INTERPOLATION IN MODAL LOGICS

By

Marta Bílková

Supervised by

Pavel Pudlák

PH.D. THESIS

DEPARTMENT OF LOGIC, FACULTY OF PHILOSOPHY AND ARTS

CHARLES UNIVERSITY PRAGUE, CZECH REPUBLIC

2006

INTERPOLACE V MODÁLNÍCH LOGIKÁCH

Marta Bílková

Školitel
RNDr. Pavel Pudlák , DrSc.

Studijní program Logika, studijní obor Logika

PH.D. DISERTACE
KATEDRA LOGIKY, FILOZOFICKÁ FAKULTA
UNIVERZITA KARLOVA V PRAZE
2006

Prohlašuji, že jsem disertační práci vypracovala samostatně s využitím uvedených pramenů a literatury.

To Albert and Dick

and to Hanneke

Contents

Introduction **1**

1 Preliminaries **6**

1.0.1 Notation 6

1.0.2 Normal modal logics 7

1.0.3 Kripke semantics 9

1.0.4 Arithmetical interpretation 11

2 Modal sequent proof systems **12**

2.1 Classical sequent calculus G 13

2.2 Sequent calculi for logics K and T 15

2.2.1 Termination 15

2.2.2 Structural rules 19

2.3 Sequent calculi for logics having arithmetical interpretations 26

2.3.1 Termination 27

2.3.2 Structural rules 31

3 Uniform Interpolation **36**

3.1 Logic K4 39

3.2 Logic K 40

3.2.1 Propositional quantifiers 45

3.2.2 Uniform interpolation 47

3.3 Logic T 48
3.4 Gödel-Löb's Logic GL 53
3.4.1 Fixed points 60
3.5 Grzegorczyk's Logic S4Grz 62
3.6 Concluding remarks 74

4 Feasible interpolation **76**
4.1 Sequent calculi 78
4.2 Disjunction property 80
4.2.1 The closure 81
4.2.2 Cut elimination 82
4.2.3 Feasible Disjunction Property 86
4.2.4 Harrop hypotheses 87
4.3 Feasible interpolation 90
4.3.1 Complexity consequences 92
4.3.2 Concluding remarks 93

Bibliography **95**

Acknowledgements There are two people I would like to thank above all for introducing me into scientific practice: First of all, I am grateful to my supervisor Pavel Pudlák for his kind encouragement, patience, and the time he spent working with me. I am grateful to Vítek Švejdar who initiated me into logic during my undergraduate studies.

There are many others I would like to mention - in no particular order - my colleagues and friends who supported me to finish the thesis: Emil Jeřábek for fruitful discussions about modal logics, Nick Bezhanishvilli for drawing my attention to Pitts' work, Albert Visser and Dick de Jongh for discussions on the topic, Joost Joosten, Hanneke and Geert Vink, Michal Peliš, Petr Cintula, Libor Běhounek, Rosťa Horčík. Very special thanks go to Ondrej Majer.

Last, but not least, I thank my family, for all the good things that make life meaningful.

Introduction

Since Craig's landmark result on interpolation for classical predicate logic, proved as the main technical lemma in [14], interpolation is considered one of the central concepts in pure logic. Various interpolation properties find their applications in computer science and have many deep purely logical consequences.

We focus on two propositional versions of Craig interpolation property:

Craig Interpolation Property: for every provable implication $(A \to B)$ there is an interpolant I containing only only common variables of A and B such that both implications $(A \to I)$ and $(I \to B)$ are provable.

Craig interpolation, although it seems rather technical, is a deep logical property. It is closely related to expressive power of a logic - as such it entails Beth's definability property, or forces functional completeness. It is also related to Robinson's joint consistency of two theories that agree on the common language. Craig interpolation has an important algebraic counterpart - it entails amalgamation or superamalgamation property of appropriate algebraic structures. In case of modal provability logics, Craig interpolation entails fixed point theorem.

There are other interpolation properties, defined w.r.t. a consequence relation rather then w.r.t. a provable implication. In presence of deduction theorem the two possibilities coincide. However, in modal logics, we have at least two possible consequence relations - local and global - and also two such interpolation properties [28]. In this case, thanks the deduction theorem for the local consequence relation, the Craig interpolation coincides with the local interpolation and entails the global interpolation, but not other way round.

A stronger version of Craig interpolation property arises in relation with quantifier elimination:

Uniform Interpolation Property: for every formula A and any choice of propositional variables $\bar{q}$, there is a post-interpolant $I_{postA}(\bar{q})$ depending only on A and $\bar{q}$ such that for all provable implications $(A \to B)$, where the shared variables of A and B are among $\bar{q}$, $(A \to I_{postA}(\bar{q}))$ and $(I_{postA}(\bar{q}) \to B)$ are provable. Similarly there is a pre-interpolant: for every formula B and any choice of propositional variables $\bar{r}$

there is a formula $I_{preB}(\bar{r})$ depending only on B and $\bar{r}$ such that for all provable implications $(A \to B)$ where the shared variables of A and B are among $\bar{r}$, $(I_{preB}(\bar{r}) \to B)$ and $(A \to I_{preB}(\bar{r}))$ are provable.

Uniform interpolation as connected to a quantifier elimination is used in computer science in slicing programs.

The presence of the (uniform) interpolation property has a proof-theoretic significance since it is closely related to the existence of analytic properties of a proof system: Suppose that the rule

$$\frac{A \to B \qquad B \to C}{A \to C}$$

is admissible in the proof system. Then interpolation property implies that looking for a proof of $A \to C$ it suffices to look for proofs of $A \to B$ and $B \to C$ where only variables occurring already in A and C respectively occur.

This reflects in such computer science applications as theorem proving, simplifications of database queries, or SAT based model checking.

We would like to stress that to have an interpolation property is significant for a logic. The fact that most of widely used logics satisfy interpolation properties does not mean that most of logics have interpolation, it is rather other way round - we usually deal with logics having interpolation. (For example, there is continuum of logics over provability logic **GL** having Craig interpolation, and there is also continuum of logics over **GL** without Craig interpolation [13].) The matter here is not so much if a logic has an interpolation, but rather where the logic interpolates (in which schematic extension or in which extension of the language).

A lot information of various interpolation and related properties in modal logic can be found in Maksimova's work [34], [35], and in Maksimova's and Gabbay's book [17].

The aim of the thesis is to study interpolation properties of propositional modal logics from a proof-theoretic point of view. We concentrate on the stronger from the two interpolation properties in the first part of our thesis.

Uniform Interpolation. As usual in the case of modal logics, semantic methods are better developed and preferred proving important characterizations of a logic which is also the case of uniform interpolation. Semantic proofs are often considered to offer better insight into a problem while proof-theoretic proofs are useful thanks their constructiveness. We do not quite share this opinion and find proof-theoretic proofs valuable as providing deep understanding as well, alternative but not very far from the semantic one. However, constructiveness is one of our main motivation to extend study of uniform interpolation by proof-theoretic methods.

Since uniform interpolants can be easily expressed using propositional quantifiers, i.e., quantifiers ranging over propositional variables, the phenomenon of the existence of uniform interpolants can be viewed as the possibility of a simulation, or equivalently an elimination, of certain propositional quantifiers. A semantic proof of uniform interpolation based on such a simulation of propositional quantifiers was given by Visser in [52] for modal logics **K**, Gödel-Löb's logic of provability **GL** and Grzegorczyk's logic **S4Grz**. (For **GL**, uniform interpolation was first proved by Shavrukov in [47].) Visser's semantic proof uses a model theoretic argument based on bisimulations on Kripke models. The proof yields a semantic meaning of uniform interpolants and information about their type - a complexity bound in terms of $\Box$-depth. However, the proof does not provide us with a construction of the interpolants. A similar semantic argument should also work for modal logic **T** but it is not given in Visser's paper. A proof of uniform interpolation for **K**, based on a semantic argument, can be found also in Kracht's book [28].

We concentrate on a proof-theoretic method introduced by Pitts in [39] where he proved that intuitionistic propositional logic satisfies uniform interpolation. In this case, a semantic argument using bisimulations on Kripke models was given later by Ghilardi and Zawadowski in [19], and independently by Visser in [52]. The Pitts' argument uses a simulation of propositional quantifiers in the framework of an analytic sequent proof system. The main point of keeping the information "to be the uniform interpolant" finite and thus represented by a single formula is in a use of a terminating sequent proof system, i.e., a proof system in which any backward proof-search terminates.

As Craig interpolation relates to cut-free proofs, uniform interpolation relates to terminating proof-search trees. Proving Craig interpolation, we start with a cut-free (or nortmalized) proof of an implication and construct an interpolant inductively from the proof. Proving uniform interpolation, we start with a kind of proof-search tree for a formula (we search for all proofs in which the formula can occur in the appropriate context) and a uniform interpolant is then the formula corresponding to such a tree.

Here our study closely relates to decision procedures and proof-search related area.

So far such a proof-theoretic proof of uniform interpolation has been given by the author for modal logics **K** and **T** in [3]. In this thesis we extend the method to logics having arithmetical interpretation - Gödel-Löb's logic of provability **GL** and Grzegorczyk's logic **S4Grz**. The main advantage of the proof-theoretic method we use is that it provides an explicit effective and also easily implementable construction of uniform interpolants. An interesting part of the proof consists in an application of terminating analytic sequent calculi for modal logics, namely in the case of logics having arithmetical interpretation which are usually not considered in this context.

The second part of the thesis is devoted to a version of the Craig's interpolation theorem considered in connection with proof complexity - so called feasible, or effective interpolation.

Feasible interpolation. The complexity of propositional proofs, especially lower bounds on their size, are of main interest in proof complexity: proving that in no proof system the lengths of proofs can be polynomially bounded would prove that $NP \neq coNP$. Various classical propositional proof systems have been concerned, including versions of sequent calculus, resolution refutations, Frege systems etc. Recently the study extends to various nonclassical propositional logics.

Proving lower bounds on size of proofs, a version of the Craig's interpolation theorem, so called feasible interpolation, is concerned. It enables to extract, from a proof of an implication, a boolean interpolation circuit whose size is polynomial in the size of the proof. If the extracted circuit is monotone, we talk about monotone feasible interpolation which turns out to be a strong property of a proof system from the complexity point of view.

Krajíček [29] proposed a method of proving lower bounds using feasible interpolation: suppose we are able to show that some implication does not have a simple interpolant, than, providing feasible interpolation holds, it cannot have a simple proof.

Methods how to obtain concrete examples of hard tautologies for a proof system satisfying feasible interpolation were proposed by Razborov in [42], and by Bonet, Pittasi, and Raz in [7]. For the case of monotone feasible interpolation it immediately yields lower bounds for a proof system, while in general case we have to use some, usually modest, complexity assumptions (like that there exist pseudorandom generators or that factoring is hard to compute).

Feasible interpolation was already proved for several classical proof systems by Krajíček [30], Pudlák [40], and for intuitionistic sequent calculus by Buss and Pudlák in [12], or by Goerdt in [22]. Monotone feasible interpolation was used to prove lower bounds e.g. for Resolution ([40],[6]), Cutting Planes ([40],[6]) or Hilbert's Nullstellensatz proof systems ([10],[2]).

The approach of [11] and [12], where intuitionistic propositional logic is considered, is to derive feasible interpolation from feasible disjunction property which is proved using a natural deduction calculus and a sequent calculus respectively.

Feasible interpolation for modal logic **S4**, which is naturaly related to intuitionistic logic, has been considered using this method by the author in [4], and by Ferrari, Fiorentini, and Fiorino in [15] where feasible disjunction property is proved for various modal logics using a different method, while feasible interpolation is derived only for **S4** using a straightforward translation of the appropriate part of the intuitionistic case.

In this part of the thesis we follow the method of [12] and simplify the proof used in [4] to obtain feasible interpolation theorem through feasible disjunction property for several modal propositional logics. Our motivation is to make clear how easily the method proposed in [12] works in case of modal logics and that it is indeed more general then the intuitionistic case, rather then use a blind translation of the more complicated intuitionistic case to particular modal logics.

As a consequence we obtain, under some complexity assumption, the existence of hard modal tautologies. A speed-up between classical proofs and proofs in modal systems can be obtained as a corollary of appropriate feasible interpolation theorems, assuming e.g. that factoring is hard [12], [7].

In very recent work of Hrubeš [26] it has been shown that modal logics **K**, **K4**, **S4**, **GL** satisfy even monotone feasible interpolation theorem and concrete examples of hard tautologies has been presented.

Overview of the thesis

The thesis is organized as follows:

- Chapter 1 **Preliminaries**: we fix notation and briefly sketch basic facts about normal modal logics - an axiomatization, Kripke semantics and arithmetical interpretation.

- Chapter 2 **Modal sequent proof systems**: introduces cut free sequent calculi that are used in the following chapter to prove uniform interpolation and their structural properties are proved. Since our method of proving uniform interpolation is closed to decision procedures and since termination of the calculi is one of its main ingredients, we also discuss proof-search and its termination in modal logics. Some of the calculi contain loop-preventing mechanisms.

- Chapter 3 **Uniform Interpolation**: we prove uniform interpolation theorem for modal logics **K**, **T**, **GL**, and **S4Grz**. The proof consists in a construction of a formula simulating propositional universal quantification. It entails uniform interpolation via an interpretation of a second order modal logic in its propositional counterpart. However, the construction itself can bee seen constructing an interpolant directly.

- Chapter 4 **Feasible Interpolation**: we prove feasible interpolation for modal propositional logics **K**, **K4**, **K4Grz**, **GL**, **T**, **S4**, and **S4Grz** via feasible disjunction property. For this chapter, we define different sequent proof systems with the cut rule, uniformly for all the logics. We derive complexity consequences - the existence of hard modal tautologies (under some modest complexity assumptions).

Chapter 1

Preliminaries

1.0.1 Notation

We shall consider propositional modal logics and quantified propositional modal logics. We follow literature in referring to quantified propositional modal logics as to second order propositional modal logics.

The letters $A, B, \ldots$ range over formulas, the letters $p, q, \ldots$ range over propositional variables, Greek letters $\Gamma, \Delta, \ldots$ range over finite multisets of formulas (in Chapters 2,3) or finite sets of formulas (in Chapter 4). It will be clear form context whether we speak about sets or multisets. We write Γ, Δ for the multiset union of Γ and Δ (the set union resp.). Membership relation sign $\in$ relates to sets as well as to multisets according to its context. $\{A|\varphi(A)\}$ denotes the multiset (set) of formulas satisfying the property φ.

For a multiset Γ, Γ° denotes the corresponding set.

$\Box\Gamma$ denotes the multiset (set) $\{\Box A|A \in \Gamma\}$. $\Gamma^{\Box}$ denotes the multiset (set) $\{A|\Box A \in \Gamma\}$.

$\Gamma\backslash A$ denotes the set $\Gamma - \{A\}$; $\Gamma\backslash A, B$ denotes the set $\Gamma - \{A, B\}$

We use the following propositional second order modal language and definition of formulas:

$$A := p|\Box A|A \wedge B|\neg A|\forall pA$$

Logical connectives $\vee, \rightarrow, \leftrightarrow$ and the constants $\top, \bot$ are defined as usual and $\exists pA \equiv_{df} \neg\forall p\neg A$, $\Diamond A \equiv_{df} \neg\Box\neg A$. We freely use the full language in the text.

We denote the set of propositional variables by Var and the set of all modal formulas Fla.

Writing $A(\bar{p}, \bar{q})$ we mean that *all* propositional variables of A are among $\bar{p}, \bar{q}$. $Var(\Gamma)$ stays for the set of all variables free in the multiset (set) Γ.

A notation of the form $\Gamma \Rightarrow \Delta$ or $\Sigma|\Gamma \Rightarrow \Delta$ is a sequent. To keep readability, we often enclose sequents in the text with brackets (). Γ is called the antecedent and Δ is called the succedent of the sequent $\Gamma \Rightarrow \Delta$.

We use the sign $\vdash_C$ for provability in the calculus C. We write $S_1; \ldots; S_n \vdash_C S$ for a fact that a sequent S is provable in calculus C from sequents $S_1 \ldots S_n$ as assumptions. Writing $\vdash_C \Gamma \Leftrightarrow \Delta$ we mean that both $\vdash_C \Gamma \Rightarrow \Delta$ and $\vdash_C \Delta \Rightarrow \Gamma$.

The *weight* $w(A)$ of a modal formula A is defined as follows:

- $w(p) = w(\bot) = 1$
- $w(B \circ C) = w(B) + w(C) + 1$
- $w(\neg B) = w(\Box B) = w(B) + 1$

The weight $w(\Gamma)$ of a multiset Γ is the sum of weights of the formula occurrences from Γ, the weight of a sequent is the sum of the weight of its antecedent and the weight of its succedent.

Quantifiers bind propositional variables; we adopt the usual definition of the scope, free, and bounded variables.

1.0.2 Normal modal logics

We focus on so called normal modal logics which extend classical propositional logic and at least contain a schema expressing that the $\Box$ modality distributes over implication. From a semantic point of view, this is a class of logic with natural frame semantics.

We just briefly list some basic facts about logics we deal with in the thesis. More on modal logics in general, as well as all missing details and proofs can be found in books [5], [13], [8].

In what follows, we treat axioms and rules as schemata. A usual definition of normal modal logic is the following one identifying logic with the set of its tautologies:

Definition 1.0.1. *Normal modal logic* is any set of modal formulas that

- contains (all instances of) classical propositional tautologies
- contains (all instances of) the schema K: $\Box(A \to B) \to (\Box A \to \Box B)$
- is closed under the rules Modus Ponens and the Necessitation rule: $A/\Box A$.

We understand normal modal logics rather as extensions of classical propositional logic in modal language with axiom schemata and the Necessitation rule. Given a Hilbert style axiomatization H of classical propositional logic, we consider following normal modal logics:

- the minimal propositional normal modal logic **K** with its Hilbert style axiomatization H_K which results from adding the schema K and the Necessitation rule to H.

- logic **T** with its Hilbert style axiomatization H_T which results from adding the reflexivity schema T: $\Box A \to A$ to H_K

- logic **K4** with its Hilbert style axiomatization H_{K4} which results from adding the schema 4: $\Box A \to \Box\Box A$ to H_K

- logic **S4** with its Hilbert style axiomatization H_{S4} which results from adding the schema T to H_{K4}

- Gödel-Löb's logic **GL** with its Hilbert style axiomatization H_{GL} which results from adding the Löb's axiom L:

$$\Box(\Box A \to A) \to \Box A$$

  to H_K or equivalently to H_{K4}

- Grzegorczyk's logic **K4Grz** with its Hilbert style axiomatization H_{K4Grz} which results from adding the the Grzegorczyk's axiom Grz:

$$\Box(\Box(A \to \Box A) \to A) \to \Box A$$

  to H_K or equivalently to H_{K4}

- Grzegorczyk's logic **S4Grz** with its Hilbert style axiomatization H_{S4Grz} which results from adding the Grzegorczyk's axiom Grz to H_T or equivalently to H_{S4}

A proof in a modal Hilbert calculus is defined as usual and a proof from assumptions is defined in two different ways as follows:

Definition 1.0.2. $\Gamma \vdash^g_{H_L} A$ iff there is a finite sequence of formulas each of them is either an axiom or an assumption from Γ, or a result of an application of the rule MP to some two preceeding formulas, or a result of an application of the rule Nec to some preceeding formula; and the last formula in the sequence is A.
$\Gamma \vdash^l_{H_L} A$ iff there is a finite $\Gamma' \subseteq \Gamma$ such that $\vdash_{H_L} \bigwedge \Gamma' \to A$.

Note that ($A \vdash^{g}_{H_L} \Box A$) and therefore we do not have the usual deduction theorem for this definition of proof from assumptions. For $\vdash^{l}_{H_L}$ deduction theorem follows immediately from the definition.

