\mathcal{A}$ to denote formulae of the form $(\mu\mathsf{X})\mathcal{A}$, $(\nu\mathsf{X})\mathcal{A}$, and $(\nu^k\mathsf{X})\mathcal{A}$ for all k.

Again, for formulae of the language $\mathcal{L}_\mu$ we define negation as usual reflecting in addition the duality laws for fixed points. Negation is not defined for the language $\mathcal{L}_\mu^+$ since we have not included duals for formulae of the form $(\nu^k\mathsf{X})\mathcal{A}$.

Semantics. We extend the standard Kripke semantics for modal logics to give meaning to $\mathcal{L}_\mu^+$ formulae as follows.

Definition 45 (Kripke structure)**.** A Kripke structure $\mathsf{K} = (S, R, \pi)$ for $\mathcal{L}_\mu^+$ is a triple where S is a non–empty set, $R : \mathsf{M} \to \mathcal{P}(S \times S)$ and $\pi : (\Phi \cup \mathsf{V}) \to \mathcal{P}(S)$ is a function such that $\pi({\sim}\mathsf{X}) = S \setminus \pi(\mathsf{X})$ for all ${\sim}\mathsf{X} \in \mathsf{V}$ and $\pi({\sim}\mathsf{p}) = S \setminus \pi(\mathsf{p})$ for all ${\sim}\mathsf{p} \in \Phi$. The function R assigns an accessibility relation to each $i \in \mathsf{M}$ where we write R_i for the relation $R(i)$. Furthermore, given a set $T \subseteq S$ and a variable $\mathsf{X} \in \mathsf{V}$ we define the Kripke structure $\mathsf{K}[\mathsf{X} := T]$ as the triple (S, R, π'), where $\pi'(\mathsf{X}) = T$, $\pi'({\sim}\mathsf{X}) = S \setminus T$ and $\pi'(P) = \pi(P)$ for all other $P \in \Phi \cup \mathsf{V}$.

Assume we are given a Kripke structure $\mathsf{K} = (S, R, \pi)$ and an $\mathcal{L}_\mu^+$ formula A. We define the set of states $\|A\|_\mathsf{K}$ of S at which A holds by induction on the structure of A, with a side induction on all natural numbers greater than 0 to treat greatest fixed point approximations.

Definition 46 (Denotation)**.** Let $\mathsf{K} = (S, R, \pi)$ be a Kripke structure. For every $A \in \mathcal{L}_\mu^+$ we define the set $\|A\|_\mathsf{K} \subseteq S$ by adding the following clauses to Definition 3:

$$\|P\|_\mathsf{K} := \pi(P) \text{ for all } P \in \mathsf{V}.$$

For every formula $(\mu\mathsf{X})\mathcal{A}$ and $(\nu\mathsf{X})\mathcal{A}$ we define

$$\begin{aligned} \|(\mu\mathsf{X})\mathcal{A}\|_\mathsf{K} &:= \bigcap\{T \subseteq S : T \supseteq F^\mathsf{K}_{\mathcal{A},\mathsf{X}}(T)\} \text{ and} \\ \|(\nu\mathsf{X})\mathcal{A}\|_\mathsf{K} &:= \bigcup\{T \subseteq S : T \subseteq F^\mathsf{K}_{\mathcal{A},\mathsf{X}}(T)\} \end{aligned}$$

where $F^\mathsf{K}_{\mathcal{A},\mathsf{X}}$ is the operator on S given by $F^\mathsf{K}_{\mathcal{A},\mathsf{X}}(T) := \|\mathcal{A}\|_{\mathsf{K}[\mathsf{X}:=T]}$ for every subset T of S. Furthermore, if $\mathcal{A}$ is an X–positive formula, then we define $\|(\nu^k\mathsf{X})\mathcal{A}\|_\mathsf{K}$ for every $k > 0$ by induction on k as follows:

$$\begin{aligned} \|(\nu^1\mathsf{X})\mathcal{A}\|_\mathsf{K} &:= \|\mathcal{A}[\top/\mathsf{X}]\|_\mathsf{K} \\ \|(\nu^{k+1}\mathsf{X})\mathcal{A}\|_\mathsf{K} &:= \|\mathcal{A}[(\nu^k\mathsf{X})\mathcal{A}]\|_\mathsf{K}. \end{aligned}$$

Already in his initial study [46], Kozen proposed a Hilbert style deductive system H_μ for the μ-calculus. Its two crucial ingredients are closure axioms - saying that the formula $(\mu\mathsf{X})\mathcal{A}$ denotes a pre-fixed point - and induction rules guaranteeing that this pre-fixed point is a least fixed point. Although this system is very simple and natural, in [46] only completeness for the so-called aconjunctive fragment could be shown. Completeness for the full system remained open for more than a decade until Walukiewicz [85] was able to provide a very intricate completeness proof making use of automata and game theoretic results about the μ-calculus.

There are also other deductive systems available for the μ-calculus. As for common knowledge, one can replace the induction rule with an ω-rule. In the context of the μ-calculus, such a rule has first been proposed by Kozen in [47]. Another approach is to make use of so-called global induction. There, proofs may have infinite long branches or may be circular. Such circular proofs and proofs with infinite long branches then need to fulfill an additional global condition in order to guarantee soundness. An example of a system with infinite long branches is the tableau system for the μ-calculus presented by Niwinski and Walukiewicz [58]. The area of circular logics is also very active.

For instance, Sprenger and Dam [74] compare two proof systems for the μ-calculus each using a different type of induction. Aldwinckle and Cockett [4] claim several proof theoretic results about circular logics. However, they only give examples; but no precise descriptions and also no proofs are provided. Santocanale [66] also investigates a calculus of circular proofs and establishes a form of cut-elimination by exploring the categorical semantics. Therefore, his result applies to systems that are based on intuitionistic logic. Closely related to the modal μ-calculus are the systems for inductive definitions which Brotherston introduces in his recent PhD thesis [19]. He studies the proof theory of systems with induction rules, of infinitary systems, as well as of cyclic systems.

3.2 Contributions

Our contributions to the proof theory of the modal μ-calculus are presented in the following papers:

1. Cut-free axiomatizations for stratified modal fixed point logic [41]
2. Canonical completeness of infinitary μ [43]
3. On the proof theory of the modal mu-calculus [78]

In the sequel we will summarize our results.