The letters g, l in superscripts refer to "global" and "local". This is motivated by corresponding relations of semantic consequence (definition of which see below). The local provability can be alternatively defined as follows: $\Gamma \vdash^{l}_{H_L} A$ iff there is a proof of A from Γ where the Necessitation rule is not used once an assumption from Γ is used, i.e., we allow to necessitate only theorems.

It is the local provability which corresponds to Gentzen style formalization of modal logics.

1.0.3 Kripke semantics

Kripke semantics is based on relational structures called Kripke frames consisting on an nonempty set (usually called a set of possible worlds) together with a binary relation on the set which is called the accessibility relation. Possible worlds can be seen as classical valuations, modal formulas are evaluated in a possible world relatively to the accessible worlds: a formula $\Box A$ holds in a possible world whenever A holds in all accessible worlds. Precisely:

Definition 1.0.3. A *frame* $\mathcal{F}$ is a pair (W, R) where W is a nonempty set and $R \subseteq W \times W$ is a binary relation on W.
A *model* $\mathcal{M}$ is a triple (W, R, V) where (W, R) is a frame and $V : Var \mapsto \mathcal{P}(W)$ is a valuation function mapping propositional variables to subsets of W.

A valuation function V generates a relation $\Vdash_V \subseteq W \times Fla$ of validity of a formula in a world as follows:

- $w \Vdash_V p$ iff $w \in V(p)$
- $w \Vdash_V A \wedge B$ iff $w \Vdash_V A$ and $w \Vdash_V B$
- $w \Vdash_V \neg A$ iff $w \nVdash_V A$
- $w \Vdash_V \Box A$ iff for all w', wRw' implies $w' \Vdash_V A$

A formula A holds in a model $\mathcal{M} = (W, R, V)$, notation $\models_{\mathcal{M}} A$, iff for all $w \in W$ $w \Vdash_V A$.
A formula A holds in a frame $\mathcal{F}$, notation $\models_{\mathcal{F}} A$, iff it holds in every model based on $\mathcal{F}$.
A formula A holds in a class of frames $\mathfrak{F}$, notation $\models_{\mathfrak{F}} A$, iff for any frame $\mathcal{F} \in \mathfrak{F}$, $\models_{\mathcal{F}} A$.

A formula A is a *local semantic consequence* of Γ w.r.t. a class of frames $\mathfrak{F}$, notation $\Gamma \models^l_{\mathfrak{F}} A$, iff for any model $\mathcal{M} = (W, R, V)$ based on a frame from $\mathfrak{F}$, and any world $w \in W$, if for all $C \in \Gamma$ $w \Vdash_V C$ then $w \Vdash_V A$.
A formula A is a *global semantic consequence* of Γ w.r.t. a class of frames $\mathfrak{F}$, notation $\Gamma \models^g_{\mathfrak{F}} A$, iff for any model $\mathcal{M}$ based on a frame from $\mathfrak{F}$, if for all $C \in \Gamma$ $\mathcal{M} \models C$ then $\mathcal{M} \models A$.

We say that a calculus H_L is *complete* w.r.t. a class of frames $\mathfrak{F}$ iff

$$\vdash_{H_L} A \quad \text{iff} \quad \models_{\mathfrak{F}} A.$$

We say that a calculus H_L is *strongly complete* w.r.t. a class of frames $\mathfrak{F}$ iff

$$\Gamma \vdash^l_{H_L} A \quad \text{iff} \quad \Gamma \models^l_{\mathfrak{F}} A.$$

The following completeness theorems hold:

- The calculus H_K is strongly complete w.r.t. the class of all Kripke frames.
- The calculus H_T is strongly complete w.r.t. the class of reflexive Kripke frames.
- The calculus H_{K4} is strongly complete w.r.t. the class of transitive Kripke frames.
- The calculus H_{S4} strongly complete w.r.t. the class of reflexive and transitive Kripke frames. It is also complete w.r.t. the class of partially ordered frames.
- The calculus H_{GL} is complete w.r.t. the class of transitive and converse well-founded Kripke frames. It is also complete w.r.t. finite irreflexive trees.
- The calculus H_{K4Grz} is complete w.r.t. the class of transitive and converse well-founded Kripke frames.
- The calculus H_{S4Grz} is complete w.r.t. the class of transitive, reflexive and converse well-founded Kripke frames. It is also complete w.r.t. finite partially ordered trees.

We define the following translation $A^\star$ of modal formulas (to interpret reflexivity): $\star$ does nothing with propositional variables, it commutes with logical connectives, and $(\Box A)^\star = \Box A \wedge A$. Then the following holds:

$$\vdash_{H_{S4}} A \quad \text{iff} \quad \vdash_{H_{K4}} A^\star,$$

$$\vdash_{H_{S4Grz}} A \quad \text{iff} \quad \vdash_{H_{GL}} A^\star.$$

1.0.4 Arithmetical interpretation

There is a possibility to interpret the $\Box$ modality as formalized provability in an arithmetical theory. For Gödel-Löb's logic **GL** this yields a natural provability interpretation. The main reference is Boolos' book [8], for a history of provability logic see also [45].

Fix an arithmetical recursively axiomatizable theory T with its axiomatization expressed by a sentence τ. Consider a standard proof predicate $Pr_\tau(\bar{\varphi})$ for T. We define an arithmetical evaluation of modal formulas to be a function from propositional variables to arithmetical sentences such that it commutes with logical connectives, and $e(\bot) = (0 = S(0))$, and $e(\Box A) = Pr_\tau(\overline{e(A)})$.

We say that modal logic L is *arithmetical complete* w.r.t. an arithmetical theory T (or it is the logic of provability of T) if

$$\forall e(\vdash_{H_L} A \quad \text{iff} \quad T \vdash e(A)).$$

Gödel-Löb's logic **GL** was proved to be complete for Peano arithmetic by Solovay [49]. Later was shown that it is the logic of provability of a large family of reasonable formal theories.

Using this fact and properties of the translation $A^\star$ from **S4Grz** to **GL**, we obtain the following arithmetical interpretation of Grzegorczyk's logic: let an arithmetical evaluation of modal formulas be as before, only now $e(\Box A) = Pr_\tau(\overline{e(A)}) \wedge \overline{e(A)}$.

Chapter 2

Modal sequent proof systems

In classical and intuitionistic logic, sequent proof systems originated by Gentzen [18] are recognized one of basic and most general proof-theoretic formulations of the logic. In case of modal logic they are no more accepted so widely as the natural formulation of derivability in a logic. A problematic point can be found in the nature of sequent rules - they usually introduce a connective and leave the context untouched. This is no more the case treating modal operators by a sequent rule. Typically, an introduction rule for the necessity modality to the succedent manipulate formulas in the antecedent as well. However, we find sequent calculi quite natural for modal logics, in the sense that they satisfactorily treat the local consequence relation of modal logics (see 1.0.2).

The fact that we deal with normal modal logics extending classical propositional logic is reflected by the design of modal sequent calculi - they are obtained extending a classical sequent calculus by modal rules. It is not the case, as one would expect, that each modal axiom corresponds to some sequent rule. To obtain a formulation of a sequent calculus with nice structural and analytic properties as e.g. cut admissibility (or elimination), one should be careful introducing modal rules. Concerning rules for the necessity modality in logics we consider in this thesis, we have one left rule corresponding to the schema T if the logic we deal with is reflexive, and one right rule corresponding to the distributivity schema K and all the other axioms at once.

The particular form of sequent calculi we have chosen for this and the following chapter fits our aim to use it for proof-search related manipulations. In particular, we use multisets of formulas to formulate a sequent, we use a definition without the cut rule which is to be proved admissible in our systems, and all other structural rules are built in strong logical rules.

Since the proof of uniform interpolation contained in the next chapter is closely related to decision procedures for modal logics and termination of a proof-search in the calculi is one of its main ingredients, we devote some space in this chapter to explain proof-search in modal logics.

For basic reference on modal sequent calculi see e.g. Wansing's chapter in [54], or Schwichtenberg's and Troelstra's book [51]. For sequent calculi of modal logics having arithmetical interpretation you may consult Sambin Valentini [46] or Avron [1].

The chapter 2 is organized as follows:

- Section 2.1: we define the sequent calculus G for classical propositional logic as the common basis for all modal sequent calculi. We briefly discuss sets vs. multisets setting.
- Section 2.2: we define the sequent calculus Gm_K for modal logic **K** and Gm_T for modal logic **T**.
  - Subsection 2.2.1: we explain proof-search in modal logics based on sequent calculi, discuss the termination problem and show that in Gm_K any proof-search terminates. Then we define the calculus Gm_T^+ for modal logic T including a simple loop preventing mechanism and show that it is terminating. Termination is one of the main requirements on the proof system we use to prove uniform interpolation using the Pitts' method.
  - Subsection 2.2.2: we prove that structural rules weakening, contraction, and cut are admissible in our calculi. We show that Gm_T and Gm_T^+ are equivalent.
- Section 2.3: we define the sequent calculus Gm_{GL} for modal logic **GL** and Gm_{Grz} for modal logic **S4Grz**.
  - Subsection 2.3.1: we show that in Gm_{GL} any proof-search terminates. Then we define the calculus Gm_{Grz}^+ for modal logic **S4Grz** including two loop preventing mechanisms and show that it is terminating.
  - Subsection 2.3.2: we prove that structural rules weakening and contraction are admissible in our calculi. We show that Gm_{Grz}^+ equals Gm_{Grz}.
  - subsection 2.3.2: we show cut admissibility in Gm_{GL} and Gm_{Grz} (and thus in Gm_{Grz}^+) using a semantic argument based on a decision procedure.

2.1 Classical sequent calculus G

First we introduce the sequent calculus G for classical propositional logic as the common basis which, extending by appropriate modal rules, results in particular modal logics.

Antecedents, succedents and principal formulas are defined as usual. We consider antecedents and succedents to be *finite multisets* of fomulas.

We consider sequent proofs in a tree form, the *height* of a proof is just its height as a tree.

Definition 2.1.1. Sequent calculus G:

$$\Gamma, p \Rightarrow p, \Delta$$

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}\ \wedge\text{-l} \qquad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}\ \vee\text{-r}$$

$$\frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta}\ \neg\text{-r} \qquad \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta}\ \neg\text{-l}$$

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}\ \wedge\text{-r} \qquad \frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\ \vee\text{-l}$$

The calculus G corresponds to the calculus G3cp from [51].

The structural rules of weakening, contraction, and cut are not listed in the definition of G, however, they are admissible in it. We prove this fact for modal sequent calculi based on G later.

Remark 2.1.2. Sets vs multisets

Since we are not dealing with substructural logics and the contraction rules are sound for all our systems, we have a choice between a formalization using sets or multisets of formulas. It is convenient to deal with multisets rather then with sets of formulas when considering proof-search and complexity related problems. The reason is that, in sets, the rules of contraction are hidden. It is therefore easier to control all steps in proofs and decision procedures dealing with a contraction-free calculus defined for multisets (although one has to prove that contraction rules are admissible). However, as will become clear later, we somehow cannot obey referring to sets establishing termination arguments for our calculi. On the other hand, if we dealt with sets, we would need to take care on steps where contractions are hidden and there it is like dealing with multisets again.

2.2 Sequent calculi for logics K and T

We introduce the sequent calculus Gm_K for modal logic K and Gm_T for modal logic T in a natural way, prove their structural properties, and show they are indeed equivalent to the corresponding Hilbert style formalizations. Then we define the sequent calculus Gm_T^+ for modal logic T including a loop preventing mechanism and show it is terminating and equivalent to Gm_T.

Definition 2.2.1. Sequent calculus Gm_K results from adding the following modal rule to G:

$$\frac{\Gamma \Rightarrow A}{\Box\Gamma, \Pi \Rightarrow \Box A, \Sigma}\ \Box_K$$

Sequent calculus Gm_T results from adding the following modal rule to Gm_K:

$$\frac{\Gamma, \Box A, A \Rightarrow \Delta}{\Gamma, \Box A \Rightarrow \Delta}\ \Box_T$$

Antecedents, succedents and principal formulas are defined as before. In the case of the $\Box_K$ rule, $\Box A$ and all formulas from $\Box\Gamma$ are principal.

Since our motivation comes from backward proof-search, we restrict the $\Box_K$ rule - Π contains only propositional variables and Σ contains only propositional variables and boxed formulas. This becomes clear in a termination argument.

The weakening rules, the contraction rules, and the cut rule are not listed among our rules, but they are admissible in our systems.

Definition 2.2.2. We say that a rule is *invertible* if whenever the conclusion of the rule has a proof, each premiss has a proof as well.

Notice that all the classical rules and the $\Box_T$ rule are invertible which can be easily shown either by a semantic argument or by induction on derivations.

2.2.1 Termination

Let us briefly explain how a proof search in modal logics works. We consider the simplest case of **K**.

We start with a sequent $(\Gamma \Rightarrow \Delta)$. Applying rules of the calculus backwards we create a tree whose nodes are labeled by sequents. Applying a rule, we create a predecessor node(s) of the current node labeled by the conclusion of the applied rule and label the new node(s) by the premiss(es) of the rule. We proceed until we reach a sequent in which all formulas are either atomic or boxed, say $(\Box\Gamma, \Pi \Rightarrow \Box\Delta, \Lambda)$.

Let us call it a *critical sequent.* If it is not an initial sequent ($\Pi \cap \Lambda = \emptyset$) and $\Box\Delta$ is nonempty we apply the $\Box_K$-rule and create a predecessor node(s) labeled by sequents $(\Gamma \Rightarrow B)$, for all $B \in \Delta$. We continue until there is no rule to be applied.

Leaves of the tree are labeled by sequents, on which no rule can be applied - they are either initial sequents or unprovable sequents. We mark the leaves as follows - the initial sequents as positive and the others as negative. We continue marking the sequents in the tree as follows: a critical sequent is marked as positive if *at least one* of its predecessors has been marked as positive. Any other sequent is marked as positive if *all* its predecessors have been marked as positive.

If the bottom sequent has been marked as positive, it is provable and by deleting all negative sequents we obtain its proof.

Since all the rules except the $\Box_K$ rule are invertible and we always first apply them backwards to reach a critical sequent, it is natural to define the following concept of a closure of a sequent $(\Gamma \Rightarrow \Delta)$ to consist of all immediately preceding critical sequents in a proof search tree for $(\Gamma \Rightarrow \Delta)$ (i.e. the critical sequents from the closure under all backward applicable invertible rules):

Definition 2.2.3. For a calculus Gm_L and a sequent $(\Gamma \Rightarrow \Delta)$, let $C(\Gamma; \Delta)$ denote the smallest set of sequents containing $(\Gamma \Rightarrow \Delta)$ and closed under backward applications of the invertible rules of Gm_L.

The *closure* of a sequent $(\Gamma \Rightarrow \Delta)$ denoted $Cl(\Gamma; \Delta)$ is then the set of all *critical* sequents from $C(\Gamma; \Delta)$.

It is clear that the closure of a sequent is finite and that conjunction of sequents from the closure proves the original sequent, and also whenever the original sequent is provable, each of sequents from the closure is provable as well. See Lemma 2.3.5 below.

The proof search tree then looks as follows: starting with a sequent $(\Gamma \Rightarrow \Delta)$, we first obtain a conjunction of branches with nodes labeled by critical sequents from the closure $Cl(\Gamma; \Delta)$, and then we apply a modal jump to each of them (if possible) to obtain a disjunction of branches with nodes labeled by all the possible $\Box_K$ predecessors.

A proof search terminates if the corresponding tree is finite. In other words, it terminates if there is a function defined on sequents which decreases in every backward application of a rule.

Any backward proof search in the calculus Gm_K obviously terminates: we consider the weight of a sequent to be the function and observe that for each rule, the weight function decreases in every backward application of the rule:

Lemma 2.2.4. *Backward proof search in Gm_K always terminates.*

This is not the case in the calculus Gm_T due to the $\Box_T$ rule in which a contraction is hidden and therefore the weight function can increase in a backward application of the $\Box_T$ rule (observe that the rule can always be applied backwards to a critical sequent). Moreover, no other function does the job - the calculus is not terminating. A counterexample is e.g. a proof search for sequent $(p \Rightarrow \Diamond(p \wedge q))$ which creates a loop.

This defect can be easily avoided by a simple loop-preventing mechanism: once we handle $\Box A$ going backward the $\Box_T$ rule, we mark it. To do it we add the third multiset Σ to each sequent to store formulas of the form $\Box A$ already handled. We empty this multiset whenever we go backward through the $\Box_K$ rule since in this case the boxed content of the antecedent properly changes. This idea results in the following calculus similar to the calculus used in [33] and [25] (in [33], it can be recognized in the decision procedure; in [25], the one-sided form of the calculus is used).

The loop preventing mechanism is built in the syntax which is usual when you have in mind an implementation of a decision procedure. The reason we have chosen this way is that, in the next chapter, we are going to use the calculus (or the sequents) in recursively called arguments of the procedure constructing the interpolants. It is easier to manage with a built-in mechanism.

We suggest reader to understand the third multiset as formulas which have been marked.

Definition 2.2.5. Sequent calculus Gm_T^+:

$$\Sigma|\Gamma, p \Rightarrow p, \Delta$$

$$\frac{\Sigma|\Gamma, A, B \Rightarrow \Delta}{\Sigma|\Gamma, A \wedge B \Rightarrow \Delta}\wedge\text{-l} \qquad \frac{\Sigma|\Gamma \Rightarrow A, B, \Delta}{\Sigma|\Gamma \Rightarrow A \vee B, \Delta}\vee\text{-r}$$

$$\frac{\Sigma|\Gamma, A \Rightarrow \Delta}{\Sigma|\Gamma \Rightarrow \neg A, \Delta}\neg\text{-r} \qquad \frac{\Sigma|\Gamma \Rightarrow A, \Delta}{\Sigma|\Gamma, \neg A \Rightarrow \Delta}\neg\text{-l}$$

$$\frac{\Sigma|\Gamma \Rightarrow A, \Delta \qquad \Sigma|\Gamma \Rightarrow B, \Delta}{\Sigma|\Gamma \Rightarrow A \wedge B, \Delta}\wedge\text{-r} \qquad \frac{\Sigma|\Gamma, A \Rightarrow \Delta \qquad \Sigma|\Gamma, B \Rightarrow \Delta}{\Sigma|\Gamma, A \vee B \Rightarrow \Delta}\vee\text{-l}$$

$$\frac{\emptyset|\Gamma \Rightarrow A}{\Box\Gamma|\Pi \Rightarrow \Box A, \Delta}\Box_K^+ \qquad \frac{\Box A, \Sigma|\Gamma, A \Rightarrow \Delta}{\Sigma|\Gamma, \Box A \Rightarrow \Delta}\Box_T^+$$

In the $\Box_K^+$ rule, Π contains only propositional variables and Δ contains only propositional variables and boxed formulas.

We define the closure of a sequent as before, only notice that here we are closing, besides the classical rules, under the $\Box_T^+$ rule as well.

Definition 2.2.6. For a calculus Gm_L^+ and a sequent $(\Sigma|\Gamma \Rightarrow \Delta)$, let $C(\Sigma|\Gamma;\Delta)$ denote the smallest set of sequents containing $(\Sigma|\Gamma \Rightarrow \Delta)$ and closed under backward applications of the invertible rules of Gm_L^+.

The *closure* of a sequent $(\Sigma|\Gamma \Rightarrow \Delta)$ denoted $Cl(\Sigma|\Gamma;\Delta)$ is then the set of all *critical* sequents from $C(\Sigma|\Gamma;\Delta)$.

Now let us see that this calculus is terminating.

Lemma 2.2.7. *Backward proof search in* Gm_T^+ *always terminates.*

PROOF OF LEMMA 2.2.7. We define $b(\Box\Sigma, \Pi, \Lambda)$ to be the number of boxed subformulas of formulas from $\Box\Sigma, \Pi, \Lambda$ counted as a *set*.