3.2.1 Cut-free axiomatizations for stratified modal fixed point logic

In the paper **Cut-free axiomatizations for stratified modal fixed point logic** [41] we introduce an infinitary Tait style deductive system for the stratified fragment SFL of the modal μ-calculus. This fragment captures many important logics like PDL, CTL, and the logic of common knowledge. Here we will not give a precise definition of SFL nor formally state our results since [41] only is a first step towards a canonical completeness proof for the modal μ-calculus. Such a completeness proof for an infinitary system of the μ-calculus will be presented in the next section.

So let us only sketch our results concerning SFL. Its language is stratified in the following sense: Consider a formula $(\mu \mathsf{X})\mathcal{A}$, where $\mathcal{A}$ is positive in the variable X. We require that $\mathcal{A}$ may contain a subformula $(\mu \mathsf{Y})\mathcal{B}$ or $(\nu \mathsf{Y})\mathcal{B}$ only if X does not appear free in $\mathcal{B}$. This allows us to compute the meaning of $(\mu \mathsf{Y})\mathcal{B}$, respectively $(\nu \mathsf{Y})\mathcal{B}$, and then use it to determine the meaning of

$(\mu \mathsf{X})\mathcal{A}$. Stratification guarantees that inner fixed points do not depend on the outer ones. Hence it is possible to determine the meaning of any formula by a simple induction on the levels of its fixed points and its complexity.

This is not possible when interleaving of fixed points is allowed. Consider the formula of the form $(\mu \mathsf{X})(\nu \mathsf{Y})\mathcal{A}[\mathsf{X}, \mathsf{Y}]$. Here the meaning of the inner fixed point $(\nu \mathsf{Y})\mathcal{A}[\mathsf{X}, \mathsf{Y}]$ depends on the value assigned to X by the interpretation of the outer fixed point $(\mu \mathsf{X})(\nu \mathsf{Y})\mathcal{A}[\mathsf{X}, \mathsf{Y}]$ which in turn depends on $(\nu \mathsf{Y})\mathcal{A}[\mathsf{X}, \mathsf{Y}]$. Hence interleaving has the effect that the meaning of nested fixed points cannot be determined one after another, but has to be treated in a more complicated way.

Turning to our deductive systems for SFL we (i) provide a canonical completeness proof for it and (ii) show soundness of the finitary version of our deductive system, similar to our result in Section 2.2.1 for common knowledge. Furthermore, it is obvious that everything provable in the infinitary system is also provable in the finitized version and, consequently, both systems are sound and complete.

3.2.2 Canonical completeness of infinitary μ

We extend our techniques to the modal μ-calculus in the paper **Canonical completeness of infinitary** μ [43]. There we introduce the cut-free infinitary system $\mathsf{T}^{\omega}_{\mu+}$ and establish its completeness by a canonical counter model construction. This is the only available completeness proof for a deductive system for the modal μ-calculus which is based on standard techniques from modal logic. Thus our completeness proof is conceptually much simpler than previous completeness proofs for systems for the μ-calculus. In fact, all the previous proofs need to make heavy use of automata- or game-theoretic machinery.

As for the logic of common knowledge and SFL, we can establish soundness and completeness for the finitary version of $\mathsf{T}^{\omega}_{\mu+}$ that is based on a restricted ω-rule. Thus we obtain a finite cut-free deductive system for the modal μ-calculus.

In the context of the μ-calculus, the ω-rule has been introduced by Kozen in [47]. There, he establishes the finite model property of the μ-calculus by relating it to the theory of well-quasi-orders. This allows him to introduce an ω-rule which derives the validity of a greatest fixed point from the validity of all its (infinitely many) finite approximations. The finite model property guarantees that it is enough to consider only the finite approximations as premises in the ω-rule. Thus the resulting system is sound and complete. However, note that Kozen's infinitary system makes crucial use of a cut rule.

Definition 47 (The system $\mathsf{T}^{\omega}_{\mu+}$)**.** The system $\mathsf{T}^{\omega}_{\mu+}$ is formulated in the language $\mathcal{L}^{+}_{\mu}$. It is defined by adding the following axioms and inference rules to $\mathsf{T}_{\mathsf{Mod}}$:

Axioms: For all sequents Γ and all X in V

$$\frac{}{\Gamma, \mathsf{X}, {\sim}\mathsf{X}} \quad (\mathsf{ID3})$$

Approximation rules: For all sequents Γ and X–positive formulae $\mathcal{A}$ and all natural numbers $k > 0$

$$\frac{\Gamma, \mathcal{A}[\top/\mathsf{X}]}{\Gamma, (\nu^1\mathsf{X})\mathcal{A}} \quad (\nu.1) \qquad\qquad \frac{\Gamma, \mathcal{A}[(\nu^k\mathsf{X})\mathcal{A}]}{\Gamma, (\nu^{k+1}\mathsf{X})\mathcal{A}} \quad (\nu.k+1)$$

Fixed point rules: For all sequents Γ and X–positive formulae $\mathcal{A}$

$$\frac{\Gamma, \mathcal{A}[(\mu\mathsf{X})\mathcal{A}]}{\Gamma, (\mu\mathsf{X})\mathcal{A}} \quad (\mu) \qquad\qquad \frac{\Gamma, (\nu^k\mathsf{X})\mathcal{A} \quad \text{for all } k \geq 1}{\Gamma, (\nu\mathsf{X})\mathcal{A}} \quad (\nu.\omega)$$

In the sequel we give a sketch of our completeness proof. We assign to every $\mathcal{L}^{+}_{\mu}$ formula A a sequence of ordinals $rk(A)$ called the *rank of* A. By $<_{lex}$ we denote the lexicographic ordering on these sequences. The rank function is defined such that the following lemma holds.