With each sequent $(\Sigma|\Pi \Rightarrow \Lambda)$ occurring during a proof search we associate an ordered pair of natural numbers $\langle b(\Sigma,\Pi,\Lambda), w(\Pi,\Lambda)\rangle$. We consider the pairs lexicographically ordered. In every backward application of a rule this measure decreases in terms of the lexicographical ordering - for all rules except the $\Box_K^+$ rule w decreases while b remains the same, for the $\Box_K^+$ rule b decreases.

For all rules except the $\Box_K^+$ rule w decreases while b remains the same. For classical rules this is obvious since they do not change the set of boxed subformulas. For the $\Box_T$ rule observe that $b(\Box A, A) = b(\Box A)$.

For the $\Box_K^+$ rule b decreases. It follows from the fact that $b(\Box\Gamma) > b(\Gamma)$ for a finite multiset of formulas Γ. To see this, let us $sf(\Gamma)$ denote the set of subformulas of a multiset Γ. Moreover, let $\preceq$ denote the well quasi-ordering on formulas defined $A \preceq B$ iff $w(A) \leq w(B)$, and let $\prec$ denote the corresponding strict ordering. Observe that, for $A \in sf(B)$, it holds that $A \preceq B$. There are two possibilities:

Either there is $\Box B \in sf(\Box\Gamma)$ such that $\Box B \notin sf(\Gamma)$ and we are done (in this case $\Box B \in \Box\Gamma$).

Or, for all $\Box B \in sf(\Box\Gamma)$, it holds $\Box B \in sf(\Gamma)$. Then each $\Box B \in \Box\Gamma$ is a subformula of a formula from Γ. Consider any formula from $\Box\Gamma$ and denote it $\Box B_1$. Then $\Box B_1$ is a subformula of a formula from Γ, say B_2. Obviously $B_1 \prec B_2$ since $\Box B_1 \preceq B_2$. Since $\Box B_2 \in \Box\Gamma$, it is a subformula of some $B_3 \in \Gamma$ such that $B_1 \prec B_2 \prec B_3$. We continue this way and create a sequence of B_i from Γ where each $\Box B_i$ is a subformula of B_{i+1} and for any $j < i$, $B_j \prec B_i$. Since Γ is finite, the sequence is also finite. Consider its last element B_n. Since the $\prec$ ordering is well founded, there is no such formula in Γ, a subformula of which is $\Box B_n$ - a contradiction.

So there is $\Box B \in sf(\Box\Gamma)$ such that $\Box B \notin sf(\Gamma)$ and hence $b(\Box\Gamma) > b(\Gamma)$.

See also [24] or [25], where another (however closely related) function is considered which depends on the weight of the sequent for which the proof search is considered. See also Remark 2.2.11. Here we can do without referring to the input sequent using the lexicographical ordering. Referring to the input sequent becomes necessary (even in the lexicographical setting) when dealing with modal logics that requires more complicated loop checking mechanisms, as e.g. **GL** or **S4Grz**. QED

2.2.2 Structural rules

Structural rules, i.e., the weakening rules, the contraction rules, and the cut rule are not listed among our rules in definitions of the calculi, but they are admissible in our systems.

Admissibility of a rule, elimination of a rule, and closure under a rule are three slightly different notions from the point of view of structural proof theory. For a discussion on this topic see [38]. What follows are proofs of a rule-admissibility established through induction on derivations.

We shall prove admissibility of structural rules for the calculus Gm_T^+. For the calculi Gm_K and Gm_T, admissibility of structural rules can be proved similarly but since it is an immediate consequence of their admissibility in Gm_T^+, we omit it.

For the cut-elimination in modal logics based on multisets see e.g. [51], where a slightly different symmetric definition of sequent calculi is used (treating both $\Box$ and $\Diamond$ modalities as primitive).

In what follows, the horizontal lines in proof figures stay for instances of rules of Gm_T^+ as well as for instances of admissible rules (see the appropriate labels).

Definition 2.2.8. We call a rule *admissible* if for each proof of an instance of its premiss(es) there is a proof of the corresponding instance of its conclusion.

We call a rule *height-preserving admissible* if for each proof of an instance of its premiss(s) of height n there is a proof of the corresponding instance of its conclusion of height $\leq n$.

We call a rule *height-preserving invertible* if whenever the conclusion of a rule has a proof of height n, each premiss has a proof of height $\leq n$.

Note that all rules except the $\Box_K$-rule and the $\Box_K^+$-rule are *height-preserving invertible.* This can be easily shown by induction on the height of the proof of the conclusion.

Lemma 2.2.9. *The weakening rules are admissible in Gm_T^+.*

PROOF OF LEMMA 2.2.9. The weakening rules are:

$$\frac{\Sigma|\Gamma \Rightarrow \Delta}{\Sigma|\Gamma, A \Rightarrow \Delta}\text{weak-l} \qquad \frac{\Sigma|\Gamma \Rightarrow \Delta}{\Sigma|\Gamma \Rightarrow \Delta, A}\text{weak-r} \qquad \frac{\Sigma|\Gamma \Rightarrow \Delta}{\Sigma, \Box A|\Gamma \Rightarrow \Delta}\text{weak-l+}$$

The proof is by induction on the weight of the weakening formula and, for each weight, on the height of the proof of the premiss. The induction runs simultaneously for all the weakening rules. Note that in the weak-l+ rule, the weakening formula is always of the form $\Box A$.

For an atomic weakening formula the proof is obvious - note that weakening is built in initial sequents as well as in the $\Box_K^+$-rule.

For non atomic and not boxed formula we use height-preserving invertibility of the appropriate rule, weaken by formula(s) of lower weight, and then apply the appropriate rule.

Let us consider the weakening formula of the form $\Box A$. If the last inference is a classical inference or a $\Box_T^+$ inference, we just use the i.h., weaken one step above, and use the appropriate rule again. Let the last inference be a $\Box_K^+$ inference. The case of weak-r is then obvious since it is built-in the $\Box_K^+$ rule. weak-l+ and weak-l are captured as follows using the i.h.:

$$\dfrac{\dfrac{\emptyset|\Sigma^{\Box} \Rightarrow B}{\emptyset|\Sigma^{\Box}, A \Rightarrow B}\text{weak-l}}{\Sigma, \Box A|\Gamma \Rightarrow \Box B, \Delta}\Box_K^+ \qquad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset|\Sigma^{\Box} \Rightarrow B}{\emptyset|\Sigma^{\Box}, A \Rightarrow B}\text{weak-l}}{\Sigma, \Box A|\Gamma \Rightarrow \Box B, \Delta}\Box_K^+}{\Sigma, \Box A|A, \Gamma \Rightarrow \Box B, \Delta}\text{weak-l}}{\Sigma|\Box A, \Gamma \Rightarrow \Box B, \Delta}\Box_T^+$$

The later is the only non height-preserving step in the proof. It is easy to see that this problem does not occur when dealing with Gm_T or Gm_K where the the height-preserving admissibility of weakening rules can easily be obtained. However, the height-preserving admissibility of weakening rules is not necessary in what follows. QED

Lemma 2.2.10. *The contraction rules are height-preserving admissible in Gm_T^+.*

PROOF OF LEMMA 2.2.10. The contraction rules are:

$$\dfrac{\Sigma|\Gamma, A, A \Rightarrow \Delta}{\Sigma|\Gamma, A \Rightarrow \Delta}\text{contr-l} \qquad \dfrac{\Sigma|\Gamma \Rightarrow \Delta, A, A}{\Sigma|\Gamma \Rightarrow \Delta, A}\text{contr-r}$$

$$\dfrac{\Sigma, \Box A, \Box A|\Gamma \Rightarrow \Delta}{\Sigma, \Box A|\Gamma \Rightarrow \Delta}\text{contr-l+}$$

The proof is by induction on the weight of the contraction formula and, for each weight, on the height of the proof of the premiss. The induction runs simultaneously for all the contraction rules. We use the height preserving invertibility of rules. Note that in the contr-l+ rule the contraction formula is always of the form $\Box A$.

For A atomic, if the premiss is an initial sequent, the conclusion is an initial sequent as well. If not, A is not principal and we use i.h. and apply contraction one step above or, in the case of $\Box_K^+$ rule, we apply the rule so that the conclusion is weakened by only one occurrence of A.

For A not atomic and not boxed we use the height preserving invertibility of the appropriate rule and by i.h. we apply contraction on formula(s) of lower weight and then the rule again. The third multiset does not make any difference here and it works precisely as in the classical logic.

All the steps are obviously height preserving.

Now suppose the contraction formula to be of the form $\Box B$. We distinguish three cases:

(i) The contraction formula is the principal formula of a $\Box_K^+$ inference in the antecedent. Then we permute the proof as follows using the i.h.:

$$\dfrac{\dfrac{\emptyset | B, B, \Gamma \Rightarrow C}{\Box B, \Box B, \Box\Gamma | \Pi \Rightarrow \Box C, \Sigma}\,\Box_K^+}{\Box B, \Box\Gamma | \Pi \Rightarrow \Box C, \Sigma}\,\text{contr-l+} \quad \Longrightarrow \quad \dfrac{\dfrac{\emptyset | B, B, \Gamma \Rightarrow C}{\emptyset | B, \Gamma \Rightarrow C}\,\text{contr-l}}{\Box B, \Box\Gamma | \Pi \Rightarrow \Box C, \Sigma}\,\Box_K$$

The permutation is obviously height preserving.

(ii) The contraction formula is the principal formula of a $\Box_T^+$ inference in the antecedent. Then we permute the proof as follows using the i.h. and the height preserving invertibility of the $\Box_T^+$ rule:

$$\dfrac{\dfrac{\Sigma, \Box B | \Box B, B, \Gamma \Rightarrow \Delta}{\Sigma | \Box B, \Box B, \Gamma \Rightarrow \Delta}\,\Box_T^+}{\Sigma | \Box B, \Gamma \Rightarrow \Delta}\,\text{contr-l} \quad \Longrightarrow \quad \dfrac{\dfrac{\dfrac{\Sigma, \Box B | \Box B, B, \Gamma \Rightarrow \Delta}{\Sigma, \Box B, \Box B | B, B, \Gamma \Rightarrow \Delta}\,\text{invert.}}{\Sigma, \Box B | B, \Gamma \Rightarrow \Delta}\,\text{contr-l,l+}}{\Sigma | \Box B, \Gamma \Rightarrow \Delta}\,\Box_T^+$$

The permutation is height preserving since the steps contr-l, contr-l+, and invert. do not change the height of the proof.

(iii) The contraction formula is the principal formula in the succedent and we want to have admissible the following contraction:

$$\dfrac{\dfrac{\emptyset | \Gamma \Rightarrow B}{\Box\Gamma | \Pi \Rightarrow \Box B, \Box B, \Sigma}\,\Box_K^+}{\Box\Gamma | \Pi \Rightarrow \Box B, \Sigma}\,\text{contr-r}$$

Then we use the $\Box_K^+$ rule so that the conclusion is not weakened by the other occurrence of $\Box B$. This step is obviously height preserving.

(iv) The contraction formula is not the principal formula. If the last step is a $\Box_K^+$ inference, $\Box B$ is in Δ. Then we use the $\Box_K^+$ rule so that the conclusion is weakened by only one occurrence of the contraction formula. If the last step is another inference, we use contraction one step above on the proof of lower height. If it is an initial sequent, the conclusion of the desired contraction is an initial sequent as well. Again, all the steps are height preserving. QED

Remark 2.2.11. **Removing duplicate formulas.**

As long as we have the height-preserving admissibility of the contraction rules, we can always remove duplicate formulas during a backward proof search. It is important for the space complexity. Consider the $\Box_T^+$ rule is applied backwards. It can be split into two cases: either the principal formula $\Box A$ is already in the third multiset Σ, and then we do not add it there, or it is not, and the inference stays as it is and we add $\Box A$ to Σ. This corresponds to treating the third multiset as a set. Try for example to search for a proof of $(\emptyset|\Box\Box\Box\Box\Box p \Rightarrow \Box\Box\Box\Box p)$ in both versions of the calculus. If we allow duplicate formulas in Σ, the increase of the weight of the sequent can be exponential. For more on this topic see Heuerding [24], the calculus $KT^{S,2}$. We do not change Gm_T^+ this way to prove uniform interpolation. However, our proof can be easily reformulated in this manner.

If we consider a proof-search for a sequent $(\Theta|\Pi \Rightarrow \Lambda)$ and put $c = w(\Theta, \Pi, \Lambda)$, an analogous function to that in [24] would be $f(\Sigma|\Gamma;\Delta) = c^2 \cdot b(\Sigma,\Gamma,\Delta) + w(\Gamma,\Delta)$. It decreases in each backward application of a rule of the variant of Gm_T^+ where we do not duplicate formulas in the third multiset Σ. Then possible increase of $w(\Gamma,\Delta)$ in a backward application of the $\Box_K^+$ rule is balanced by c^2. If we do not remove duplicate formulas, the constant c^2 has to be replaced by an exponential function of c. [1]

Lemma 2.2.12. *The following cut rules are admissible in* Gm_T^+.

$$\frac{\emptyset|\Gamma \Rightarrow \Delta, A \qquad \emptyset|A, \Pi \Rightarrow \Lambda}{\emptyset|\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{cut} \qquad \frac{\Sigma|\Gamma \Rightarrow \Delta, \Box A \qquad \Theta, \Box A|\Pi \Rightarrow \Sigma}{\Sigma, \Theta|\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{cut+}$$

The above cut rule cannot be replaced by the expected form of cut:

$$\frac{\Sigma|\Gamma \Rightarrow \Delta, A \qquad \Theta|A, \Pi \Rightarrow \Lambda}{\Sigma, \Theta|\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{cut'}\ ,$$

since it is not admissible in Gm_T^+. The counterexample is the following use of cut':

$$\frac{\dfrac{\emptyset|p \Rightarrow p}{\Box p|\emptyset \Rightarrow \Box p}\,\Box_K^+ \qquad \emptyset|\Box p \Rightarrow p}{\Box p|\emptyset \Rightarrow p}\,\text{cut'}$$

[1] In Heuerding [24] (where one-sided version of the calculus is used treating both $\Box, \Diamond$ as primitive), $b(\Gamma)$ is replaced by the number of boxes in Γ. There is a gap since the function can increase in a backward application of the $(\Diamond, new)$ rule of his calculus $KT^{S,2}$. An example is a proof search for $\Diamond\Box p$ where $f(\emptyset|\Diamond\Box p) < f(\Diamond\Box p|\Box p)$ since then the number of boxes in the sequent increases.

which results sequent $(\Box p|\emptyset \Rightarrow p)$ unprovable in Gm_T^+.

However, the cut rule above suffices to go through the proof of Theorem 3.3.1 and it corresponds to system Gm_T in view of Lemma 2.2.13. The cut+ rule is only needed to prove admissibility of the cut rule and it will not be used in the proof of Theorem 3.3.1. What we care on here are only sequents with the third multiset empty since they matches usual sequents of the system Gm_T and therefore they have clear meaning (see Lemma 2.2.13, 2.2.16).

PROOF OF LEMMA 2.2.12. The proof of cut-admissibility is by induction on the weight of the cut formula and, for each weight, on the sum of the heights of the proofs of the premisses. The main step is the following: Given cut-free proofs of the premisses we have to show that there is a proof of the conclusion using only cuts where the cut formula is of lower weight or cuts where the sum of the heights of the proofs of the premisses is lower.

We proceed simultaneously for both the cut rules. Note that in the cut+ rule, the cut formula is always of the form $\Box A$.

If the cut formula is an atom and principal in one premiss (which is then an initial sequent) then we can replace the cut inference by weakening inferences. If the cut formula is principal in both premisses, the conclusion is an initial sequent. If it is principal in neither premiss, we can apply the cut rule one step above so that the sum of the heights of the proofs of its premisses is lower, then apply the original rule and finally some contractions (if one premiss is an initial sequent, the conclusion is an initial sequent as well).

Let us consider non atomic and not boxed cut formula. If it is not principal formula in one premiss we can apply the cut rule one step above so that the sum of the heights of the proofs of its premisses is lower, then apply the original rule and finally some contractions. If the cut formula is principal in both premisses we proceed the same way as in the case of classical sequent calculus. For missed details (reduction steps treating classical connectives) see the proof for calculus G3cp in [51] or [38]. We deal with the cut rule where the third multiset is empty and therefore it does not make any change here.

Let the cut formula be of the form $\Box B$. Again, if it is not principal in one premiss we can apply the cut rule one step above so that the sum of the heights of the proofs of its premisses is lower, then apply the original rule and finally some contractions. So let the cut formula be principal in both premisses. Then there are two cases to distinguish:

(i) The cut formula is the principal formula of a $\Box_K^+$ inference in both premisses (i.e. the following instance of the cut+ rule):

$$\dfrac{\dfrac{\emptyset|\Gamma \Rightarrow B}{\Box\Gamma|\Gamma' \Rightarrow \Box B, \Delta}\,\Box_K^+ \qquad \dfrac{\emptyset|\Pi, B \Rightarrow C}{\Box B, \Box\Pi|\Pi' \Rightarrow \Box C, \Lambda}\,\Box_K^+}{\Box\Gamma, \Box\Pi|\Gamma', \Pi' \Rightarrow \Delta, \Box C, \Lambda}\,\text{cut+}$$

Here we apply the i.h. and use the following cut inference with the cut formula of lower weight and the $\Box_K^+$ rule to permute the proof as follows:

$$\dfrac{\dfrac{\emptyset|\Gamma \Rightarrow B \qquad \emptyset|\Pi, B \Rightarrow C}{\emptyset|\Gamma, \Pi \Rightarrow C}\,\text{cut}}{\Box\Gamma, \Box\Pi|\Gamma', \Pi' \Rightarrow \Delta, \Box C, \Lambda}\,\Box_K^+$$

(ii) The cut formula is the principal formula of a $\Box_K^+$ inference in one premiss while it is the principal formula of a $\Box_T^+$ inference in the other. The only possibility how this situation can occur is the following instance of the cut rule:

$$\dfrac{\dfrac{\emptyset|\emptyset \Rightarrow B}{\emptyset|\Gamma \Rightarrow \Box B, \Delta}\,\Box_K^+ \qquad \dfrac{\Box B|\Pi, B \Rightarrow \Lambda}{\emptyset|\Box B, \Pi \Rightarrow \Lambda}\,\Box_T^+}{\emptyset|\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{cut}$$

In this case we use, by the i.h., one cut+ inference with a lower sum of the heights of its premisses and one cut inference with the cut formula of a lower weight to permute the proof as follows:

$$\dfrac{\dfrac{\dfrac{\emptyset|\emptyset \Rightarrow B}{\emptyset|\Gamma \Rightarrow \Box B, \Delta}\,\Box_K^+ \qquad \Box B|\Pi, B \Rightarrow \Lambda}{\emptyset|\Gamma, B, \Pi \Rightarrow \Delta\Lambda}\,\text{cut+} \qquad \emptyset|\emptyset \Rightarrow B}{\emptyset|\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{cut}$$

QED

Lemma 2.2.13. *Gm_T^+ is equivalent to Gm_T:*

$$\vdash_{Gm_T} \Gamma \Rightarrow \Delta \textit{ iff } \vdash_{Gm_T^+} \emptyset|\Gamma \Rightarrow \Delta$$

PROOF OF LEMMA 2.2.13. The right-left implication follows immediately since deleting the "|" symbol from all sequents in a Gm_T^+ proof of $(\emptyset|\Gamma \Rightarrow \Delta)$ yields a Gm_T proof of $(\Gamma \Rightarrow \Delta)$.

The left-right implication is proved by induction on the height of the proof $\vdash_{Gm_T}$ $\Gamma \Rightarrow \Delta$ using admissibility of structural rules (weakening and contraction suffice here).

The steps for initial sequents and classical rules are obvious since they do not change the third multiset. So let us consider the box rules.

The $\Box_K$ rule is captured in Gm_T^+ as follows

$$\cfrac{\cfrac{\cfrac{\emptyset|\Gamma \Rightarrow A}{\Box\Gamma|\Pi \Rightarrow \Box A, \Delta}\ \Box_K^+}{\Box\Gamma|\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \text{admiss. weak.}}{\emptyset|\Box\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \Box_T^+ \text{ inferences}$$

The $\Box_T$ rule is captured as follows:

$$\cfrac{\cfrac{\cfrac{\emptyset|\Gamma, \Box A, A \Rightarrow \Delta}{\Box A|\Gamma, A, A \Rightarrow \Delta}\ \text{invert. of } \Box_T^+}{\Box A|\Gamma, A \Rightarrow \Delta}\ \text{admiss. contr.}}{\emptyset|\Gamma, \Box A \Rightarrow \Delta}\ \Box_T^+$$

QED

As an immediate consequence of Lemma 2.2.10 , 2.2.9, and 2.2.13 we obtain:

Corollary 2.2.14. *The weakening and the contraction rules are admissible in Gm_T and Gm_K.*

PROOF OF COR. 2.2.14. For Gm_T it follows from the three lemmata immediately. For admissibility of weak-l in Gm_K, we only remove the symbol "—" from the left proof-tree in 2.2.9, weak-r is obviously admissible as before.

For admissibility of contraction rules, we use (i) and (iii) form 2.2.10 removing the symbol "—" again and omitting steps for the $\Box_T^+$ rule. QED

The height preserving admissibility of the weakening and the contraction rules in Gm_T and Gm_K can also be obtained using a similar proof as for Gm_T^+.

As an immediate consequence of Lemma 2.2.12 and 2.2.13 we obtain the following admissibility of the usual cut rule in Gm_T and Gm_K:

Corollary 2.2.15. *The cut rule*

$$\frac{\Gamma \Rightarrow \Delta, A \qquad A, \Pi \Rightarrow \Lambda}{\Gamma, \Pi \Rightarrow \Delta, \Sigma}\ cut$$

is admissible in Gm_T and Gm_K.

PROOF OF COR. 2.2.15. For Gm_T it follows from 2.2.12 and 2.2.13 immediately.

For Gm_K we again use argument from 2.2.12 removing the symbol "—" and omitting steps for the $\Box_T^+$ rule. QED

Lemma 2.2.16. *Gm_K and Gm_T are equivalent to the corresponding Hilbert style definitions H_K and H_T:*

$$\vdash_{Gm_K} \Gamma \Rightarrow \Delta \text{ iff } \vdash_{H_K} \bigwedge \Gamma \rightarrow \bigvee \Delta$$
$$\vdash_{Gm_T} \Gamma \Rightarrow \Delta \text{ iff } \vdash_{H_T} \bigwedge \Gamma \rightarrow \bigvee \Delta$$

PROOF OF LEMMA 2.2.16. Easy induction on the height (the length) of the proof of $\Gamma \Rightarrow \Delta$ ($\bigwedge \Gamma \rightarrow \bigvee \Delta$ resp.) using admissibility of structural rules. QED

2.3 Sequent calculi for logics having arithmetical interpretations

Consider the form of Lőb's and Grzegorczyk's axioms:

$$\Box(D \rightarrow p) \rightarrow \Box p$$

where D is $\Box p$ and $\Box(p \rightarrow \Box p)$ respectively. Let us call D a diagonal formula. The presence of the diagonal formula in the axioms reflects in its presence in the appropriate sequent rules - in both cases it appears in the antecedent of its premiss.

It causes problems proving structural properties of such a sequent system, e.g. cut elimination. Although both calculi are known to admit cut elimination, a direct syntactic proof of cut elimination is highly nontrivial.

We have formulated our calculi without the cut rule so we have to show that it is admissible in our systems. We refer to the semantical completeness argument given by a form of a decision procedure for the calculi.

For more information see [46], [1].

Definition 2.3.1. Sequent calculus Gm_{GL} results from G adding the following modal rule (as before, Π contains only propositional variables and Δ contains propositional variables and boxed formulas):

$$\frac{\Box\Gamma, \Gamma, \Box A \Rightarrow A}{\Box\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \Box_{GL}$$

Sequent calculus Gm_{Grz} results from G adding the rule $\Box_T$ and the following modal rule:

$$\frac{\Box\Gamma, \Box(A \rightarrow \Box A) \Rightarrow A}{\Box\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \Box_{Grz}$$

2.3.1 Termination

We shall se that, for termination of proof search in **GL** and **Grz**, the presence of the diagonal formula in the $\Box_L$ rule is substantial since it provides us with a nice and natural loop checker which is already built in the syntax.

In Gm_{GL}, consider a proof search for a sequent $(\Pi \Rightarrow \Lambda)$. First we create a tree, as before for **K** and **T**, going backwards the rules of Gm_{GL}.

To obtain termination we would need to make one more restriction here - if one of the critical branches above a $\Box_{GL}$ inference is closed, the others are closed as well (this branching is disjunctive and you can think of the branches as treating simultaneously). Try e.g. to create such a tree for $(\Box\neg\Box\Box p \Rightarrow \Box p)$ to get feeling what is the matter here - this proof search creates an infinite branch repeating the $\Box_{GL}$ inference with $\Box\Box p$ principal.

It is important to note that this looping is not substantial for creating a proof or a counterexample since we reach an initial sequent (on another branch of course) *before* this looping starts. Also note that this looping occurs on the disjunctive branching of a proof-search tree. Let us see that this kind of looping can occur only in the case of provable sequents (in contrast to logics **S4** or **K4** where a similar proof search creates a loop in the case of an unprovable sequent and the resulting counterexample then must contain an infinite branch or a loop):

Since for the classical rules the weight function decreases, a loop must contain at least one $\Box_L$ inference. Think of the critical sequent of this $\Box_{GL}$ inference. To create a loop we need to meet following two things: we need a formula (in the antecedent) which returns the same boxed formula again and again to the succedent - i.e. we need a formula $\Box\neg\Box B$ in the antecedent. Then we need the $\Box_{GL}$ inference to be applied - i.e. we need at least one formula $\Box C$ in the succedent. But a sequent of this form, i.e. $(\Box\neg\Box B, \Gamma \Rightarrow \Box C, \Delta)$, is provable in GL (for admissibility of weakening see 2.3.6 below, $(\Pi, B \Rightarrow B, \Lambda)$ is obviously provable):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Box B, B, \Box B \Rightarrow B}}{\Box B \Rightarrow \Box B}\Box_{GL}}{\Box\neg\Box B, \Box B \Rightarrow B, \Box B}\text{admiss. weak.}}{\Box\neg\Box B, \neg\Box B, \Box B \Rightarrow B}\neg\text{-l}}{\Box\neg\Box B \Rightarrow \Box B}\Box_{GL}}{\Box\neg\Box B, \Box C \Rightarrow C, \Box B}\text{admiss. weak.}}{\Box\neg\Box B, \neg\Box B, \Box C \Rightarrow C}\neg\text{-l}}{\Box\neg\Box B \Rightarrow \Box C}\Box_{GL}}{\Box\neg\Box B, \Gamma \Rightarrow \Box C, \Delta}\text{admiss. weak.}$$

However, a simpler loop preventing mechanism using the substantial presence of the diagonal formula can be used as follows: the looping can be prevented by checking, when applying the $\Box_{GL}$ rule backwards, if the diagonal formula is (already) in the antecedent or not, since it detect possible previous backward application of the $\Box_{GL}$ rule with the same principal formula. If the diagonal formula is in the antecedent, the critical sequent is of the form $(\Box\Gamma, \Box A, \Phi \Rightarrow \Box\Delta, \Box A, \Psi)$, which is obviously provable, and we immediately close the branch as in the case of an initial sequent. This mechanism can be built in the calculus itself splitting the $\Box_{GL}$ rule into two cases, but we do not change the definition of the calculus and only use this loop preventing mechanism proving termination of the calculus Gm_{GL} and Theorem 3.4.1.

For a decision procedure for **GL** and a termination argument for its sequent calculus (based on sets) see also [53].

Now let us precisely state that a proof search in Gm_{GL} terminates. This means that the resulting proof search tree is finite.

Lemma 2.3.2. *Proof search in the calculus Gm_{GL} always terminates.*

PROOF OF LEMMA 2.3.2. Consider a proof search for a sequent $(\Pi \Rightarrow \Lambda)$. Let d be the maximal box-depth of Π, Λ. This is the maximal number of $\Box_{GL}$ inferences in a branch of the proof search tree providing we use the loop preventing mechanism as described above, i.e., we do not apply the $\Box_{GL}$ rule if the diagonal formula is already in the antecedent. This is crucial since it enables us to bound the weight of sequents occurring in a proof search:

Put $c = 2^d w(\Pi, \Lambda)$, i.e. an upper bound of the weight of a sequent occurring in a proof search for a sequent $(\Pi \Rightarrow \Lambda)$ (c is then a constant for $(\Pi \Rightarrow \Lambda)$.)

Let $b(\Gamma)$ be the number of boxed formulas in Γ counted as a set.

For a sequent $(\Gamma \Rightarrow \Delta)$, consider an ordered pair $\langle c - b(\Gamma), w(\Gamma, \Delta)\rangle$. Now this measure decreases in every backward application of a rule in terms of the lexicographical ordering:

c is certainly greater or equal to the maximal number of boxed formulas in the antecedent which can occur during the proof search, so the first number does not decrease below zero. For a classical rule, the weight of a sequent decreases. For the $\Box_{GL}$ rule b increases and so $c - b$ decreases. Note that we are using the loop preventing mechanism here and do not apply the $\Box_{GL}$ rule backwards if the principal formula is already in the antecedent.

Notice that in contrast with the case of Gm_T^+ in 2.2.7 where a similar idea is used, this measure also depends on the complexity of the input sequent.

Another way (closer to the approach of [25] or [24]) how to formulate the function is the following: For any sequent $(\Gamma \Rightarrow \Delta)$ consider the following function:

$$f(\Gamma \Rightarrow \Delta) = c^2 - cb(\Gamma) + w(\Gamma, \Delta).$$

This function (values of which are nonnegative integers) decreases in every backward application of a rule in a proof search for $(\Pi \Rightarrow \Lambda)$.

Here c is a constant, c^2 is included to ensure that f doesn't decrease below zero, and $cb(\Gamma)$ balances the possible increase of $w(\Gamma \Rightarrow \Delta)$ in the case of a backward application of the $\Box_{GL}$-rule.

QED

Gm_{Grz} itself is not terminating for the same reason as Gm_T - we have to prevent reflexive looping. It is done precisely as in the case of the calculus Gm_T^+ by adding the third multiset of formulas to a sequent.

The proof search is analogous to the previous case of **GL** but this time the sequents that can cause 'transitive' looping are *not* provable any more. In contrast to the previous case, the looping occurs on the conjunctive branching here (thanks the form of the diagonal formula it occurs in a backward application of the $\vee$-l rule). See the following example of looping - the two bold sequents are, up to contraction, the same $(\Box(p \to \Box p) \leftrightarrow \Box(\neg p \vee \Box p))$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\vdots \qquad \dfrac{\dfrac{\vdots}{\boldsymbol{\Box\neg\Box p, \Box(\neg p \vee \Box p), \Box(\neg p \vee \Box p), \Rightarrow p, p, \Box p}}}{\Box\neg\Box p, \Box(\neg p \vee \Box p), \Box(\neg p \vee \Box p), \neg p, \Rightarrow p, \Box p}\;\neg\text{-l}}{\Box\neg\Box p, \Box(\neg p \vee \Box p), \Box(\neg p \vee \Box p), \neg p \vee \Box p, \Rightarrow p, \Box p}\;\vee\text{-l}}{\Box\neg\Box p, \neg\Box p, \Box(\neg p \vee \Box p), \Box(\neg p \vee \Box p), \neg p \vee \Box p, \Rightarrow p}\;\neg\text{-l}}{\dfrac{\boldsymbol{\Box\neg\Box p, \Box(\neg p \vee \Box p) \Rightarrow p, \Box p}}{\Box\neg\Box p, \neg\Box p, \Box(\neg p \vee \Box p) \Rightarrow p}\;\neg\text{-l}}\;\Box_{Grz}}{\Box\neg\Box p \Rightarrow \Box p}\;\Box_{Grz}
$$

However, as in the case of **GL**, these loops are not substantial for creating a proof or a counterexample. Diagonal formula plays a crucial role also here and can be used as a natural loop-preventing mechanism:

The looping is prevented by splitting the $\Box_{Grz}$ rule into two cases distinguishing if the diagonal formula is present in the antecedent or not (this time we have to build the mechanism into the calculus itself since it changes the rule and not only close a branch of a proof search tree). We also change the premisses of the Grz rules closing under the $\Box_T$ rule at the same time. This results in the following calculus Gm_{Grz}^+ containing two loop-preventing mechanisms:

Definition 2.3.3. The calculus Gm_{Grz}^+ results from the calculus Gm_T^+ by adding the following two rules:

$$\frac{\Box\Gamma, \Box(A \to \Box A)|\emptyset\Gamma \Rightarrow A}{\Box\Gamma|\Pi \Rightarrow \Box A, \Delta}\,\Box^+_{Grz1}, (A \to \Box A) \notin \Gamma \qquad \frac{\Box\Gamma|\emptyset \Rightarrow A}{\Box\Gamma|\Pi \Rightarrow \Box A, \Delta}\,\Box^+_{Grz2}, (A \to \Box A) \in \Gamma$$

Consider the second, $\Box^+_{Grz2}$ rule bottom up. When the diagonal formula is already in the third multiset, we apply the rule so that we neither add the diagonal formula to the third multiset, nor we add Γ to the antecedent. The latter relates to the following: to move from $(\Box\Gamma|\ldots)$ to $(\Box\Gamma|\Gamma\ldots)$ in the antecedent in a backward application of the $\Box_L$ rule corresponds to treating transitivity (a similar phenomenon can be seen in completeness proofs for transitive modal logics). This is omitted here to prevent looping. However, the calculus remains complete - it is equivalent to the Gm_{Grz} as we show in Lemma 2.3.10. First let us see that Gm^+_{Grz} is terminating.

To make the argument easier, we adopt the same restriction to the $\Box^+_T$ rule as in the remark 2.2.11 about duplicate formulas - we shall treat the third multiset as a set.

Lemma 2.3.4. *Proof search in Gm^+_{Grz} for sequents of the form $(\emptyset|\Gamma \Rightarrow \Delta)$ always terminates.*

PROOF OF LEMMA 2.3.4. Consider a proof search for a sequent $(\emptyset|\Pi \Rightarrow \Lambda)$. Let d be maximal box depth in $(\emptyset|\Pi \Rightarrow \Lambda)$, which is, as in the case of **GL**, the maximal number of $\Box^+_{Grz}$ rules along one branch of the proof search tree. Let $b(\Gamma)$ be the number of boxed subformulas of Γ counted as a set.

With each sequent $(\Sigma|\Gamma \Rightarrow \Delta)$ occurring during the proof search, we associate an ordered pair $\langle e - |\Sigma^\circ|, w(\Gamma, \Delta)\rangle$. Here $e = d.b(\Pi, \Lambda)$ is an upper bound of the number of formulas stored in Σ if we do not duplicate formulas. Therefore the first number does not decrease below zero. The measure obviously decreases in every backward application of a rule of the calculus. For the $\Box^+_{Grz1}$ rule, $|\Sigma^\circ|$ increases and so $e - |\Sigma^\circ|$ decreases, while for other rules the weight $w(\Gamma, \Delta)$ decreases.

If we would allow duplicate formulas in Σ, then $b(\Gamma)$ has to be counted as a multiset, and e would be a highly exponential function of b.

QED

The closure of a sequent is for Gm_{GL} and Gm^+_{Grz} defined as before for Gm_K and Gm^+_T respectively.

Notice that for a non-critical sequent any sequent from its closure is of strictly less weight.

The following lemma is an easy observation about the closure we shall use later in our proofs:

Lemma 2.3.5. **(1)** *Let Gm_L be one of Gm_K, Gm_GL and $(\Gamma \Rightarrow \Delta)$ be a sequent, $Cl(\Gamma; \Delta) \equiv \{\Pi_1 \Rightarrow \Lambda_1, \ldots, \Pi_n \Rightarrow \Lambda_n\}$. Then:*

(i) $\Pi_1 \Rightarrow \Lambda_1; \ldots; \Pi_n \Rightarrow \Lambda_n \vdash \Gamma \Rightarrow \Delta$
if $\vdash_{Gm_L} \Gamma \Rightarrow \Delta$ *then* $\vdash_{Gm_L} \Pi_i \Rightarrow \Lambda_i$ *for each* i.

(ii) $\Pi_1, \Theta \Rightarrow \Omega, \Lambda_1; \ldots; \Pi_n, \Theta \Rightarrow \Omega, \Lambda_n \vdash \Gamma, \Theta \Rightarrow \Omega, \Delta$
if $\vdash_{Gm_L} \Gamma, \Theta \Rightarrow \Omega, \Delta$ *then* $\vdash_{Gm_L} \Pi_i, \Theta \Rightarrow \Omega, \Lambda_i$ *for each* i.

(2) *Let* Gm_L^+ *be one of* $Gm_T^+, Gm_{G}rz^+$ *and* $(\Sigma|\Gamma \Rightarrow \Delta)$ *be a sequent,* $Cl(\Sigma|\Gamma; \Delta) \equiv \{\Upsilon_1|\Pi_1 \Rightarrow \Lambda_1, \ldots, \Upsilon_n|\Pi_n \Rightarrow \Lambda_n\}$. *Then:*

(i) $\Upsilon_1|\Pi_1 \Rightarrow \Lambda_1; \ldots; \Upsilon_n|\Pi_n \Rightarrow \Lambda_n \vdash \Sigma|\Gamma \Rightarrow \Delta$
if $\vdash_{Gm_L^+} \Sigma|\Gamma \Rightarrow \Delta$ *then* $\vdash_{Gm_L^+} \Upsilon_i|\Pi_i \Rightarrow \Lambda_i$ *for each* i.

(ii) $\Upsilon_1, \Phi|\Pi_1, \Theta \Rightarrow \Omega, \Lambda_1; \ldots; \Upsilon_n, \Phi|\Pi_n, \Theta \Rightarrow \Omega, \Lambda_n \vdash \Sigma, \Phi|\Gamma, \Theta \Rightarrow \Omega, \Delta$
if $\vdash_{Gm_L^+} \Sigma|\Gamma, \Theta \Rightarrow \Omega, \Delta$ *then* $\vdash_{Gm_L^+} \Pi_i, \Upsilon_i|\Theta \Rightarrow \Omega, \Lambda_i$ *for each* i.

PROOF OF LEMMA 2.3.5. (i) follows in both cases immediately from the definition of the closure and the invertibility of the rules.
The first part of (ii) follows in both cases from (i) taking the proof-tree obtained in (i) and adding the same context to all the sequents which by the admissibility of weakening yields again a proof-tree. The second part of (ii) follows by the invertibility of the rules. QED

2.3.2 Structural rules

Lemma 2.3.6. *Weakening and contraction rules are height-preserving admissible in* Gm_{GL}.

PROOF OF LEMMA 2.3.6. The arguments are similar as used in 2.2.10 and 2.2.9, we only state the modal steps here. Weak-r is again built in the modal rule.

Weak-l by $\Box A$, the last step is a $\Box_{GL}$ inference:

$$\dfrac{\dfrac{\Box\Gamma, \Gamma, \Box B \Rightarrow B}{\Box A, A, \Box\Gamma, \Gamma, \Box B \Rightarrow B}\text{weak-l}}{\Box A, \Box\Gamma, \Pi \Rightarrow \Box B, \Lambda}\Box_{GL}$$

Contr-r on $\Box A$, with $\Box A$ principle of a $\Box_{GL}$ inference: we use the $\Box_{GL}$ rule so that we do not weaken by the other occurrence of $\Box A$ in the conclusion.