Lemma 48. *For all formulae B, C, and $(\nu\mathsf{X})\mathcal{A}$ of $\mathcal{L}^{+}_{\mu}$ and all natural numbers $n > 0$ we have*

1. $rk(B), rk(C) <_{lex} rk(B \vee C) = rk(B \wedge C)$
2. $rk(B) <_{lex} rk(\Box_i B) = rk(\Diamond_i B)$
3. $rk(\mathcal{A}[\top/\mathsf{X}]) <_{lex} rk((\nu^1\mathsf{X})\mathcal{A})$
4. $rk(\mathcal{A}[(\nu^n\mathsf{X})\mathcal{A}]) <_{lex} rk((\nu^{n+1}\mathsf{X})\mathcal{A})$
5. $rk((\nu^n\mathsf{X})\mathcal{A}) <_{lex} rk((\nu\mathsf{X})\mathcal{A})$

Remark 49. *It is not possible that the rank function additionally satisfies the following condition*

$$rk(\mathcal{A}[(\mu\mathsf{X})\mathcal{A}]) \leq_{lex} rk((\mu\mathsf{X})\mathcal{A})$$

for then we would have

$$\begin{aligned} rk((\mu\mathsf{X})(\nu\mathsf{Y})\mathsf{X} \wedge \mathsf{Y}) &<_{lex} rk(((\mu\mathsf{X})(\nu\mathsf{Y})\mathsf{X} \wedge \mathsf{Y}) \wedge \top) \\ &<_{lex} rk((\nu^1\mathsf{Y})((\mu\mathsf{X})(\nu\mathsf{Y})\mathsf{X} \wedge \mathsf{Y}) \wedge \mathsf{Y}) \\ &<_{lex} rk((\nu\mathsf{Y})((\mu\mathsf{X})(\nu\mathsf{Y})\mathsf{X} \wedge \mathsf{Y}) \wedge \mathsf{Y}) \\ &\leq_{lex} rk((\mu\mathsf{X})(\nu\mathsf{Y})\mathsf{X} \wedge \mathsf{Y}) \end{aligned}$$

which is a contradiction.

Note that $<_{lex}$ is a wellordering on every set of sequences of ordinals with length bounded by some natural number, though not a wellordering in general. Hence, proofs by induction on the rank of formulae are only possible if we can restrict ourselves to a classes of formulae where the length of the rank is bounded. The strong closure $\mathbb{SC}(D)$ of a formula D, see [43], is such a class which suffices for our purposes,

In order to show completeness of $\mathsf{T}^{\omega}_{\mu+}$, we aim at building a counter model to any non-provable formulae D. The worlds of this model will consist of so-called D-saturated sets.

Definition 50 (D–saturated set)**.** Let D be a closed formula of $\mathcal{L}_{\mu}$. A finite subset Γ of $\mathbb{SC}(D)$ is called D–saturated (with respect to $\mathsf{T}^{\omega}_{\mu+}$) if all of the following conditions are satisfied:

(S.1) $\mathsf{T}^{\omega}_{\mu+} \nvdash \Gamma$.

(S.2) For all formulae A and B of $\mathcal{L}^{+}_{\mu}$ we have

$$\begin{aligned} A \vee B \in \Gamma \quad &\Longrightarrow \quad A \in \Gamma \quad \text{and} \quad B \in \Gamma, \\ A \wedge B \in \Gamma \quad &\Longrightarrow \quad A \in \Gamma \quad \text{or} \quad B \in \Gamma. \end{aligned}$$

(S.3) For all X–positive formulae $\mathcal{A}$ of $\mathcal{L}^{+}_{\mu}$ and all natural numbers $n > 0$ we have

$$\begin{aligned} (\mu\mathsf{X})\mathcal{A} \in \Gamma \quad &\Longrightarrow \quad \mathcal{A}[(\mu\mathsf{X})\mathcal{A}] \in \Gamma, \\ (\nu\mathsf{X})\mathcal{A} \in \Gamma \quad &\Longrightarrow \quad (\nu^{i}\mathsf{X})\mathcal{A} \in \Gamma \text{ for some natural number } i > 0, \\ (\nu^{n+1}\mathsf{X})\mathcal{A} \in \Gamma \quad &\Longrightarrow \quad \mathcal{A}[(\nu^{n}\mathsf{X})\mathcal{A}] \in \Gamma, \\ (\nu^{1}\mathsf{X})\mathcal{A} \in \Gamma \quad &\Longrightarrow \quad \mathcal{A}[\top/\mathsf{X}] \in \Gamma. \end{aligned}$$

Given a closed formula D of $\mathcal{L}_{\mu}$, any non–provable sequent consisting only of formulae from $\mathbb{SC}(D)$ may be extended to a D–saturated sequent which also only contains formulae from $\mathbb{SC}(D)$. Starting from a non–provable sequent we choose an iterative approach, repeatedly selecting a formula which violates one of the conditions (S.2) or (S.3) and adding suitable formulae to the sequent in order to make the respective condition satisfied. Seeing that this process becomes stable after a finite number of iterations then finishes the proof. Problems arise when we encounter a least fixed point formula, say of the form $(\mu\mathsf{X})\mathcal{A}$ which violates condition (S.3) and for which we must thus add $\mathcal{A}[(\mu\mathsf{X})\mathcal{A}]$. Since this latter formula may itself violate one of the saturation conditions and in general has a greater rank than $(\mu\mathsf{X})\mathcal{A}$ (see Remark 49), the overall rank of violating formulae does not decrease during this step and termination is not guaranteed. Therefore we have to make use of a modified rank function, keeping a history of least fixed point formulae which have already been considered and ignoring these. We obtain the following lemma about the existence of saturated sets.

Lemma 51. *Let D be a closed formula of $\mathcal{L}_\mu$. For every sequent Γ of $\mathbb{SC}(D)$ which is not provable in $\mathsf{T}^\omega_{\mu+}$, there exists a sequent Δ of $\mathbb{SC}(D)$ which is D–saturated and $\Gamma \subseteq \Delta$.*

Definition 52 (Canonical counter model)**.** Let D be a closed formula of $\mathcal{L}_\mu$. Define the triple $\mathsf{K}_D = (S_D, R_D, \pi_D)$ as follows, where $i \in \mathsf{M}$:

$$\begin{aligned} S_D &:= \{\Gamma \subseteq \mathbb{SC}(D) : \Gamma \ D\text{–saturated}\}, \\ R_D(i) &:= \{(\Gamma, \Delta) \in S_D \times S_D : \{B \in \mathbb{SC}(D) : \Diamond_i B \in \Gamma\} \subseteq \Delta\}, \\ \pi_D(P) &:= \{\Gamma \in S_D : P \notin \Gamma\} \text{ for } P \in \Phi \cup \mathsf{V}. \end{aligned}$$

In the sequel, we write $\|A\|_D$ for $\|A\|_{\mathsf{K}_D}$. The so-called Truth Lemma is the crucial ingredient in completeness proofs for modal logics.