Contr-l on $\Box A$, with $\Box A$ principle of a $\Box_{GL}$ inference - we permute the proof as follows:

$$\dfrac{\dfrac{B, B, \Gamma, \Box C \Rightarrow C}{\Box B, \Box B, \Box\Gamma, \Pi \Rightarrow \Box C, \Sigma}\Box_{GL}}{\Box B, \Box\Gamma, \Pi \Rightarrow \Box C, \Sigma}\text{contr-l} \quad \Longrightarrow \quad \dfrac{\dfrac{B, B, \Gamma \Rightarrow C}{B, \Gamma, \Box C \Rightarrow C}\text{contr-l}}{\Box B, \Box\Gamma, \Pi \Rightarrow \Box C, \Sigma}\Box_{GL}$$

The permutation is obviously height preserving. QED

Lemma 2.3.7. *Weakening rules are height-preserving admissible in Gm_{Grz}.*

PROOF OF LEMMA 2.3.7. As before, the argument is similar as used in 2.2.9, we only state the modal step here. Weak-r is again built in the modal rule.

Weak-l by $\Box A$, the last step is a $\Box_{Grz}$ inference:

$$\dfrac{\dfrac{\Box\Gamma, \Gamma, \Box(B \to \Box B) \Rightarrow B}{\Box A, A, \Box\Gamma, \Gamma, \Box(B \to \Box B) \Rightarrow B}\text{weak-l}}{\Box A, \Box\Gamma, \Pi \Rightarrow \Box B, \Lambda}\Box_{Grz}$$

QED

Also contraction rules are height-preserving admissible in Gm_{Grz}, but we do not use this fact here.

Lemma 2.3.8. *Weakening rules are admissible in Gm^+_{Grz}.*

PROOF OF LEMMA 2.3.8. The three weakening rules are that of Lemma 2.2.9 and also the proof is fully analogous to that of Lemma 2.2.9, the same reason why this is not height-preserving admissibility applies here. QED

Lemma 2.3.9. *Contraction rules are height-preserving admissible in Gm^+_{Grz}.*

PROOF OF LEMMA 2.3.9. The three contraction rules are that of Lemma 2.2.10 and the proof is fully analogous. We only include the steps for the boxed contraction formula: (see (i), (ii), and (iii) of Lemma 2.2.10).
(ia) The contraction formula is the principal formula of a $\Box^+_{Grz1}$ inference in the antecedent. Then we permute the proof as follows using the i.h.:

$$\dfrac{\dfrac{\Box\Gamma, \Box B, \Box B, \Box(C \to \Box C)|B, B, \Gamma \Rightarrow C}{\Box B, \Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\Box^+_{Grz1}}{\Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\text{contr-l+}$$

$$\dfrac{\dfrac{\Box\Gamma, \Box B, \Box B, \Box(C \to \Box C)|B, B, \Gamma \Rightarrow C}{\Box\Gamma, \Box B, \Box(C \to \Box C)|B, \Gamma \Rightarrow C}\text{contr-l, contr-l+}}{\Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\Box^+_{Grz1}$$

The permutation is obviously height preserving.
(ib)The contraction formula is the principal formula of a $\Box^+_{Grz2}$ inference in the antecedent. Then we permute the proof as follows using the i.h.:

$$\cfrac{\cfrac{\Box B, \Box B, \Box\Gamma|\emptyset \Rightarrow C}{\Box B, \Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\ \Box^+_{Grz2}}{\Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\ \text{contr-l+}$$

$$\cfrac{\cfrac{\Box B, \Box B, \Box\Gamma|\emptyset \Rightarrow C}{\Box\Gamma, \Box B|\emptyset \Rightarrow C}\ \text{contr-l+}}{\Box B, \Box\Gamma|\Pi \Rightarrow \Box C, \Sigma}\ \Box^+_{Grz2}$$

The permutation is obviously height preserving.
(ii) The contraction formula is the principal formula of a $\Box^+_T$ inference in the antecedent. (ii) of Lemma 2.2.10 applies here.
(iii) The contraction formula is the principal formula in the succedent. Then we use the appropriate $\Box^+_{Grz}$ rule so that the conclusion is not weakened by the other occurrence of $\Box B$. This step is obviously height preserving.

QED

Lemma 2.3.10. *The calculi Gm_{Grz} and Gm^+_{Grz} are equivalent:*

$$\vdash_{Gm_{Grz}} \Gamma \Rightarrow \Delta \quad \textit{iff} \quad \vdash_{Gm^+_{Grz}} \emptyset|\Gamma \Rightarrow \Delta.$$

Proof of Lemma 2.3.10. The right-left implication: deleting the "|" symbol from a Gm^+_{Grz} proof of $(\emptyset|\Gamma \Rightarrow \Delta)$ yields correct instances of rules of Gm_{Grz}, except the $\Box^+_{Grz2}$ rule. It has to be treated as follows:

$$\cfrac{\cfrac{\Box\Gamma, \Box(A \to \Box A) \Rightarrow A}{\Box\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \Box_{Grz}}{\Box\Gamma, \Box(A \to \Box A), \Pi \Rightarrow \Box A, \Delta}\ \text{admiss. weak.}$$

We end up with a Gm_{Grz} proof of $\Gamma \Rightarrow \Delta$.

The left-right implication: The classical rules and the $\Box_T$ rule are treated as in Lemma 2.2.13.

The $\Box_{Grz}$ rule is simulated as follows ($(A \to \Box A) \leftrightarrow (\neg A \vee \Box A)$ and $(A \to \Box A) \notin \Gamma$):

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\emptyset|\Box\Gamma, \Box(\neg A \vee \Box A) \Rightarrow A}{\Box\Gamma, \Box(\neg A \vee \Box A)|\Gamma, \neg A \vee \Box A \Rightarrow A}\ \textit{inv. of } \Box^+_T}{\Box\Gamma, \Box(\neg A \vee \Box A)|\Gamma \Rightarrow A, A}\ \text{inv. of } \vee\text{-l and } \neg\text{-l}}{\Box\Gamma, \Box(\neg A \vee \Box A)|\Gamma \Rightarrow A}\ \text{admiss. contr-r}}{\Box\Gamma|\Pi \Rightarrow \Box A, \Delta}\ \Box^+_{Grz1}}{\Box\Gamma|\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \text{admiss. weak-l inferences}}{\emptyset|\Box\Gamma, \Pi \Rightarrow \Box A, \Delta}\ \Box^+_T \text{ inferences}$$

If $(A \to \Box A) \in \Gamma$, we use some admissible contr-r+ inferences before the $\Box^{+}_{Grz1}$ inference is used.

QED

Cut admissibility

We state a semantic argument of cut admissibility here - it proofs that the calculi Gm_{GL} and Gm_{Grz} are complete without the cut rule w.r.t. Kripke semantics. Then an easy semantic argument of soundness of the cut rule entails its admissibility.

Lemma 2.3.10 then yields admissibility of the appropriate cut rule in Gm^{+}_{Grz} which is used in the proof of Theorem 3.5.1.

For proofs you may see also [1] for **GL** and Grzegorczyk's logic, and [53] or [46] for **GL** where redundancy of the cut rule is established through a decision procedure which either creates a cut-free proof or a Kripke counterexample to a given sequent.

Although they use a formulation via sets of formulas, observe, that a cut-free proof with sets can be equivalently formulated using multisets and contraction rules, which are, as we have proved, admissible in our cut-free calculi. Equivalently, if a sequent does not have a cut-free proof in the system based on multisets, its set-based counterpart sequent does not have a cut-free proof in the system based on sets.

Lemma 2.3.11. *(Avron [1]:) There are a canonical Kripke model* $(W, <)$ *and a canonical valuation* V *such that:*

- $<$ *is irreflexive and transitive*
- *for every* $w \in W$*, the set* $\{v | v < w\}$ *is finite*
- *if* $(\Gamma \Rightarrow \Delta)$ *has no cut-free proof in* Gm_{GL}*, then there is a* $w \in W$ *such that* $w \Vdash_V A$ *for every* $A \in \Gamma$ *and* $w \nVdash_V B$ *for every* $B \in \Delta$.

There are a canonical Kripke model $(W, \leq)$ *and a canonical valuation* V *such that:*

- $\leq$ *partially orders* W
- *for every* $w \in W$*, the set* $\{v | v \leq w\}$ *is finite*
- *if* $(\Gamma \Rightarrow \Delta)$ *has no cut-free proof in* Gm_{Grz}*, then there is a* $w \in W$ *such that* $w \Vdash_V A$ *for every* $A \in \Gamma$ *and* $w \nVdash_V B$ *for every* $B \in \Delta$.

PROOF OF LEMMA 2.3.11. See [1]. The canonical model is built from all saturated sequents (closed under subformulas) that have no cut-free proof in appropriate calculi.

The lemma entails completeness of Gm_{GL} w.r.t. transitive, well-founded Kripke models; and completeness of Gm_{Grz} w.r.t. transitive, reflexive and well-founded Kripke models.

QED

Corollary 2.3.12. *The cut rule*

$$\frac{\Gamma \Rightarrow \Delta, C \qquad C, \Pi \Rightarrow \Lambda}{\Gamma, \Pi \Rightarrow \Delta, \Lambda}$$

is admissible in Gm_{GL} and Gm_{Grz}.

PROOF OF COR. 2.3.12. It is easy to give a semantic argument of soundness of the cut rule. Given a counterexample of the conclusion $(\Gamma, \Pi \Rightarrow \Delta, \Lambda)$ of a cut inference, there is a counterexample to one of its premisses: consider the counterexample (W,R) and a world $w \in W$ in it such that $w \Vdash_V A$ for every $A \in \Gamma \cup \Pi$ and $w \nVdash_V B$ for some $B \in \Delta \cup \Lambda$. For any formula C it is either the case that $w \Vdash_V C$, and then w refutes $(C, \Pi \Rightarrow \Lambda)$, or $w \nVdash_V C$, and then w refutes $(\Gamma \Rightarrow \Delta, C)$.

Now Lemma 2.3.11 (completeness of Gm_{GL} and Gm_{Grz}) entails admissibility of the cut rule in the calculi. QED

Corollary 2.3.13. *The cut rule*

$$\frac{\emptyset | \Gamma \Rightarrow \Delta, C \qquad \emptyset | C, \Pi \Rightarrow \Lambda}{\emptyset | \Gamma, \Pi \Rightarrow \Delta, \Lambda}$$

is admissible in Gm^{+}_{Grz}.

PROOF OF COR. 2.3.13. Follows from Corollary 2.3.12 and Lemma 2.3.10. QED

Chapter 3

Uniform Interpolation

In this chapter we concentrate on the stronger from the two Craig interpolation properties - the uniform interpolation property. We shall prove uniform interpolation for modal propositional logics **K**, **T**, **GL**, **S4Grz**.

The uniform interpolation property for a propositional logic is a strengthening of the Craig interpolation property. It states that for every formula A and any choice of propositional variables $\bar{q}$, there is a post-interpolant $I_{postA}(\bar{q})$ depending only on A and $\bar{q}$ such that for all B, whenever $(A \to B)$ is provable and the shared variables of A and B are among $\bar{q}$, $(A \to I_{postA}(\bar{q}))$ and $(I_{postA}(\bar{q}) \to B)$ are provable. Similarly there is a pre-interpolant: for every formula B and any choice of propositional variables $\bar{r}$ there is a formula $I_{preB}(\bar{r})$ depending only on B and $\bar{r}$ such that for all A, whenever $(A \to B)$ is provable and the shared variables of A and B are among $\bar{r}$, then $(I_{preB}(\bar{r}) \to B)$ and $(A \to I_{preB}(\bar{r}))$ are provable.

Uniform interpolants are unique up to the provable equivalence. Concerning Craig interpolation this means that every implication has the minimal and the maximal interpolants w.r.t. the provability ordering.

It was proved in Wolter [55] that uniform interpolation is preserved under fusion of modal logics.

The task of proving uniform interpolation is easy when dealing with logics satisfying *local tabularity* [13], which means that there is only *finitely* many nonequivalent formulas for each finite number of propositional variables. If a logic satisfies both local tabularity and Craig then the conjunction of all formulas $I(\bar{q})$ implied by $A(\bar{p}, \bar{q})$ is the post-interpolant of A, and the disjunction of all formulas $J(\bar{r})$ implying $B(\bar{r}, \bar{s})$ is the pre-interpolant of B. This simple argument works e.g. in the case of classical propositional logic or modal logic **S5**, while it is not the case of modal logics **K**, **T**, **K4**, **S4**.

Uniform interpolation can also be proved via a simulation (or equivalently an elimination) of certain propositional quantifiers. If we can simulate propositional quantification satisfying usual reasonable properties given e.g. by usual quantifier axioms and rules then the simulations of $\exists\bar{p}A$ and $\forall\bar{r}B$ are the post-interpolant of $A(\bar{p},\bar{q})$ and the pre-interpolant of $B(\bar{q},\bar{r})$ respectively.

The main point is that even if the logic does not satisfy local tabularity we can still keep the information "to be the uniform interpolant" *finite* and thus represented by a single formula (a conjunction in the case of the existential quantifier or a disjunction in the case of the universal quantifier).

Visser's semantic proof of uniform interpolation yields a semantic characterization of the simulated so-called *bisimulation* quantifiers: from the semantic point of view, quantifying over p, we quantify over possible worlds that bisimulate w.r.t. all propositional variables other then p. Also a complexity bound of uniform interpolants in terms of $\Box$-depth is obtained in the proof. However, the proof does not provide us with a construction of the interpolants. (For more on bisimulation see [52].)

There is a proof of uniform interpolation for **K** in Kracht's book [28] which uses as a crucial fact the completeness of **K** w.r.t. finite irreflexive trees.

In this chapter, we apply a proof-theoretic method which was introduced by Pitts in [39] to modal propositional logics. The argument is based on a simulation of propositional quantifiers in the framework of an analytic sequent proof system. The main point of keeping the information "to be the uniform interpolant" finite and thus represented by a single formula is in a use of a terminating sequent proof system, i.e., a proof system in which any backward proof-search terminates. The method provides an explicit effective (and also easily implementable) construction of uniform interpolants.

Concerning proof-theoretic approach to proofs of interpolation the situation is as follows - as Craig interpolation relates to cut-free proofs, uniform interpolation relates to terminating proof-search trees. Proving Craig interpolation, we start with a cut-free proof of an implication (a sequent) and construct an interpolant inductively from the proof. Proving uniform interpolation, we start with a proof-search tree for a formula (we search for all proofs in which the formula can occur in the appropriate context. So it is rather a finite proof-search subtree what we use here.) Here termination of the calculus is crucial, but we need even a bit more to prove that our procedure terminates. A uniform interpolant is then the formula corresponding to such a tree.

The relatively easy case of modal logics **K** and **T** (contained in sections 3.2, 3.3) has been already treated by the author in [3], we have just slightly changed technical details of the proof. We have extended our study to logics having arithmetical interpretations - **GL** and **S4Grz**.

The chapter 3 is organized as follows:

- Section 3.1: we show that uniform interpolation fails for modal logic **K4**. This follows immediately from the failure of uniform interpolation in modal logic **S4** proved by Ghilardi and Zawadowski in [20].

- Section 3.2: we prove the main technical theorem 3.2.1 providing us with an explicit algorithm which for a sequent $(\Gamma \Rightarrow \Delta)$ constructs a formula $A_p(\Gamma; \Delta)$ to simulate universal quantification over p in **K**. In subsection 3.2, just before the proof of Theorem 3.2.1, we have put an overview of the proof method.

  - Subsection 3.2.1: we introduce second order $\mathbf{K}^2$ extending **K** by propositional quantification and prove that **K** simulates $\mathbf{K}^2$ using a translation based on the formula A_p constructed in the proof of Theorem 3.2.1.

  - Subsection 3.2.2: we state the uniform interpolation theorem - Corollary 3.2.6 - and show that it follows from the fact that **K** simulates $\mathbf{K}^2$ which already satisfies uniform interpolation. We also show that we have in fact constructed the interpolants proving Theorem 3.2.1 since they are nothing else then quantified formulas.

  The simple case of **K** is intended as a basic step, analogues of Theorem 3.2.1 are to be proved for all the other logics using the same method and also analogues of the corollaries can be obtained for all the other logics.

- Section 3.3: we prove the main technical theorem 3.3.1 for logic **T**. The proof is analogous to that for **K**, a difference is that it makes use of a sequent calculus that includes a built in loop-preventing mechanism to enforce its termination. It is still relatively simple and can be seen as a basic step for reflexive modal logics.

- Section 3.4: we prove the main technical theorem 3.4.1 for logic **GL**. The proof is much like that for **K**, the main complication here is to prevent looping of our construction caused by the fact that we deal with a transitive logic.

  - Subsection 3.4.1: we show that the uniform interpolation theorem provides us with a constructive proof of the fixed point theorem.

- Section 3.5: we prove the main technical theorem 3.5.1 for logic **S4Grz**. This time the proof is much like that for **T** since **S4Grz** extends **T**. The same complication with looping as above in the case of **GL** is treated analogously here.

3.1 Logic K4

Since our aim of further work is to investigate uniform interpolation in provability logics **GL** and **S4Grz** which extend modal logic **K4** let us briefly discuss the failure of uniform interpolation in **K4**.

It is known that modal logic **S4** does not have the uniform interpolation property. A counterexample was provided by Ghilardi and Zawadowski in [20].

Using the following translation from **S4** to **K4** and the fact that **K4** is a subsystem of **S4** we conclude that **K4** does not have the uniform interpolation either. Although it is an easy observation, we include it here since as far as we know it is not mentioned in the literature.

Definition 3.1.1. Translation $A^\star$ of a modal formula A:

- $p^\star = p$
- $(A \circ B)^\star = A^\star \circ B^\star$
- $(\Box A)^\star = \Box A^\star \wedge A^\star$, i.e., $(\Box A)^\star = \boxdot A^\star$

Lemma 3.1.2. *[8]*

$$\vdash_{H_{S4}} A \quad \text{iff} \quad \vdash_{H_{K4}} A^\star$$

$$\vdash_{H_{S4}} A \leftrightarrow A^\star$$

Lemma 3.1.3. *[20] There is a modal formula $B(p_1, p_2, q)$ which does not have a uniform post-interpolant $I_{postB}(p_1, p_2)$ in **S4**, i.e., there is no formula $I_{postB}(p_1, p_2)$ satisfying*

- $\vdash_{H_{S4}} B \to I_{postB}$
- *for all $C(p_1, p_2, \overline{r})$ such that $\vdash_{H_{S4}} B \to C$, $\vdash_{H_{S4}} I_{postB} \to C$*

The counterexample provided in [20] is :

$$B \equiv p_1 \wedge \Box(p_1 \to \Diamond p_2) \wedge \Box(p_2 \to \Diamond p_1) \wedge \Box(p_1 \to q) \wedge \Box(p_2 \to \neg q)$$

There is no formula simulating $\exists p_1 \exists p_2 B$. It follows that B cannot have a uniform post-interpolant. See also [52].

Corollary 3.1.4. *There is a modal formula which does not have a uniform post-interpolant in **K4**.*

PROOF OF COROLLARY 3.1.4. Consider the **S4** counterexample $B(p_1, p_2, q)$. Consider for the contradiction that **K4** does have the uniform interpolation property. This means that for $B^\star$, there is a formula $I_{postB^\star}(p_1, p_2)$ such that $\vdash_{H_{K4}} B^\star \rightarrow I_{postB^\star}$ and for all $C(p_1, p_2, \overline{r})$ we have that $\vdash_{H_{K4}} B^\star \rightarrow C$ implies $\vdash_{H_{K4}} I_{postB^\star} \rightarrow C$. Then we have the same for all $C^\star$ of the form of a translation of a formula C. Moreover by the fact that $\vdash_{H_{K4}} A$ implies $\vdash_{H_{S4}} A$ and that $\vdash_{H_{S4}} A \leftrightarrow A^\star$ we obtain $\vdash_{H_{S4}} B \rightarrow I_{postB^\star}$.

Using the property of the translation $\vdash_{H_{S4}} A$ iff $\vdash_{H_{K4}} A^\star$, and again the fact that $\vdash_{H_{K4}} A$ implies $\vdash_{H_{S4}} A$, and that $\vdash_{H_{S4}} A \leftrightarrow A^\star$, yields the following: for all C, $\vdash_{H_{S4}} B \rightarrow C$ implies $\vdash_{H_{S4}} I_{postB^\star} \rightarrow C$. But then we have obtained the uniform interpolant for B in **S4** which is the desired contradiction. QED

3.2 Logic K

Our main technical result is the following theorem. Its proof provides us with an explicit algorithm which for a sequent $(\Gamma \Rightarrow \Delta)$ constructs a formula $A_p(\Gamma; \Delta)$ to simulate universal quantification over p. The formula $\forall p B(p, \bar{q})$ (or equivalently the preinterpolant $I_{preB}(\bar{q})$) is to be simulated by $A_p(\emptyset; B)$. To do the job, the formula $A_p(\Gamma; \Delta)$ has to satisfy (i)-(iii) of the following theorem which can bee seen as analogues of an axiom of specification and a generalization rule:

Theorem 3.2.1. *Let Γ, Δ be finite multisets of formulas. For every propositional variable p there exists a formula $A_p(\Gamma; \Delta)$ such that:*

- *(i)*
$$Var(A_p(\Gamma; \Delta)) \subseteq Var(\Gamma, \Delta) \backslash \{p\}$$
- *(ii)*
$$\vdash_{Gm_K} \Gamma, A_p(\Gamma; \Delta) \Rightarrow \Delta$$
- *(iii) moreover let Π, Σ be multisets of formulas not containing p and $\vdash_{Gm_K} \Pi, \Gamma \Rightarrow \Lambda, \Delta$. Then*
$$\vdash_{Gm_K} \Pi \Rightarrow A_p(\Gamma; \Delta), \Lambda.$$

We define a formula $A_p(\Gamma; \Delta)$ inductively on the weight of the multiset (Γ, Δ) as described in the following table. In the line 2, q and r are any propositional variables other than p, and Φ and Ψ are multisets containing only propositional variables. Moreover we require that at least one of the multisets $\Gamma', \Delta', \Phi, \Psi$ is nonempty in the line 2, so that $\emptyset, \emptyset$ does not match the line (to prevent looping).

The formula $A_p(\Gamma; \Delta)$ is defined recursively to equal $\bigwedge_{(\Theta \Rightarrow \Xi) \in Cl(\Gamma; \Delta)} A_p(\Theta; \Xi)$.

The recursive steps for the critical sequents are given by the following table:

	$\Box\Gamma', \Phi; \Box\Delta', \Psi$ matches	$A_p(\Box\Gamma', \Phi; \Box\Delta', \Psi)$ equals
1	if $p \in \Phi \cap \Psi$	$\top$
2	otherwise	$\bigvee_{q\in\Psi} q \bigvee_{r\in\Phi} \neg r$ $\bigvee_{B\in\Delta'} \Box A_p(\Gamma'; B)$ $\vee \Diamond A_p(\Gamma'; \emptyset)$

$A_p(\Gamma; \Delta)$ where $\Gamma; \Delta$ does not match any line of the table is defined to equal $\bot$. (In particular, $A_p(\emptyset; \emptyset) \equiv \bot$.)

Consider for example $A_p(\Box(p \wedge q); \Box p)$. It matches the line 2 and thus we obtain $\Box A_p(p \wedge q; p) \vee \Diamond A_p(p \wedge q; \emptyset)$. This yields $\Box A_p(p, q; p) \vee \Diamond A_p(p, q; \emptyset)$ by the closure, and then, using lines 1 and 2, $\Box(\neg q \vee \top) \vee \Diamond\neg q$. We have obtained $A_p(\Box(p \wedge q); \Box p) \equiv \Diamond\neg q \vee \Box(\neg q \vee \top)$, which is provably equivalent to $\top$.

Overview of the proof method We are to construct, for a given sequent $(\Gamma; \Delta)$, a formula satisfying (i)-(iii) of Theorem 3.2.1. It is much like to write down the appropriate proof-search tree for the sequent $(\Gamma; \Delta)$: first we close under the invertible rules and define $A_p(\Gamma; \Delta)$ to equal $\bigwedge_{(\Theta \Rightarrow \Xi) \in Cl(\Gamma; \Delta)} A_p(\Theta; \Xi)$ (this corresponds to conjunctive branching of the proof-search tree on classical inferences). Then, for a critical sequent, we test whether $p \in \Phi \cap \Psi$. If so, the sequent is initial and we end up with $\top$ (the case there is another variable then p in $\Phi \cap \Psi$ is included in the following modal jump). Otherwise we apply a modal jump (which corresponds to disjunctive branching of the proof-search tree on a modal jump): we write down a disjunction of all variables other then p from Ψ, a disjunction of all negated variables other then p from Φ, a disjunction of $\Box A_p$ of all possible predecessors - premisses of a $\Box_K$ inference, and one more disjunct starting with $\Diamond$. This one is included to prove, in the part (iii) of the theorem which is done by induction on the height of a proof of $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$, the step for a $\Box_K$ inference with the principal formula not containing p. To be more precise, what we are doing here is, rather then a proof-search for $(\Gamma; \Delta)$, a part of a proof-search for any sequent extending $(\Gamma; \Delta)$ by contexts not containing p. This main idea is common to all the modal logics we consider in the thesis.

PROOF OF THEOREM 3.2.1. The definition of $A_p(\Gamma; \Delta)$ runs inductively on the weight of Γ, Δ. Note that recursively called arguments of A_p are strictly less in terms of the weight function then the corresponding match of $(\Gamma; \Delta)$. For a noncritical sequent it is a property of the closure, for a critical sequent it is clear from the table.

Thus our definition always terminates.

(i) follows easily by induction on Γ, Δ just because we never add p during the definition of the formula $A_p(\Gamma; \Delta)$.

(ii) We proceed by induction on the weight of Γ, Δ. We prove that

$$\vdash_{Gm_K} \Gamma, A_p(\Gamma; \Delta) \Rightarrow \Delta.$$

Let $(\Gamma \Rightarrow \Delta)$ be a noncritical sequent. Then sequents $(\Theta_i \Rightarrow \Xi_i) \in Cl(\Gamma; \Delta)$ are of lower weight. By the induction hypothesis

$$\vdash_{Gm_K} \Theta_i, A_p(\Theta_i; \Xi_i) \Rightarrow \Xi_i \quad \text{for each i.}$$

Then by admissibility of weakening and by Lemma 2.3.5

$$\vdash_{Gm_K} \Gamma, A_p(\Theta_1; \Xi_1), \ldots, A_p(\Theta_k; \Xi_k) \Rightarrow \Delta,$$

and so

$$\vdash_{Gm_K} \Gamma, \bigwedge_{(\Theta_i \Rightarrow \Xi_i) \in Cl(\Gamma;\Delta)} A_p(\Theta_i; \Xi_i) \Rightarrow \Delta,$$

which is

$$\vdash_{Gm_K} \Gamma, A_p(\Gamma; \Delta) \Rightarrow \Delta.$$

Let $(\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 1. Then (ii) is an initial sequent.

Let $(\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 2.

- for each $B \in \Delta'$, we have $\vdash_{Gm_K} \Gamma', A_p(\Gamma'; B) \Rightarrow B$ by the i.h., which gives $\vdash_{Gm_K} \Box\Gamma', \Phi, \Box A_p(\Gamma'; B) \Rightarrow \Box B, \Box\Delta'', \Psi$ by a $\Box_K$ inference.
- by the i.h. we also have $\vdash_{Gm_K} \Gamma', A_p(\Gamma'; \emptyset) \Rightarrow \emptyset$, which gives, using negation rules and the $\Box_K$ rule, $\vdash_{Gm_K} \Box\Gamma', \Phi, \Diamond A_p(\Gamma'; B) \Rightarrow \Box\Delta', \Psi$.
- for each $r \in \Phi$ obviously $\vdash_{Gm_K} \Phi, \neg r, \Box\Gamma' \Rightarrow \Box\Delta', \Psi$.
- for each $q \in \Psi$ obviously $\vdash_{Gm_K} \Phi, q, \Box\Gamma' \Rightarrow \Box\Delta', \Psi$.

Together this yields, using $\vee$-l inferences,

$$\vdash_{Gm_K} \Phi, \Box\Gamma', \bigvee_{q \in \Psi} q \bigvee_{r \in \Phi} \neg r \bigvee_{B \in \Delta'} \Box A_p(\Gamma'; B) \vee \Diamond A_p(\Gamma'; \emptyset) \Rightarrow \Box\Delta', \Psi,$$

that is, by the line 2, $\vdash_{Gm_K} \Phi, \Box\Gamma', A_p(\Phi, \Box\Gamma'; \Box\Delta', \Psi) \Rightarrow \Box\Delta', \Psi$.

(iii) We proced by induction on the height of a proof of $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$. We can restrict ourselves to initial sequents and critical steps (a $\Box_K$ inferences). Let us see first that for classical (invertible) parts of the proof the task reduces to appropriate critical sequents:

Let the last inference of the proof of $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ be a classical inference. Then $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is not a critical sequent and for all $(\Theta \Rightarrow \Xi) \in Cl(\Gamma; \Delta)$ we have $\vdash_{Gm_K} \Pi, \Theta \Rightarrow \Xi, \Lambda$ by 2.3.5. Then the following are equivalent:

$$\vdash_{Gm_K} \Pi \Rightarrow A_p(\Theta; \Xi), \Lambda \quad \text{for all} \quad (\Theta \Rightarrow \Xi) \in Cl(\Gamma; \Delta).$$

$$\vdash_{Gm_K} \Pi \Rightarrow \bigwedge_{(\Theta \Rightarrow \Xi) \in Cl(\Gamma;\Delta)} A_p(\Theta; \Xi), \Lambda$$

$$\vdash_{Gm_K} \Pi \Rightarrow A_p(\Gamma; \Delta), \Lambda.$$

So let us consider then the last step of the proof of $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is an initial sequent.

Then $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is an axiom, say $(\Sigma, r \Rightarrow r, \Theta)$. We distinguish two cases - either $r \equiv p$ or not:

- $r \equiv p$: then $p \in \Gamma \cap \Delta$, which means that $A_p(\Gamma; \Delta) \equiv \top$ and since obviously $\vdash_{Gm_K} \Pi \Rightarrow \top, \Lambda$, we obtain (iii).
- $r \not\equiv p$: there are four cases:
  - $r \in \Pi \cap \Lambda$, then (iii) is an axiom.
  - $r \in \Pi \cap \Delta$ then the line 2 gives by invertibility of the $\vee$-l rule
  $$\vdash_{Gm_K} r \Rightarrow A_p(\Gamma; r, \Delta').$$
  - $r \in \Gamma \cap \Lambda$ then the line 2 gives by invertibility of the $\vee$-l rule
  $$\vdash_{Gm_K} \neg r \Rightarrow A_p(\Gamma'; r, \Delta).$$
  - $r \in \Gamma \cap \Delta$ then the line 2 gives by invertibility of the $\vee$-l rule
  $$\vdash_{Gm_K} r \vee \neg r \Rightarrow A_p(\Gamma; \Delta),$$
  and so by cut admissibility
  $$\vdash_{Gm_K} \emptyset \Rightarrow A_p(\Gamma; \Delta).$$

  In all the three cases above admissibility of the weakening rule yields what is required.

To treat the case of an axiom of the form $(\bot \Rightarrow \Theta)$ we use the line 1 of the table similarly.

For the remaining case let us consider that the last inference is a $\Box_K$ inference:

Consider the principal formula $\Box A \in \Lambda$ first, i.e. A doesn't contain p. Then the proof ends with:

$$\frac{\Pi', \Gamma' \Rightarrow A}{\Box\Pi', \Box\Gamma', \Pi'', \Gamma'' \Rightarrow \Box A, \Lambda', \Delta}$$

where $\Box\Pi', \Pi''$ is Π; $\Box\Gamma', \Gamma''$ is Γ; and $\Box A, \Lambda'$ is Λ.

Then the induction hypothesis gives

$$\vdash_{Gm_K} \Pi' \Rightarrow A_p(\Gamma'; \emptyset), A$$

and by a $\neg$-l inference we obtain

$$\vdash_{Gm_K} \Pi', \neg A_p(\Gamma'; \emptyset) \Rightarrow A.$$

Now, by a $\Box_K$ and a negation inference, we obtain

$$\vdash_{Gm_K} \Box\Pi', \Pi'' \Rightarrow \Diamond A_p(\Gamma'; \emptyset), \Box A, \Lambda'.$$

By the line 2 of the table and invertibility of the $\vee$-l rule we have

$$\vdash_{Gm_K} \Diamond A_p(\Gamma'; \emptyset) \Rightarrow A_p(\Box\Gamma', \Gamma''; \Delta).$$

The two sequents above yield (iii) by cut admissibility.

Consider the principal formula $\Box A \in \Delta$. Then the proof ends with:

$$\frac{\Pi', \Gamma' \Rightarrow A}{\Box\Pi', \Box\Gamma', \Pi'', \Gamma'' \Rightarrow \Box A, \Delta', \Lambda}$$

where $\Box\Pi', \Pi''$ is Π; $\Box\Gamma', \Gamma''$ is Γ; and $\Box A, \Delta'$ is Δ.

Now the induction hypothesis gives

$$\vdash_{Gm_K} \Pi' \Rightarrow A_p(\Gamma'; A)$$

and by a $\Box_K$ inference we obtain

$$\vdash_{Gm_K} \Box\Pi', \Pi'' \Rightarrow \Box A_p(\Gamma'; A), \Lambda.$$

The line 2 of the table and invertibility of the $\vee$-l rule yields

$$\vdash_{Gm_K} \Box A_p(\Gamma'; A) \Rightarrow A_p(\Box\Gamma', \Gamma''; \Box A, \Delta').$$

We obtain (iii) again by cut admissibility. QED

The following two subsections capture the connection between propositional quantifiers and uniform interpolants. We state and prove the results for the basic case of **K**, however, analogues of them apply for all the other logics as well by similar proofs.

3.2.1 Propositional quantifiers

Propositional quantifiers are usually introduced via their semantical meaning. In the framework of Kripke semantics they are defined as ranging over propositions, i.e., sets of possible worlds. This definition is used in Fine [16], see also Bull [9] and Kremer [32]. The second order modal systems over logics **K**, **T**, **K4**, **S4** obtained this way are recursively isomorphic to full second order classical logic. This was proved independently by Fine and Kripke shortly after Fine's paper [16] was published, as Kremer remarked in [32]. Also Kremer's strategy from [31] can be extended to prove the same result, as he claims in [32]. In particular it means that these systems are undecidable while their propositional counterparts are decidable.

Another way of defining quantified propositional logic is extending a proof system of the propositional logic we deal with by new axioms and analogues of usual quantifier rules. This approach was applied e.g. in Bull's paper [9], or in [39] in the case of intuitionistic logic. Bull in [9] proved completeness of such second order calculi over S4 and S5 w.r.t. Kripke semantics. This sort of proof is analogous to standard completeness proofs in first order predicate modal logics. It can also be given for second order $\mathbf{K}^2$ and $\mathbf{T}^2$ considered here but it is outside of the scope of this paper. The difference is that Bull doesn't allow quantifiers to range over *all* subsets of possible worlds but only over those given by validating some formula. In this case we quantify over *substitutions*. These two possible semantical definitions are different and do not seem to yield systems of the same complexity.

We adopt the syntactical approach and define quantified propositional modal logic $\mathbf{K}^2$ as follows. Consider the following sequent calculus Gm_{K^2}:

Definition 3.2.2. Sequent calculus Gm_{K^2} results from extending Gm_K by structural rules, an initial sequent

$$\forall p \Box A \Rightarrow \Box \forall p A,$$

and two quantifier rules:

$$\frac{\Gamma, A[p/B] \Rightarrow \Delta}{\Gamma, \forall p A \Rightarrow \Delta}\ \forall\text{-l} \qquad \frac{\Gamma \Rightarrow A, \Delta}{\Gamma \Rightarrow \forall p A, \Delta}\ \forall\text{-r},\ p \text{ not free in } \Gamma, \Delta$$

The added axiom represents the propositional version of the *Barcan formula.* Note that its converse is easily provable in the calculus using the quantifier rules.

The desirability of Barcan formula is usually discussed in first order predicate modal logics where it relates to the question whether there is a constant domain in all possible worlds or not. Since it is certainly the case here because we have a constant set of propositional variables we include this scheme to our calculus.

The calculus as defined here does not have nice structural properties but is transparent and suffices to capture the semantical meaning of $\mathbf{K}^2$ quantifiers in means of

Bull's paper. If we want to do without cut (if it is at all possible), we should include the Barcan formula another way.

To simulate propositional quantifiers of Gm_{K^2} in Gm_K we define the following translation A^* of a second order modal formula A:

- $p^* := p$
- $(C \circ B)^* := C^* \circ B^*$
- $(\neg C)^* := \neg C^*$
- $(\Box B)^* := \Box(B^*)$
- $(\forall p C)^* := A_p(C^*)$

Observe that for a quantifier-free formula B, $B^* = B$ holds.

Now let us see that our Theorem 3.2.1 yields the desired simulation of propositional quantifiers.

Corollary 3.2.3. *Let C be a modal formula and Γ, Δ multisets of formulas not containing p. There is a formula $A_p(C)$ such that:*
(i) $\vdash_{Gm_K} \Gamma \Rightarrow C, \Delta$ implies $\vdash_{Gm_K} \Gamma \Rightarrow A_p(C), \Delta$
(ii) $\vdash_{Gm_K} \Gamma \Rightarrow A_p(C), \Delta$ implies for all B, $\vdash_{Gm_K} \Gamma \Rightarrow C[p/B], \Delta$.

Proof of Corollary 3.2.3. We define $A_p(\Delta) = A_p(\emptyset; \Delta)$. The first part follows immediately from 3.2.1 (iii).

By 3.2.1 (ii) we have $A_p(C) \Rightarrow C$. As $A_p(C)$ does not contain p, we obtain $A_p(C) \Rightarrow C[p/B]$ by substitution, which yields the second part. QED

To obtain the desired simulation we moreover need our construction of A_p to commute with substitution:

Corollary 3.2.4. $\vdash_{Gm_K} A_p(C[q/B]) \Rightarrow (A_p(C))[q/B]$ *and* $\vdash_{Gm_K} (A_p(C))[q/B] \Rightarrow A_p(C[q/B])$, *where B doesn't contain p, q.*

Proof of Corollary 3.2.4. The first direction uses the following congruence property of modal logic **K**: $C[q/A] \leftrightarrow C[q/B]$ whenever $A \leftrightarrow B$.

By 3.2.1 (ii) we have that $A_p(C[q/B]) \Rightarrow C[q/B]$. Now by the congruence property we get $(q \leftrightarrow B), A_p(C[q/B]) \Rightarrow C$, and since the antecedent doesn't contain p also $(q \leftrightarrow B), A_p(C[q/B]) \Rightarrow A_p(C)$. Substituting $[q/B]$ it results $A_p(C[q/B]) \Rightarrow A_p(C)[q/B]$.

The other direction: by 3.2.1 (ii) we have $A_p(C) \Rightarrow C$. By substitution we get $(A_p(C))[q/B] \Rightarrow C[q/B]$ and since the antecedent doesn't contain p, we also get by 3.2.1 (iii) $(A_p(C))[q/B] \Rightarrow A_p(C[q/B])$. QED

Now we are ready to prove:

Corollary 3.2.5. *If* $\vdash_{Gm_{K^2}} \Gamma \Rightarrow \Delta$ *then* $\vdash_{Gm_K} \Gamma^* \Rightarrow \Delta^*$.

PROOF OF COROLLARY 3.2.5. By induction on the proof of $\Gamma \Rightarrow \Delta$ in Gm_{K^2} using Corollary 3.2.3 and Corollary 3.2.4.