Lemma 53 (Truth Lemma)**.** *Let D be a closed formula of $\mathcal{L}_\mu$ and A a closed formula of $\mathbb{SC}(D)$. Then for all D–saturated sequents Γ of $\mathbb{SC}(D)$ we have*

$$A \in \Gamma \implies \Gamma \notin \|A\|_D. \tag{3.1}$$

Proof. We give only a sketch of the proof. We cannot show (3.1) directly. First we have to show that for all sequences of ordinals $\boldsymbol{\sigma}$ of a given length, we have

$$A \in \Gamma \implies \Gamma \notin \|A\|^{\boldsymbol{\sigma}}_D \tag{3.2}$$

where in $\|A\|^{\boldsymbol{\sigma}}_D$ a formula of the form $(\mu\mathsf{X})\mathcal{A}$ is not interpreted by the least fixed point but only by an approximation of the least fixed point. It is $\boldsymbol{\sigma}$ that specifies which approximations we have to take. We can show (3.2) by main induction on $\boldsymbol{\sigma}$ and side induction on the rank of A. The interesting case is if A is of the form $(\mu\mathsf{X})\mathcal{A}$. Then, since $A \in \Gamma$ and Γ is D–saturated, we also have

$$\mathcal{A}[(\mu\mathsf{X})\mathcal{A}] \in \Gamma. \tag{3.3}$$

In order to establish (3.2), we assume that

$$\Gamma \in \|A\|^{\boldsymbol{\sigma}}_D \tag{3.4}$$

and aim to arrive at a contradiction. Since A is of the form $(\mu \mathsf{X})\mathcal{A}$, there exists a sequence of ordinals $\boldsymbol{\tau} <_{lex} \boldsymbol{\sigma}$ with

$$\Gamma \in \|\mathcal{A}[(\mu \mathsf{X})\mathcal{A}]\|_D^{\boldsymbol{\tau}}. \tag{3.5}$$

On the other hand, $\boldsymbol{\tau} <_{lex} \boldsymbol{\sigma}$ implies that (3.3) together with the main induction hypothesis yields

$$\Gamma \notin \|\mathcal{A}[(\mu \mathsf{X})\mathcal{A}]\|_D^{\boldsymbol{\tau}}. \tag{3.6}$$

Since (3.5) and (3.6) present us with a contradiction, our assumption (3.4) must have been false. Thus we have established (3.2). Further, we can show that there is a sequence of ordinals $\boldsymbol{\kappa}$ with $\|A\|_D \subseteq \|A\|_D^{\boldsymbol{\kappa}}$. We conclude

$$A \in \Gamma \implies \Gamma \notin \|A\|_D^{\boldsymbol{\kappa}} \implies \Gamma \notin \|A\|_D. \qquad \square$$

Theorem 54 (Completeness of $\mathsf{T}_{\mu+}^{\omega}$)**.** *For all closed formulae A of $\mathcal{L}_\mu$ we have that if A is valid, then $\mathsf{T}_{\mu+}^{\omega} \vdash A$.*

Proof. We show the contrapositive of the asserted implication and thus assume that A is not provable in $\mathsf{T}_{\mu+}^{\omega}$. Then by Lemma 51 there exists an A–saturated sequent Γ of $\mathbb{SC}(A)$ such that $A \in \Gamma$. Applying Lemma 53 we conclude that $\Gamma \notin \|A\|_A$, meaning that A cannot be valid. This concludes the proof. $\square$

Again, it is possible to show soundness of a finitary version $\mathsf{T}_{\mu+}$ of $\mathsf{T}_{\mu+}^{\omega}$. Moreover, note that these systems do not include a cut rule. Thus $\mathsf{T}_{\mu+}$ and $\mathsf{T}_{\mu+}^{\omega}$ are sound and complete cut-free systems for the modal μ-calculus.

3.2.3 On the proof theory of the modal mu-calculus

There are two approaches to give infinitary axiomatizations for the modal μ-calculus. The first approach is to make use of an ω-rule in order to ensure that a fixed point is a least (respectively greatest) one. We followed this approach in the previous section to introduce the system $\mathsf{T}_{\mu+}^{\omega}$.

The second approach is to define a deductive system $\mathsf{T}_{\mu}^{\mathsf{pre}}$ such that in a proof search procedure fixed points are simply unfolded which corresponds to closure of fixed points. This results in a so-called preproof which may have infinitely long branches. A global condition is then added which (roughly) says that in each infinite branch, there must be an outermost greatest fixed point unfolded infinitely often. A tableau version of such a system has first been proposed by Niwinski and Walukiewicz [58]. They establish a completeness result for their system which is the starting point for the completeness proof of the finitary axiomatizations carried out by Walukiewicz [84, 85]. Dax, Hofmann, and Lange [27] present a proof system with infinitely long branches for the linear time μ-calculus. They also mention a related system for the modal μ-calculus. We will employ their formulation of such an infinitary proof system.

The main contribution of our paper **On the proof theory of the modal mu-calculus [78]** is the embedding of $\mathsf{T}^{\omega}_{\mu+}$ in $\mathsf{T}^{\mathsf{pre}}_{\mu}$. That means we provide a translation from proofs in the first system to proofs in the second. This provides completeness of $\mathsf{T}^{\mathsf{pre}}_{\mu}$ since $\mathsf{T}^{\omega}_{\mu+}$ is complete. Moreover, we get a new proof of the finite model property of the μ-calculus. Note that these two results are not new. Already Niwinski and Walukiewicz [58] established a completeness result for a tableau version of $\mathsf{T}^{\mathsf{pre}}_{\mu}$. Moreover, we do not get the exponential bound for the size of the model obtained by Emerson and Jutla [31]. However, our proof translation is a novel construction. We hope that it contributes to a better understanding of the proof theory of modal fixed point logics.

Definition 55. A *preproof* for a sequent Γ of $\mathcal{L}_\mu$ formulae is a possibly infinite tree whose root is labeled with Γ and which is built according to the following rules.

Axioms: For all sequents Γ of $\mathcal{L}_\mu$, all p in Φ, and all X in V

$$\Gamma, \mathsf{p}, {\sim}\mathsf{p} \quad (\mathsf{ID1}), \qquad \Gamma, \top \quad (\mathsf{ID2}), \qquad \Gamma, \mathsf{X}, {\sim}\mathsf{X} \quad (\mathsf{ID3}).$$

Propositional rules: For all sequents Γ and formulae A and B of $\mathcal{L}_\mu$

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

Modal rules: For all sequents Γ and Σ and formulae A of $\mathcal{L}_\mu$ and all indices i from M

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

Fixed point rules: For all sequents Γ and X–positive formulae $\mathcal{A}$ of $\mathcal{L}_\mu$

$$\frac{\Gamma, \mathcal{A}[(\mu\mathsf{X})\mathcal{A}]}{\Gamma, (\mu\mathsf{X})\mathcal{A}}\ (\mu) \qquad\qquad \frac{\Gamma, \mathcal{A}[(\nu\mathsf{X})\mathcal{A}]}{\Gamma, (\nu\mathsf{X})\mathcal{A}}\ (\nu)$$

In the sequel we are going to introduce the notion of a thread in a branch of the proof tree.

Definition 56. The *distinguished 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 rule. The formulae in Γ and Σ are called *side formulae* of a rule.

Definition 57. Assume we are given a proof tree for some sequent. For all rule applications r occurring in this proof tree, we define a *connection relation* $\mathsf{Con}(r)$ on formulae as follows.

1. Assume r is not an instance of $(\Box)$. We have $(A, B) \in \mathsf{Con}(r)$ if $A = B$ is a side formula of r or A is an active formula in the conclusion and B is an active formula in a premise of r.

2. Assume r is an instance of $(\Box)$. We have $(\Box_i A, A) \in \mathsf{Con}(r)$ if $\Box_i A$ is the active formula in the conclusion of r and $(\Diamond_i B, B) \in \mathsf{Con}(r)$ if $\Diamond_i B \in \Diamond_i \Gamma$.

Definition 58. Assume we are given a branch $\Gamma_0, \Gamma_1, \ldots$ in a proof tree and let r_i be the rule application that derived Γ_i from Γ_{i+1}. 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.

Definition 59. An $\mathcal{L}_\mu$ formula A is called *well-named* if every variable is bound at most once. Note that for a bound variable X in a well-named formula A, there exists exactly one subformula of A that has the form $(\sigma\mathsf{X})\mathcal{B}$. We then call $(\sigma\mathsf{X})\mathcal{B}$ the *binding formula* of X. If the binding formula of a variable X is of the form $(\nu\mathsf{X})\mathcal{B}$, then X is called a *ν-variable* in A. Let A be formula containing two bound variables X and Y. We say X is *higher* than Y if the binding formula of Y is a subformula of the binding formula of X.

In the sequel we consider only proofs for sequents of well-named formulae.

Note that $\mathsf{T}_\mu^{\mathsf{pre}}$ preproofs may have infinitely long branches and thus also threads may be infinite sequences. We have the following fact about threads.

Lemma 60. *Assume we are given an infinite branch of a preproof for an $\mathcal{L}_\mu$ sequent Γ. Assume we are given a thread in this branch such that infinitely many of its formulae are distinguished formulae of applications of (μ) and (ν). Then there is a unique bound variable X such that*

1. *the binding formula of X occurs infinitely often in the thread and*

2. *for every other formula of the form $(\sigma\mathsf{Y})\mathcal{A}$ which occurs infinitely often, we have that X is higher than Y.*

Definition 61. Assume we are given an infinite branch of a preproof for an $\mathcal{L}_\mu$ sequent Γ. Assume we are given a thread in this branch such that infinitely many of its formulae are distinguished formulae of applications of (μ) and (ν). Such a thread is called a *ν-thread* if the unique variable given by the previous lemma is a ν-variable in Γ.

Definition 62. A $\mathsf{T}_\mu^{\mathsf{pre}}$ *proof* for a sequent Γ of $\mathcal{L}_\mu$ formulae is a preproof of Γ such that every finite branch ends in an axiom and every infinite branch contains a ν-thread. We write $\mathsf{T}_\mu^{\mathsf{pre}} \vdash \Gamma$ if there exists a $\mathsf{T}_\mu^{\mathsf{pre}}$ proof for Γ.

Given a $\mathsf{T}_{\mu+}^{\omega}$ proof of an $\mathcal{L}_\mu$ sequent Γ, it is possible to construct a a $\mathsf{T}_\mu^{\mathsf{pre}}$ proof of Γ. Let us illustrate our approach by the following simple example. Assume we are given the following $\mathsf{T}_{\mu+}^{\omega}$ proof of $(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}$:

$$
\dfrac{
\dfrac{\dfrac{\dfrac{(\mu \mathsf{X})\Box\mathsf{X}, \top}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu^1 \mathsf{Y})\Diamond\mathsf{Y}}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\mu \mathsf{X})\Box\mathsf{X}, \top}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu^1 \mathsf{Y})\Diamond\mathsf{Y}}}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond((\nu^1 \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond((\nu^1 \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu^2 \mathsf{Y})\Diamond\mathsf{Y}}
\qquad \cdots
}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}}
$$

Starting from this proof we can construct a $\mathsf{T}_\mu^{\mathsf{pre}}$ proof as follows. We take the branch through the premise $(\nu^2\mathsf{Y})\Diamond\mathsf{Y}$ of the infinitary greatest fixed point rule. In that branch we drop all the iteration numbers. That is we replace all subexpressions of the form $(\nu^k\mathsf{X})\mathcal{C}$ by $(\nu\mathsf{X})\mathcal{C}$. This gives us the following:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\mu \mathsf{X})\Box\mathsf{X}, \top}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu^1 \mathsf{Y})\Diamond\mathsf{Y}}}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond((\nu^1 \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond((\nu^1 \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu^2 \mathsf{Y})\Diamond\mathsf{Y}}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}}
\quad\Longrightarrow\quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\mu \mathsf{X})\Box\mathsf{X}, \top}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond\top}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}}}{\Box((\mu \mathsf{X})\Box\mathsf{X}), \Diamond((\nu \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, \Diamond((\nu \mathsf{Y})\Diamond\mathsf{Y})}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}}}{(\mu \mathsf{X})\Box\mathsf{X}, (\nu \mathsf{Y})\Diamond\mathsf{Y}}
$$