As of the added initial sequent $\forall p \Box B \Rightarrow \Box \forall p B$, note that $A_p(\Box B)$ yields $\Box A_p(B)$ and thus $\vdash_{Gm_K} A_p(\Box B) \Rightarrow \Box A_p(B)$ can be easily proved form the line 6 of the table in 3.2.1. QED

The other direction cannot be obtained. An example of a schema valid on our simulated quantifiers in **K** and not valid on propositional quantifiers in $\mathbf{K}^2$ is the $\forall$ quantifier commuting with the $\Diamond$ modality:

$$(\Diamond \forall \bar{p} A)^* \leftrightarrow (\forall \bar{p} \Diamond A)^*,$$

which can be easily proved from the line 7 of the table in 3.2.1. The right-left implication can be seen not to hold in the second order case using Kripke semantics in means of Bull's paper [9], i.e., quantifying over substitutions.

3.2.2 Uniform interpolation

Corollary 3.2.6. ***K*** *has the uniform interpolation property: For any multisets of formulas* $\Gamma(\bar{p}, \bar{q})$ *and* $\Delta(\bar{p}, \bar{q})$ *and variables* $\bar{q}$ *there is a single formula* $I_{post\Gamma\Delta}(\bar{q})$ *such that*

- $\vdash_{Gm_K} \Gamma(\bar{p}, \bar{q}) \Rightarrow I_{post\Gamma\Delta}(\bar{q}), \Delta(\bar{p}, \bar{q})$
- *for any multisets of formulas* $\Pi(\bar{q}, \bar{r})$, $\Sigma(\bar{q}, \bar{r})$, *if* $\vdash_{Gm_K} \Gamma(\bar{p}, \bar{q}), \Pi(\bar{q}, \bar{r}) \Rightarrow \Delta(\bar{p}, \bar{q}), \Sigma(\bar{q}, \bar{r})$ *then* $\vdash_{Gm_K} \Pi(\bar{q}, \bar{r}), I_{post\Gamma\Delta}(\bar{q}) \Rightarrow \Sigma(\bar{q}, \bar{r})$.

For any multisets of formulas $\Pi(\bar{t}, \bar{u})$ *and* $\Sigma(\bar{t}, \bar{u})$ *and variables* $\bar{t}$ *there is a single formula* $I_{pre\Pi\Sigma}(\bar{t})$ *such that*

- $\vdash_{Gm_K} \Pi(\bar{t}, \bar{u}), I_{pre\Pi\Sigma}(\bar{t}) \Rightarrow \Sigma(\bar{t}, \bar{u})$
- *for any multisets of formulas* $\Gamma(\bar{s}, \bar{t})$, $\Delta(\bar{s}, \bar{t})$, *if* $\vdash_{Gm_K} \Pi(\bar{t}, \bar{u}), \Gamma(\bar{s}, \bar{t}) \Rightarrow \Sigma(\bar{t}, \bar{u}), \Delta(\bar{s}, \bar{t})$ *then* $\vdash_{Gm_K} \Gamma(\bar{s}, \bar{t}) \Rightarrow I_{pre\Pi\Sigma}(\bar{t}), \Delta(\bar{s}, \bar{t})$.

PROOF OF COROLLARY 3.2.6. The result follows immediately from Corollary 3.2.5 and the fact that $\mathbf{K}^2$ satisfies the uniform interpolation. It is easy to see that

$(\exists\bar{p}\neg(\bigwedge\Gamma \rightarrow \bigvee\Delta))^*$ and $(\forall\bar{r}(\bigwedge\Pi \rightarrow \bigvee\Sigma))^*$ are the interpolants $I_{post\Gamma\Delta}$ and $I_{pre\Pi\Sigma}$ respectively.

To see that we have in fact constructed the interpolants proving Theorem 3.2.1, observe that our construction of A_p works as well for more then one propositional variable p. We can construct $A_{\bar{p}}$ using the procedure for all $\bar{p}$ simultaneously.

Let us have $\Gamma(\bar{p},\bar{q}), \Delta(\bar{p},\bar{q})$. Theorem 3.2.1 yields the formula $\neg A_{\bar{p}}(\Gamma;\Delta)$ (constructed only from Γ,Δ and containing only the variables $\bar{q}$) such that from (ii) it follows:

$$\vdash_{Gm_K} \Gamma \Rightarrow \neg A_{\bar{p}}(\Gamma;\Delta), \Delta.$$

Let us have $\Gamma(\bar{p},\bar{q}), \Pi(\bar{q},\bar{r}) \Rightarrow \Delta(\bar{p},\bar{q}), \Sigma(\bar{q},\bar{r})$. From (iii) we get:

$$\vdash_{Gm_K} \Pi, \neg A_{\bar{p}}(\Gamma;\Delta) \Rightarrow \Sigma.$$

Let us have $\Pi(\bar{t},\bar{u}), \Sigma(\bar{t},\bar{u})$. Theorem 3.2.1 yields the formula $A_{\bar{u}}(\Pi;\Sigma)$ (constructed only from Π,Σ and containing only the variables $\bar{t}$) such that it follows from (ii):

$$\vdash_{Gm_K} \Pi, A_{\bar{u}}(\Pi;\Sigma) \Rightarrow \Sigma.$$

Let us have $\Pi(\bar{t},\bar{u}), \Gamma(\bar{s},\bar{t}) \Rightarrow \Sigma(\bar{t},\bar{u}), \Delta(\bar{s},\bar{t})$. From (iii) we get:

$$\vdash_{Gm_K} \Gamma \Rightarrow A_{\bar{u}}(\Pi;\Sigma), \Delta.$$

QED

3.3 Logic T

The following analogue of Theorem 3.2.1 holds for the calculus Gm_T^+:

Theorem 3.3.1. *Let Σ,Γ,Δ be finite multisets of formulas. For every propositional variable p there exists a formula $A_p(\Sigma|\Gamma;\Delta)$ such that:*

- *(i)*
$$Var(A_p(\Sigma|\Gamma;\Delta)) \subseteq Var(\Sigma,\Gamma,\Delta)\backslash\{p\}$$
- *(ii)*
$$\vdash_{Gm_T^+} \Sigma|\Gamma, A_p(\Sigma|\Gamma;\Delta) \Rightarrow \Delta$$
- *(iii) moreover let Π,Λ,Θ be multisets of formulas not containing p and $\vdash_{Gm_T^+}$ $\Theta,\Sigma|\Pi,\Gamma \Rightarrow \Lambda,\Delta$. Then*
$$\vdash_{Gm_T^+} \emptyset|\Theta,\Pi \Rightarrow A_p(\Sigma|\Gamma;\Delta),\Lambda.$$

We define a formula $A_p(\Sigma|\Gamma;\Delta)$ inductively as in 3.2.1, changing the table as follows.

The formula $A_p(\Gamma;\Delta)$ is defined recursively to equal $\bigwedge_{(\Theta\Rightarrow\Xi)\in Cl(\Gamma;\Delta)} A_p(\Theta;\Xi)$.

Notice that the closure here includes also the closure under the $\Box_T$ rule.

The recursive steps for the critical sequents are given by the following table: (again, multisets Φ and Ψ contain only propositional variables, q and r are propositional variables other then p, and at least one of the multisets $\Box\Gamma', \Phi, \Box\Delta', \Psi$ is required to be nonempty):

	$\Box\Gamma'\|\Phi;\Box\Delta',\Psi$ matches	$A_p(\Box\Gamma'\|\Phi;\Box\Delta',\Psi)$ equals
1	if $p\in\Phi\cap\Psi$	$\top$
2	otherwise	$\bigvee_{q\in\Psi} q \bigvee_{r\in\Phi} \neg r$ $\bigvee_{B\in\Delta'} \Box A_p(\emptyset\|\Gamma';B)$ $\vee\Diamond A_p(\emptyset\|\Gamma';\emptyset)$

Proof of Theorem 3.3.1. The procedure runs precisely as that from Theorem 3.2.1. This time the recursively called arguments of A_p are strictly less then the corresponding match of $(\Sigma|\Gamma;\Delta)$ in terms of the function used in 2.2.7 to prove termination of Gm_T^+.

(i) holds since we never add p during a run of the procedure constructing the formula A_p.

(ii) Similarly as in Theorem 3.2.1 (ii), we proceed by induction on the complexity of $(\Sigma|\Gamma;\Delta)$ given by the terminating function.

Let $(\Sigma|\Gamma\Rightarrow\Delta)$ be a noncritical sequent. Then sequents $(\Omega_i|\Theta_i\Rightarrow\Xi_i)\in Cl(\Sigma|\Gamma;\Delta)$ are of lower complexity. By the induction hypothesis

$$\vdash_{Gm_T^+} \Omega_i|\Theta_i, A_p(\Omega_i|\Theta_i;\Xi_i)\Rightarrow\Xi_i \quad \text{for each i.}$$

Then by admissibility of weakening and by Lemma 2.3.5

$$\vdash_{Gm_T^+} \Sigma|\Gamma, A_p(\Omega_k|\Theta_1;\Xi_1),\ldots,A_p(\Omega_k|\Theta_k;\Xi_k)\Rightarrow\Delta,$$

and so

$$\vdash_{Gm_T^+} \Sigma|\Gamma, \bigwedge_{(\Omega_i|\Theta_i\Rightarrow\Xi_i)\in Cl(\Sigma|\Gamma;\Delta)} A_p(\Omega_i|\Theta_i;\Xi_i)\Rightarrow\Delta,$$

which is

$$\vdash_{Gm_T^+} \Sigma|\Gamma, A_p(\Sigma|\Gamma;\Delta)\Rightarrow\Delta.$$

Let $(\Sigma|\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 1. Then (ii) is an initial sequent.

Let $(\Sigma|\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 2. We have, similarly as in 3.2.1, the following:

- for each $B \in \Delta'$, we have $\vdash_{Gm_T^+} \emptyset|\Gamma', A_p(\emptyset|\Gamma'; B) \Rightarrow B$ by the i.h., which gives $\vdash_{Gm_T^+} \Box\Gamma', \Box A_p(\emptyset|\Gamma'; B)|\Phi, \Rightarrow \Box\Delta', \Psi$ by a $\Box_K$ inference. Then by weakening and $\Box_T$ inferences $\vdash_{Gm_T^+} \Box\Gamma'|\Box A_p(\emptyset|\Gamma'; B), \Phi \Rightarrow \Box\Delta', \Psi$.
- by the i.h. we also have $\vdash_{Gm_T^+} \emptyset|\Gamma', A_p(\emptyset|\Gamma'; \emptyset) \Rightarrow \emptyset$, which gives, using negation rules and the $\Box_K$ rule, $\vdash_{Gm_T^+} \Box\Gamma'|\Diamond A_p(\emptyset|\Gamma'; B), \Phi \Rightarrow \Box\Delta', \Psi$.
- for each $r \in \Phi$ obviously $\vdash_{Gm_T^+} \Box\Gamma'|\Phi, \neg r \Rightarrow \Box\Delta', \Psi$.
- for each $q \in \Psi$ obviously $\vdash_{Gm_T^+} \Box\Gamma'|\Phi, q \Rightarrow \Box\Delta', \Psi$.

Together this yields, using $\vee$-l inferences,

$$\vdash_{Gm_T^+} \Box\Gamma'|\Phi, \bigvee_{q\in\Psi} q \bigvee_{r\in\Phi} \neg r \bigvee_{B\in\Delta'} \Box A_p(\emptyset|\Gamma'; B) \vee \Diamond A_p(\emptyset|\Gamma'; \emptyset) \Rightarrow \Box\Delta', \Psi,$$

that is, by the line 2, $\vdash_{Gm_T^+} \Box\Gamma'|\Phi, A_p(\Box\Gamma'|\Phi; \Box\Delta', \Psi) \Rightarrow \Box\Delta', \Psi$.

(iii) We proceed by induction on the height of the proof of sequent $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ in Gm_T^+. The same as in Theorem 3.2.1 applies here. We can restrict ourselves to initial sequents and critical steps (a $\Box_K$ inferences). Let us see first that for invertible parts of the proof the task reduces to appropriate critical sequents:

Let the last inference of the proof of $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ be a classical inference. Then $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is not a critical sequent and for all $(\Omega|\Upsilon \Rightarrow \Xi) \in Cl(\Sigma|\Gamma; \Delta)$ we have $\vdash_{Gm_T^+} \Theta, \Omega|\Pi, \Upsilon \Rightarrow \Xi, \Lambda$ by 2.3.5. Then the following are equivalent:

$$\vdash_{Gm_T^+} \Theta|\Pi \Rightarrow A_p(\Omega|\Upsilon; \Xi), \Lambda \quad \text{for all} \quad (\Omega|\Upsilon \Rightarrow \Xi) \in Cl(\Sigma|\Gamma; \Delta)$$

$$\vdash_{Gm_T^+} \Theta|\Pi \Rightarrow \bigwedge_{(\Omega|\Upsilon\Rightarrow\Xi)\in Cl(\Sigma|\Gamma;\Delta)} A_p(\Omega|\Upsilon; \Xi), \Lambda$$

$$\vdash_{Gm_T^+} \Theta|\Pi \Rightarrow A_p(\Sigma|\Gamma; \Delta), \Lambda.$$

Then by weakening and $\Box_T$ inferences

$$\vdash_{Gm_T^+} \emptyset|\Theta, \Pi \Rightarrow A_p(\Sigma|\Gamma; \Delta), \Lambda.$$

So let us consider then the last step of the proof of $(\Sigma, \Theta|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is an initial sequent. It works similarly as in 3.2.1, the third multiset has no influence here.

Let us consider that the last inference of the proof of $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is a $\Box_K^+$ inference.

- Consider the principal formula $\Box A \in \Delta$. Then the proof ends with:

$$\frac{\emptyset|\Theta^\Box, \Sigma^\Box \Rightarrow A}{\Theta, \Sigma|\Gamma, \Pi \Rightarrow \Box A, \Delta', \Lambda}\ \Box_K^+$$

  where $\Box A, \Delta'$ is Δ.

  Then by the induction hypothesis $\vdash_{Gm_T^+} \emptyset|\Theta^\Box \Rightarrow A_p(\emptyset|\Sigma^\Box; A)$ and by a $\Box_{K^+}$ inference

$$\vdash_{Gm_T^+} \Theta|\Pi \Rightarrow \Box A_p(\emptyset|\Sigma^\Box; A), \Lambda.$$

  By weakening inferences

$$\vdash_{Gm_T^+} \Theta|\Theta^\Box, \Pi \Rightarrow \Box A_p(\emptyset|\Sigma^\Box; A), \Lambda.$$

  By $\Box_{T^+}$ inferences we obtain

$$\vdash_{Gm_T^+} \emptyset|\Theta, \Pi \Rightarrow \Box A_p(\emptyset|\Sigma^\Box; A), \Lambda.$$

  By the line 2 of the table and invertibility of the $\vee$-l rule we have

$$\vdash_{Gm_T^+} \emptyset|\Box A_p(\emptyset|\Sigma^\Box; A) \Rightarrow A_p(\Sigma|\Gamma; \Box A, \Delta').$$

  The two sequents above yield (iii+) by admissibility of the cut rule in Gm_T^+.

- Consider the principal formula $\Box A \in \Lambda$, i.e., A doesn't contain p. Then the proof ends with:

$$\frac{\emptyset|\Theta^\Box, \Sigma^\Box \Rightarrow A}{\Theta, \Sigma|\Gamma, \Pi \Rightarrow \Delta, \Box A, \Lambda'}\ \Box_K^+$$

  where $\Box A, \Lambda'$ is Λ.

  Then by the induction hypothesis

$$\vdash_{Gm_T^+} \emptyset|\Theta^\Box \Rightarrow A_p(\emptyset|\Sigma^\Box; \emptyset), A$$

and by a $\neg$-l inference and a $\Box_{K^+}$ inference

$$\vdash_{Gm_T^+} \Theta, \Box\neg A_p(\emptyset|\Sigma^\Box;\emptyset)|\Pi \Rightarrow \Box A, \Lambda'.$$

Since weakening is admissible in Gm_T^+, we obtain

$$\vdash_{Gm_T^+} \Theta, \Box\neg A_p(\emptyset|\Sigma^\Box;\emptyset)|\neg A_p(\emptyset|\Sigma^\Box;\emptyset), \Pi \Rightarrow \Box A, \Lambda'$$

and now $\Box_T^+$ inferences and a $\neg$-l inference yield

$$\vdash_{Gm_T^+} \Theta|\Pi \Rightarrow \Diamond A_p(\emptyset|\Sigma^\Box;\emptyset), \Box A, \Lambda'.$$

By weakening inferences

$$\vdash_{Gm_T^+} \Theta|\Theta^\Box, \Pi \Rightarrow \Diamond A_p(\emptyset|\Sigma^\Box;\emptyset), \Box A, \Lambda'.$$

By $\Box_T^+$ inferences

$$\vdash_{Gm_T^+} \emptyset|\Theta, \Pi \Rightarrow \Diamond A_p(\emptyset|\Sigma^\Box;\emptyset), \Box A, \Lambda'.$$

By the line 2 of the table and invertibility of the $\vee$-l rule we have

$$\vdash_{Gm_T^+} \emptyset|\Diamond A_p(\emptyset|\Sigma^\Box;\emptyset) \Rightarrow A_p(\Sigma|\Gamma;\Box A, \Delta').$$

The two sequents above yield (iii+) by admissibility of the cut rule in Gm_T^+.

QED

Analogues of Corollaries 3.2.3, 3.2.4, 3.2.5 and 3.2.6 hold also for modal logic T by very similar proofs, so we obtain, from Theorem 3.3.1, the uniform interpolation and a simulation of propositional quantifiers.

The schema $(\Diamond\forall\bar{p}A)^* \leftrightarrow (\forall\bar{p}\Diamond A)^*$, used in the previous section to separate second order quantifiers and our simulated quantifiers, holds for **T** as well. The reflexivity itself does not brake it.

3.4 Gödel-Löb's Logic GL

Theorem 3.4.1. *Let Γ, Δ be finite multisets of formulas. For every propositional variable p there exists a formula $A_p(\Gamma; \Delta)$ such that:*

- *(i)*
$$Var(A_p(\Gamma;\Delta)) \subseteq Var(\Gamma,\Delta)\backslash\{p\}$$
- *(ii)*
$$\vdash_{Gm_{GL}} \Gamma, A_p(\Gamma;\Delta) \Rightarrow \Delta$$
- *(iii) moreover let Π, Λ be multisets of formulas not containing p and $\vdash_{Gm_{GL}}$ $\Pi, \Gamma \Rightarrow \Lambda, \Delta$. Then*
$$\vdash_{Gm_{GL}} \Pi \Rightarrow A_p(\Gamma;\Delta), \Lambda.$$

We define a formula $A_p(\Gamma; \Delta)$ inductively as in 3.2.1, changing the table as follows (again, q and r are propositional variables other then p, multisets Φ and Ψ contain only propositional variables and at least one of the multisets is required to be nonempty).

Also multisets Υ and Θ in the line 2 contain only propositional variables.

The formula $A_p(\Gamma; \Delta)$ is defined recursively to equal $\bigwedge\limits_{(\Theta\Rightarrow\Xi)\in Cl(\Gamma;\Delta)} A_p(\Theta; \Xi)$.

The recursive steps for the critical sequents are given by the following table:

	$\Box\Gamma', \Phi; \Box\Delta', \Psi$ matches	$A_p(\Box\Gamma', \Phi; \Box\Delta', \Psi)$ equals
1	if $p \in \Phi \cap \Psi$ or $\Gamma' \cap \Delta' \neq \emptyset$	$\top$
2	otherwise	$\bigvee\limits_{q\in\Psi} q \vee \bigvee\limits_{r\in\Phi} \neg r$ $\bigvee\limits_{B\in\Delta'} \Box A_p(\Box\Gamma', \Gamma', \Box B; B) \vee$ $\Diamond(\bigwedge\limits_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ \\ \Sigma\cap\Omega=\emptyset}}$ $(\bigvee\limits_{q\in\Theta} q \vee \bigvee\limits_{r\in\Upsilon} \neg r \vee \bigvee\limits_{B\in\Omega} \Box A_p(\Box\Sigma, \Sigma, \Box B; B))$ $\bigwedge\limits_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ}} A_p(\Box\Sigma, \Upsilon; \Box\Omega, \Theta))$

Proof of Theorem 3.4.1. The first line corresponds to the case when the critical sequent is an initial sequent or the diagonal formula is already in the antecedent (here we are using the loop preventing mechanism from the termination argument in 2.3.1). Then the procedure ends up with $\top$.