Note that dropping the iteration numbers in the sequents $(\mu\mathsf{X})\Box\mathsf{X}, (\nu^2\mathsf{Y})\Diamond\mathsf{Y}$ and $(\mu\mathsf{X})\Box\mathsf{X}, (\nu^1\mathsf{Y})\Diamond\mathsf{Y}$ makes them identical. Therefore we can loop between these two sequents which results in the following infinite $\mathsf{T}_\mu^{\mathsf{pre}}$ proof:

$$\cfrac{\cfrac{\cfrac{\cfrac{\vdots}{(\mu\mathsf{X})\Box\mathsf{X}, (\nu\mathsf{Y})\Diamond\mathsf{Y}}}{\Box((\mu\mathsf{X})\Box\mathsf{X}), \Diamond((\nu\mathsf{Y})\Diamond\mathsf{Y})}}{(\mu\mathsf{X})\Box\mathsf{X}, \Diamond((\nu\mathsf{Y})\Diamond\mathsf{Y})}}{(\mu\mathsf{X})\Box\mathsf{X}, (\nu\mathsf{Y})\Diamond\mathsf{Y}}$$

In this example, we could choose the branch through the second premise of the $(\nu.\omega)$ in order to find two identical sequents. To show that this approach works in general, we have to guarantee that if we derive a greatest fixed point by a $(\nu.\omega)$ rule, then there is a branch providing two identical sequents to build a loop. We can employ a cardinality argument (using the so-called Fischer-Ladner closure which is a finite set) to show that after dropping the iteration numbers, there will be a branch with two identical sequents with the same distinguished formula. Therefore, from a given $\mathsf{T}^{\omega}_{\mu+}$ proof, we can construct the corresponding $\mathsf{T}^{\mathsf{pre}}_{\mu}$ preproof. In order to show that this preproof is a proof, it remains to show that every infinite branch of the preproof contains a ν-thread. This can be established by keeping track of how fixed points (and their approximations) are unfolded in the $\mathsf{T}^{\omega}_{\mu+}$ proof, and how this translates into the $\mathsf{T}^{\mathsf{pre}}_{\mu}$ preproof. Finally, we obtain a procedure which constructs from a $\mathsf{T}^{\omega}_{\mu+}$ proof of a formula D a $\mathsf{T}^{\mathsf{pre}}_{\mu}$ proof of D.

Theorem 63. *For all closed $\mathcal{L}_\mu$ formulae D we have*

$$\mathsf{T}^{\omega}_{\mu+} \vdash D \quad\Longrightarrow\quad \mathsf{T}^{\mathsf{pre}}_{\mu} \vdash D.$$

Dax et al. [27] provide a simple soundness proof of their system for the linear time μ-calculus. A straightforward adaptation of this proof shows the soundness of $\mathsf{T}^{\mathsf{pre}}_{\mu}$. Simply replace the case for the 'next'-rule by an appropriate treatment of $(\Box)$.

Theorem 64. *The system $\mathsf{T}^{\mathsf{pre}}_{\mu}$ is sound.*

Completeness of $\mathsf{T}^{\omega}_{\mu+}$ is established in Section 3.2.2 by a canonical counter-model construction. We immediately obtain the following corollary about soundness and completeness of $\mathsf{T}^{\omega}_{\mu+}$ and $\mathsf{T}^{\mathsf{pre}}_{\mu}$ with respect to $\mathcal{L}_\mu$ formulae.

Corollary 65. *Let A be an $\mathcal{L}_\mu$ formula. We have*

$$A \textit{ is valid} \quad\Longrightarrow\quad \mathsf{T}^{\omega}_{\mu+} \vdash A \quad\Longrightarrow\quad \mathsf{T}^{\mathsf{pre}}_{\mu} \vdash A \quad\Longrightarrow\quad A \textit{ is valid.}$$

Note that Corollary 65 provides soundness of $\mathsf{T}^{\omega}_{\mu+}$ without referring to the finite model property of the modal μ-calculus. This is interesting insofar as one usually makes use of the finite model property to show that it suffices to consider only the finite approximations as premises in the ω-rule. That means the finite model property is used to show that the ω-rule preserves validity and hence the system with the ω-rule is sound. Now we have a soundness proof which does not use the finite model property.

We can even employ Corollary 65 to obtain the finite model property of the modal μ-calculus. Looking closely at the construction of the $\mathsf{T}_\mu^{\mathsf{pre}}$ preproof, we notice that it is enough to consider finitely many premises of the ω-rule. Therefore we obtain soundness for a system with a finitized version of the ω-rule. Then we can adapt the canonical counter model construction of Section 3.2.2 such that it constructs a finite counter model. This results in a proof-theoretic proof of the finite model property of the modal μ-calculus. However, the best we get from such a construction is a double exponential bound for the size of the model (compare with the exponential bound provided by [31]).

Chapter 4

Conclusion

We have investigated deductive systems for the logic of common knowledge and the modal μ-calculus. Venema writes in [83] that *the completeness theory for the μ-calculus is a largely undeveloped field.* We think that our work contributes to the development of this field. For example, we could provide a completeness proof for the modal μ-calculus which is based on a canonical counter model construction. That means we only use classical methods from modal logic. Moreover, we could clarify on a syntactic level the proof-theoretic relationship between the ω-rule and global induction by giving a syntactic embedding of a system with an ω-rule into a system based on global induction. Together with the above mentioned counter model construction this gives a new proof of the finite model property for the μ-calculus.

Deduction chains are another classical method to establish completeness of a deductive system. The constructive nature of this method elucidates the underlying proof-theoretic principles of the system under consideration. We have extended the method of deduction chains such that it can be applied to the logic of common knowledge. Among other things this approach has revealed that applying rules deep inside formulae is an inherent concept of infinitary sequent calculi for modal fixed point logic.

A further issue is the development of deductive systems for modal fixed point logics that have 'nice' proof-theoretic properties. Of course, there cannot be a rigorous definition of what a 'nice' system is. However there is a consens that such a system should allow for syntactic proofs for the admissibility of weakening, contraction, and inverse rules as well as for a syntactic cut-elimination procedure. Making use of deep inference, we were able to provide an infinitary system for common knowledge that has all the desired properties. Moreover, we could establish $\varphi_2 0$ as an upper bound on the depth of cut-free proofs. Recently, we extended our techniques such that we are able to provide a 'nice' infinitary system for the modal μ-calculus. We obtain $\varphi_\omega 0$ as an upper bound on the depth of cut-free proof in that system. Details will be given in a publication under preparation.

These results give rise to some questions: What is the mathematical meaning of the upper bound on the depth of cut-free proofs in the context of modal fixed point logics? 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? Are the bounds mentioned above the best possible upper bounds on the depth of cut-free proofs? What would be the equivalent of a wellordering proof in modal logic?

The big question that remains is whether there are 'nice' *finitary* deductive systems for modal fixed point logics. We have shown that it is possible to finitize our systems. That means we do not need all of the infinitely many premises of the ω-rule. It is enough to consider only finitely many of them in order to guarantee that the rule preserves validity. As we have seen, this fact is strongly related to the finite model property of the respective logic. Unfortunately, by doing this modification of the ω-rule, one loses all the 'nice' properties of the infinitary systems. In fact, no 'nice' deductive system for common knowledge is available so far.

We have provided a proof that the logic of common knowledge does not have the Beth property and that it also lacks interpolation. This failure of interpolation can be seen as an explanation why it is so difficult to find 'nice' deductive systems for common knowledge. Often the existence of a cut-free system for a logic implies an interpolation property for that logic, see any introduction to proof theory, for example [23, 36, 82]. However, if interpolation is a consequence of cut-elimination, then by contraposition we obtain that the failure of interpolation 'implies' the non-existence of a 'nice' cut-free system.

A set of agents may acquire common knowledge of a proposition A if there is a public announcement of A. We have presented a system for public announcements (and common knowledge) in which announcements are total. That means announcements need not be truthful in our system. This is of particular importance if not only the agents' knowledge but also their beliefs are considered. See Steiner's forthcoming PhD thesis [75] for a detailed treatment of this topic.

Bibliography

[1] 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*.

[2] L. Alberucci. *The modal mu-calculus and the logic of common knowledge.* PhD thesis, Universität Bern, Institut für Informatik und angewandte Mathematik, 2002.

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

[4] J. Aldwinckle and R. Cockett. The proof theory of modal μ logics. In *Proc. Fixed Points in Computer Science*, 2001.

[5] 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.

[6] S. Artemov. Logic of proofs. *Annals of Pure and Applied Logic*, 67(1-3):29–59, 1994.

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

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

[9] J. W. de Bakker and W. P. de Roever. A calculus for recursive program schemes. In *ICALP*, pages 167–196, 1972.

[10] J. W. de Bakker and D. Scott. A theory of programs, 1969. Unpublished notes.

[11] A. Baltag and L. S. Moss. Logics for epistemic programs. *Synthese*, 139(2):165–224, 2004.

[12] A. Baltag, L. S. Moss, and S. Solecki. The logic of public announcements, common knowledge, and private suspicions. In *Proc. of TARK '98*, pages 43–56. Morgan Kaufmann, 1998.

[13] 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.

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

[15] J. van Benthem, J. van Eijck, and B. Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, 2006.

[16] J. van Benthem and D. Ikegami. Modal fixed-point logic and changing models. In A. Avron, N. Dershowitz, and A. Rabinovich, editors, *Pillars of Computer Science*, pages 146–165. Springer, 2008.

[17] P. Blackburn, J. van Benthem, and F. Wolter. *Handbook of Modal Logic*. Elsevier, 2006.

[18] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*, volume 53 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2002.

[19] J. Brotherston. *Sequent Calculus Proof Systems for Inductive Definitions*. PhD thesis, University of Edinburgh, 2006.

[20] 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.

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

[22] K. Brünnler and T. Studer. Syntactic cut-elimination for common knowledge. *Annals of Pure and Applied Logic*, to appear. Available at `http://www.sciencedirect.com/science/article/B6TYB-4VK68YM-1/2/1de3977dfb2af94903bbc3451fd7071c`. DOI: 10.1016/j.apal.2009.01.014.

[23] S. R. Buss. An introduction to proof theory. In S. R. Buss, editor, *Handbook of Proof Theory*, pages 1–78. Elsevier, 1998.

[24] A. Chagrov and M. Zakharyaschev. *Modal Logic*. Oxford Science Publications, 1997.

[25] E. M. Clarke and E. A. Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In *Logic of Programs, Workshop*, pages 52–71, 1982.

[26] W. Craig. Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory. *Journal of Symbolic Logic*, 22(3):269–285, 1957.

[27] 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.

[28] H. van Ditmarsch. The russian cards problem. *Studia Logica*, 75(4):31–62, 2003.

[29] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic epistemic logic*. Springer, 2007.

[30] H. van Ditmarsch and B. Kooi. The secret of my success. *Synthese*, 151(2):202–232, 2005.

[31] E. A. Emerson and C. S. Jutla. The complexity of tree automata and logics of programs (extended abstract). In *29th Annual Symposium on Foundations of Computer Science FOCS*, pages 328–337. IEEE, 1988.

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

[33] S. Feferman. Introductory note to 1931c. In *Kurt Gödel: Collected works, vol. I*, pages 208–213. Oxford University Press, 1986.

[34] M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Science*, 18(2):194–211, 1979.

[35] D. M. Gabbay and L. Maksimova. *Interpolation and Definability in Modal Logics*. Clarendon Press, 2005.

[36] J.-Y. Girard. *Proof Theory and Logical Complexity.* Bibliopolis, 1987.

[37] A. Guglielmi. A system of interaction and structure. *ACM Transactions on Computational Logic*, 8(1), 2007.

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

[39] M. Hennessy and R. Milner. On observing nondeterminism and concurrency. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 299–309, 1980.

[40] D. Hilbert. Die Grundlegung der elementaren Zahlenlehre. *Mathematische Annalen*, 104:485–494, 1931.

[41] G. Jäger, M. Kretz, and T. Studer. Cut-free axiomatizations for stratified modal fixed point logic. In H. Schlingloff, editor, *Proceedings of the 4th Workshop Methods for Modalities*, pages 125–143. 2005.

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

[43] G. Jäger, M. Kretz, and T. Studer. Canonical completeness for infinitary μ. *Journal of Logic and Algebraic Programming*, 76(2):270–292, 2008.

[44] G. Jäger and T. Strahm. Bar induction and omega model reflection. *Annals of Pure and Applied Logic*, 97(1-3):221–230, 1999.

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

[46] D. Kozen. Results on the propositional modal μ–calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[47] D. Kozen. A finite model theorem for the propositional μ–calculus. *Studia Logica*, 47(3):233–241, 1988.

[48] M. Kracht. *Tools and Techniques in Modal Logic.* Elsevier, 1999.

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

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

[51] 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.

[52] C. Lewis. *Survey of Symbolic Logic*. 1918.

[53] D. Lewis. *Convention: A Philosophical Study*. 1969.

[54] L. Maksimova. Temporal logics of “the next” do not have the Beth property. *Journal of Applied Non-Classical Logics*, 1(1):73–76, 1991.

[55] L. Maksimova. Temporal logics with “the next” operator do not have interpolation or the Beth property. *Siberian Mathematical Journal*, 32(6):989–993, 1991.

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

[57] S. Negri. Proof analysis in modal logic. *Journal of Philosophical Logic*, 34:507–544, 2005.

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

[59] D. Park. Fixpoint induction and proofs of program properties. In Meltzer and D. Michie, editors, *Machine Intelligance*, volume 5, pages 59–78. Edinburgh University Press, 1969.

[60] J. A. Plaza. Logics of public communications. In M. Emrich, M. Pfeifer, M. Hadzikadic, and Z. Ras, editors, *Proc. of Methodologies for Intelligent Systems*, pages 201–216, 1989.

[61] R. Pliuskevicius. Investigation of finitary calculus for a discrete linear time logic by means of infinitary calculus. In *Baltic Computer Science, Selected Papers*, pages 504–528. Springer, 1991.

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

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

[64] V. R. Pratt. Semantical considerations on Floyd-Hoare logic. In *IEEE Symposium on Foundations of Computer Science*, pages 109–121, 1976.

[65] B. Renne. Bisimulation and public announcements in logics of evidence-based knowledge. In S. Artemov and R. Parikh, editors, *ESSLLI '06: Rationality and Knowledge*, pages 112–123. Association for Logic, Language and Information, 2006.

[66] L. Santocanale. A calculus of circular proofs and its categorical semantics. In *FoSSaCS '02: Proceedings of the 5th International Conference on Foundations of Software Science and Computation Structures*, pages 357–371. Springer, 2002.

[67] T. Schelling. *The Strategy of Conflict*. 1960.

[68] S. Schiffer. *Meaning*. 1972.

[69] K. Schütte. Schlussweisen-Kalküle der Prädikatenlogik. *Mathematische Annalen*, 122:47–65, 1950.

[70] K. Schütte. *Beweistheorie*. Springer, 1960.

[71] K. Schütte. *Vollständige Systeme modaler und intuitionistischer Logik*. Springer, 1968.

[72] K. Schütte. *Proof Theory*. Springer, 1977.

[73] H. Schwichtenberg. Proof theory: Some applications of cut-elimination. In J. Barwise, editor, *Handbook of Mathematical Logic*, pages 867–895. North-Holland, 1977.

[74] C. Sprenger and M. Dam. On the structure of inductive reasoning: Circular and tree-shaped proofs in the mu-calculus. In *Proc. FOSSACS'03*, Springer LNCS, pages 425–440, 2003.

[75] D. Steiner. *Belief Change Functions for Multi-agent Systems*. PhD thesis, University of Bern. In preparation.

[76] D. Steiner and T. Studer. Total public announcements. In S. N. Artemov and A. Nerode, editors, *Logical Foundations of Computer Science, LFCS 2007*, volume 4514 of *LNCS*, pages 498–511. Springer, 2007.

[77] C. Stewart and P. Stouppa. A systematic proof theory for several modal logics. In R. A. Schmidt, I. Pratt-Hartmann, M. Reynolds, and H. Wansing, editors, *Advances in Modal Logic 5*, pages 309–333. King's College Publications, 2004.

[78] T. Studer. On the proof theory of the modal mu-calculus. *Studia Logica*, 89:343–363, 2008.

[79] T. Studer. Common knowledge does not have the Beth property. *Information Processing Letters*, to appear. Available at http://www.iam.unibe.ch/~tstuder/papers/ckint.pdf. DOI: 10.1016/j.ipl.2009.02.011.

[80] W. Tait. Normal derivability in classical logic. In J. Barwise, editor, *The Syntax and Semantics of Infinitary Languages*, pages 204–236. Springer, Berlin, 1968.

[81] Y. Tanaka. Some proof systems for common knowledge predicate. *Reports on Mathematical Logic*, 37:79–100, 2003.

[82] A. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge, 1996.

[83] Y. Venema. Lectures on the modal μ-calculus, 2008. Available at: http://staff.science.uva.nl/~yde/teaching/ml/mu/mu.pdf.

[84] I. Walukiewicz. A complete deductive system for the μ–calculus. In *Proceedings of the Eighth Annual IEEE Symposium on Logic in Computer Science*, pages 136–147. IEEE Computer Science Press, 1993.

[85] I. Walukiewicz. Completeness of Kozen's axiomatization of the propositional μ–calculus. *Information and Computation*, 157:142–182, 2000.

[86] H. Wansing. Sequent systems for modal logics. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, volume 8, pages 61–145. Kluwer, 2002.

[87] R. Wehbe. A cut-free axiomatization for relativized common knowledge. In *Logic Colloquim 2008: Booklet of Abstracts*, pages 55–56. University of Bern, 2008.