For the termination of this procedure (see below) we are going to use a similar function as the one used proving termination of Gm_{GL} in 2.3.1. So words "strictly less" in the following paragraph refer to such a function.

The second line, as in previous proofs, corresponds to the modal jump. It treats propositional variables from multisets Φ, Ψ, all the possibilities of a $\Box_{GL}$ inference with the principal formula from $\Box\Delta'$ and the possibility of a $\Box_{GL}$ inference with the principal formula not from $\Box\Delta'$ (i.e., appropriate inductive steps in the proof of (iii) of the Theorem). The last disjunct starting with a $\Diamond$ needs some explanation. Proceeding as in previous proofs, we would add $\Diamond A_p(\Box\Gamma', \Gamma'; \emptyset)$ to prove (iii) of the theorem (it captures the case of a $\Box_{GL}$ inference with the principal formula not containing p). This presents a problem since $(\Box\Gamma', \Gamma')$ needn't be strictly less then $(\Box\Gamma', \Phi; \Box\Delta', \Psi)$. As a simple example shows, it cannot be solved using any terminating function: a run of the procedure for $(\Box p, p; \emptyset)$ would create a loop then. A solution is as follows: we skip $(\Box\Gamma', \Gamma'; \emptyset)$ and go to the next level of its proof-search tree, which is $Cl(\Box\Gamma', \Gamma'; \emptyset)$, and consider all critical sequents from the closure. For those strictly less then $(\Box\Gamma', \Phi; \Box\Delta', \Psi)$ (which means with more boxed formulas in the antecedent) we just take their A_p, while for those that needn't be strictly less then $(\Box\Gamma', \Phi; \Box\Delta', \Psi)$ we apply the second line of the table *without* the $\Diamond$ disjunct. That this is sufficient becomes clear proving (ii) and (iii) of the theorem and it can be also seen from Lemma 3.4.2.

Let us see that the definition terminates. The argument is similar to that we have used to prove termination of the calculus Gm_{GL} in 2.3.1.

Consider a run of the procedure for $A_p(\Pi; \Lambda)$ and let d be the maximal box-depth of $(\Pi; \Lambda)$, which is the maximal number of critical steps occurring along a branch in the tree corresponding to the run of the procedure. This is crucial since it enables us to consider an upper bound of the weight of an argument of A_p occurring during a run of the procedure.

Put $c = 4^d w(\Pi, \Lambda)$, i.e. an upper bound of the weight of an argument of A_p occurring during the run of the procedure for $(\Pi; \Lambda)$ (c is again a constant for $\Pi; \Lambda$.) Here, in contrast to the termination argument for the calculus Gm_{GL}, we need 4^d since the weight of a recursively called argument of A_p can increase more. This is caused by the last disjunct in the second line starting with $\Diamond$, since it misses the actual level of $(\Box\Gamma', \Gamma'; \emptyset)$ and calls arguments from the next one presented by $Cl(\Box\Gamma', \Gamma'; \emptyset)$.

Let $b(\Gamma)$ be the number of boxed formulas in Γ counted as a set.

For an A_p argument $(\Gamma; \Delta)$, consider an ordered pair $\langle c - b(\Gamma), w(\Gamma, \Delta)\rangle$. Now this measure decreases in every recursive step of the procedure in terms of the lexicographical ordering:

It is obvious that, for each noncritical sequent $(\Theta \Rightarrow \Xi) \in Cl(\Gamma; \Delta)$, $w(\Theta, \Xi) < w(\Gamma, \Delta)$ and that b does not decrease.

Consider a critical argument $(\Box\Gamma', \Phi; \Box\Delta', \Psi)$, i.e., line 2 of the table. For all the three recursively called arguments b increases, thus $c - b$ as well as the whole measure decreases.

- $(\Box\Gamma', \Gamma', \Box B; B)$: Obviously $b(\Box\Gamma', \Gamma', \Box B) > b(\Box\Gamma')$ since $\Box B \notin \Box\Gamma'$. (If it is, $\Gamma' \cap \Delta' \neq \emptyset$ and the line 1 is used.)

- $(\Box\Sigma, \Sigma, \Box B; B)$ where $B \in \Omega$ and $(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset)$ and $\Sigma^\circ = \Gamma'^\circ$ and $\Sigma \cap \Omega = \emptyset$: Since $\Sigma \cap \Omega = \emptyset$, $B \notin \Sigma$ and $b(\Box\Sigma, \Sigma, \Box B) > b(\Box\Sigma)$. Moreover $\Sigma^\circ = \Gamma'^\circ$ and thus $b(\Box\Sigma) = b(\Box\Gamma')$. Therefore $b(\Box\Sigma, \Sigma, \Box B) > b(\Box\Gamma')$.

- $(\Box\Sigma, \Upsilon; \Box\Omega, \Theta)$ where $(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset)$ and $\Sigma^\circ \supset \Gamma'^\circ$: Since $\Sigma^\circ \supset \Gamma'^\circ$, it holds that $b(\Box\Sigma) > b(\Box\Gamma')$ and therefore $b(\Box\Sigma, \Upsilon) > b(\Box\Gamma')$.

Before we continue proving the theorem, we prove the following lemma which will help us to proceed as in 3.2.1.

Lemma 3.4.2.

$$\vdash_{Gm_{GL}} \Diamond(\bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ}} (\bigvee_{q\in\Theta} q \vee \bigvee_{r\in\Upsilon} \neg r \vee \bigvee_{B\in\Omega} \Box A_p(\Box\Sigma, \Sigma, \Box B; B))\wedge$$

$$\bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ}} A_p(\Box\Sigma, \Upsilon; \Box\Omega, \Theta))$$

$\Leftrightarrow$

$$\Diamond A_p(\Box\Gamma', \Gamma'; \emptyset).$$

Proof of Lemma 3.4.2. Let us denote the first part of the equivalence by $\Diamond D$. The sense of the lemma stating a provable equivalence $\Diamond D \Leftrightarrow \Diamond A_p(\Box\Gamma', \Gamma'; \emptyset)$ is that the long disjunct starting with $\Diamond$ in the second line of the table can be replaced by $\Diamond A_p(\Box\Gamma', \Gamma'; \emptyset)$ in following proofs. This makes (iii) of the theorem provable as in the case of modal logic K.

First observe that, by definition,

$$\Diamond A_p(\Box\Gamma', \Gamma'; \emptyset) \equiv \Diamond \bigwedge_{\mathcal{S}\in Cl(\Box\Gamma',\Gamma';\emptyset)} A_p(\mathcal{S}).$$

This holds even if $\Box\Gamma', \Gamma' \Rightarrow \emptyset$ is a critical sequent.

$$\Diamond \bigwedge_{\mathcal{S}\in Cl(\Box\Gamma',\Gamma';\emptyset)} A_p(\mathcal{S}) \equiv \Diamond(\bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ}} A_p(\Box\Sigma, \Upsilon; \Box\Omega, \Theta)\wedge$$

$$\bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ}} A_p(\Box\Sigma,\Upsilon;\Box\Omega,\Theta)),$$

where, by definition given in the table,

$$\bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ}} A_p(\Box\Sigma,\Upsilon;\Box\Omega,\Theta)$$

$$\equiv \bigwedge_{\substack{(\Box\Sigma,\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma',\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ}} (\bigvee_{q\in\Theta} q \vee \bigvee_{r\in\Upsilon} \neg r \vee \bigvee_{B\in\Omega} \Box A_p(\Box\Sigma,\Sigma,\Box B;B)\vee\Diamond D).$$

Now, for short concentrating only on the form of what we are to prove, we show in Gm_{GL} that the following holds:

$$\vdash_{Gm_{GL}} \underbrace{\Diamond(\bigwedge_i(A_i\vee\Diamond D)\wedge\bigwedge_j B_j)}_{E} \Leftrightarrow \underbrace{\Diamond(\bigwedge_i A_i\wedge\bigwedge_j B_j)}_{D}.$$

Equivalently

$$\vdash_{Gm_{GL}} \underbrace{\Box(\bigvee_i\neg A_i\vee\bigvee_j\neg B_j)}_{\neg D} \Leftrightarrow \underbrace{\Box(\bigvee_i(\neg A_i\wedge\Box\neg D)\vee\bigvee_j\neg B_j)}_{\neg E}.$$

Consider the left-right direction first. Since

$$\forall i;\quad \vdash_{Gm_{GL}} \Box\neg D,\neg A_i\Rightarrow\bigvee_i(\neg A_i\wedge\Box\neg D)$$

and

$$\forall j;\quad \vdash_{Gm_{GL}} \neg B_j\Rightarrow\bigvee_j\neg B_j,$$

we obtain by $\vee$ inferences and weakening

$$\vdash_{Gm_{GL}} \Box\neg D,\underbrace{\bigvee_i\neg A_i\vee\bigvee_j\neg B_j}_{\neg D},\Box\neg E\Rightarrow\underbrace{\bigvee_i(\neg A_i\wedge\Box\neg D)\vee\bigvee_j\neg B_j}_{\neg E},$$

which, by a $\Box_L$ inference, yields

$$\vdash_{Gm_{GL}} \Box\neg D\Rightarrow\Box\neg E.$$

Now consider the right-left direction. Since

$$\forall i; \quad \vdash_{GmGL} \neg A_i \wedge \Box\neg D \Rightarrow \bigvee_i \neg A_i$$

and

$$\forall j; \quad \vdash_{GmGL} \neg B_j \Rightarrow \bigvee_j \neg B_j,$$

we obtain by $\vee$ inferences and weakening

$$\vdash_{GmGL} \Box\neg D, \underbrace{\bigvee_i (\neg A_i \wedge \Box\neg D) \vee \bigvee_j \neg B_j}_{\neg E}, \Box\neg E \Rightarrow \underbrace{\bigvee_i \neg A_i \vee \bigvee_j \neg B_j}_{\neg D},$$

which, by a $\Box_L$ inference, yields

$$\vdash_{GmGL} \Box\neg E \Rightarrow \Box\neg D.$$

Notice that the diagonal formulas were in both cases above introduced by weakening and so K4 would suffice to prove the lemma. QED

Let us continue proving the Theorem:
(i) follows easily by induction on Γ, Δ just because we never add p during the definition of the formula $A_p(\Gamma; \Delta)$.

(ii) We proceed by induction on the complexity of Γ, Δ given by the termination function. We prove that $\vdash_{GmGL} \Gamma, A_p(\Gamma; \Delta) \Rightarrow \Delta$.
Let $(\Gamma \Rightarrow \Delta)$ be a noncritical sequent. Then sequents $(\Theta_i \Rightarrow \Xi_i) \in Cl(\Gamma; \Delta)$ are of lower complexity. By the induction hypotheses

$$\vdash_{GmGL} \Theta_i, A_p(\Theta_i; \Xi_i) \Rightarrow \Xi_i$$

for each i.

Then by admissibility of weakening and by Lemma 2.3.5

$$\vdash_{GmGL} \Gamma, A_p(\Theta_1; \Xi_1), \dots, A_p(\Theta_k; \Xi_k) \Rightarrow \Delta,$$

and so

$$\vdash_{GmGL} \Gamma, \bigwedge_{(\Theta_i \Rightarrow \Xi_i) \in Cl(\Gamma; \Delta)} A_p(\Theta_i; \Xi_i) \Rightarrow \Delta,$$

which is

$$\vdash_{GmGL} \Gamma, A_p(\Gamma; \Delta) \Rightarrow \Delta.$$

Let $(\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 1. Then (ii) is an initial sequent.

Let $(\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 2.

- For each $B \in \Delta'$, we have $\vdash_{Gm_{GL}} \Box\Gamma', \Gamma', \Box B, A_p(\Box\Gamma', \Gamma', \Box B; B) \Rightarrow B$ by the i.h., which gives $\vdash_{Gm_{GL}} \Box\Gamma', \Phi, \Box A_p(\Box\Gamma', \Gamma', \Box B; B) \Rightarrow \Box B, \Box\Delta'', \Psi$ by a $\Box_L$ inference.

- For each $(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset); \Sigma^\circ = \Gamma'^\circ; \Sigma \cap \Omega = \emptyset$ we have the following (since induction here is on the complexity of (Γ, Δ) we cannot use Lemma 3.4.2 and prove this line for $\Diamond A_p(\Box\Gamma', \Gamma'; \emptyset)$ as in 3.2.1):

  - obviously $\vdash_{Gm_{GL}} \bigvee_{q \in \Theta} \Rightarrow \Theta$ and by admissibility of weakening

$$\vdash_{Gm_{GL}} \Box\Sigma, \Upsilon, \bigvee_{q \in \Theta} \Rightarrow \Box\Omega, \Theta.$$

  - obviously $\vdash_{Gm_{GL}} \bigvee_{\neg r \in \Upsilon}, \Upsilon \Rightarrow$ and by admissibility of weakening

$$\vdash_{Gm_{GL}} \Box\Sigma, \Upsilon, \bigvee_{\neg r \in \Upsilon} \Rightarrow \Box\Omega, \Theta.$$

  - for each $B \in \Omega$ by the induction hypotheses

$$\vdash_{Gm_{GL}} \Box\Sigma, \Sigma, \Box B, A_p(\Box\Sigma, \Sigma, \Box B; B) \Rightarrow B$$

  and by weakening and a $\Box_{GL}$ inference

$$\vdash_{Gm_{GL}} \Box\Sigma, \Box A_p(\Box\Sigma, \Sigma, \Box B; B) \Rightarrow \Box B.$$

  Together this yields, using $\vee$-l inferences,

$$\vdash_{Gm_{GL}} \Box\Sigma, \Upsilon, \bigvee_{q \in \Theta} \vee \bigvee_{\neg r \in \Upsilon} \vee \bigvee_{B \in \Omega} \Box A_p(\Box\Sigma, \Sigma, \Box B; B) \Rightarrow \Box\Omega, \Theta.$$

For each $(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset); \Sigma^\circ \supset \Gamma'^\circ$ by the induction hypotheses $\vdash_{Gm_{GL}} \Box\Sigma, \Upsilon, A_p(\Box\Sigma, \Upsilon; \Box\Omega, \Theta) \Rightarrow \Box\Omega, \Theta$. Let us denote the conjunction

$$\bigwedge_{\substack{(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset) \\ \Sigma^\circ = \Gamma'^\circ \\ \Sigma \cap \Omega = \emptyset}} (\bigvee_{q \in \Theta} q \vee \bigvee_{r \in \Upsilon} \neg r \vee \bigvee_{B \in \Omega} \Box A_p(\Box\Sigma, \Sigma, \Box B; B))$$

$$\bigwedge_{\substack{(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset) \\ \Sigma^\circ \supset \Gamma'^\circ}} A_p(\Box\Sigma, \Upsilon; \Box\Omega, \Theta)$$

by C. Then, for each $(\Box\Sigma, \Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma', \Gamma'; \emptyset)$,

$$\vdash_{Gm_{GL}} \Box\Sigma, \Upsilon, C \Rightarrow \Box\Omega, \Theta$$

by weakening and $\wedge$-l inferences. Now, by Lemma 2.3.5,

$$\vdash_{Gm_{GL}} \Box\Gamma', \Gamma', C \Rightarrow \emptyset$$

. Using negation and weakening inferences $\vdash_{Gm_{GL}} \Box\Gamma', \Gamma', \Box\neg C \Rightarrow \neg C$, and by a $\Box_{GL}$ inference $\vdash_{Gm_{GL}} \Box\Gamma', \Phi \Rightarrow \Box\neg C, \Box\Delta', \Psi$. Now, using a negation inference again, we obtain

$$\vdash_{Gm_{GL}} \Box\Gamma', \Phi, \Diamond C \Rightarrow \Box\Delta', \Psi.$$

- for each $r \in \Phi$ obviously $\vdash_{Gm_{GL}} \Phi, \neg r, \Box\Gamma' \Rightarrow \Box\Delta', \Psi$.
- for each $q \in \Psi$ obviously $\vdash_{Gm_{GL}} \Phi, q, \Box\Gamma' \Rightarrow \Box\Delta', \Psi$.

Together this yields, using $\vee$-l inferences,

$$\vdash_{Gm_{GL}} \Phi, \Box\Gamma', \bigvee_{q\in\Psi} q \bigvee_{r\in\Phi} \neg r \bigvee_{B\in\Delta'} \Box A_p(\Box\Gamma', \Gamma', \Box B; B) \vee \Diamond C \Rightarrow \Box\Delta', \Psi,$$

that is, by the line 2, $\vdash_{Gm_{GL}} \Phi, \Box\Gamma', A_p(\Phi, \Box\Gamma'; \Box\Delta', \Psi) \Rightarrow \Box\Delta', \Psi$.

(iii) We proced by induction on the height of a proof of $(\Pi, \Gamma \Rightarrow \Lambda, \Delta)$. We can restrict ourselves to critical steps (a $\Box_L$ inferences). The argument from Theorem 3.2.1 applies for the rest. So let us consider that the last inference is a $\Box_{GL}$ inference:

Consider the principal formula $\Box A \in \Lambda$ first, i.e. A doesn't contain p. Then the proof ends with:

$$\frac{\Box\Pi', \Box\Gamma', \Pi', \Gamma', \Box A \Rightarrow A}{\Box\Pi', \Box\Gamma', \Pi'', \Gamma'' \Rightarrow \Box A, \Lambda', \Delta}$$

where $\Box\Pi', \Pi''$ is Π; $\Box\Gamma', \Gamma''$ is Γ; and $\Box A, \Lambda'$ is Λ. Consider $\Gamma' \cap \Delta^{\Box} = \emptyset$ (otherwise $A_p(\Gamma; \Delta) \equiv \top$ and (iii) holds) so we can use the line 2. Then the induction hypothesis gives

$$\vdash_{Gm_{GL}} \Pi', \Box A \Rightarrow A_p(\Box\Gamma', \Gamma'; \emptyset), A$$

and by a $\neg$-l inference we obtain

$$\vdash_{Gm_{GL}} \Pi', \Box A, \neg A_p(\Box\Gamma', \Gamma'; \emptyset) \Rightarrow A$$

. Now, by a $\Box_L$ and a negation inference, we obtain

$$\vdash_{Gm_{GL}} \Box\Pi', \Pi'' \Rightarrow \Diamond A_p(\Box\Gamma', \Gamma'; \emptyset), \Box A, \Lambda'.$$

By the line 2 of the table, invertibility of the $\vee$-l rule, and Lemma 3.4.2 we have

$$\vdash_{GmGL} \Diamond A_p(\Box\Gamma', \Gamma'; \emptyset) \Rightarrow A_p(\Box\Gamma', \Gamma''; \Delta).$$

The two sequents above yield (iii) by cut admissibility.

Consider the principal formula $\Box A \in \Delta$. Again, consider $\Gamma' \cap \Delta^{\Box} = \emptyset$ so we can use the line 2. Then the proof ends with:

$$\frac{\Box\Pi', \Box\Gamma', \Pi', \Gamma', \Box A \Rightarrow A}{\Box\Pi', \Box\Gamma', \Pi'', \Gamma'' \Rightarrow \Box A, \Delta', \Lambda}$$

where $\Box\Pi', \Pi''$ is Π; $\Box\Gamma', \Gamma''$ is Γ; and $\Box A, \Delta'$ is Δ.

Now the induction hypothesis gives

$$\vdash_{GmGL} \Box\Pi', \Pi' \Rightarrow A_p(\Box\Gamma', \Gamma', \Box A; A)$$

and by weakening and a $\Box_L$ inference we obtain

$$\vdash_{GmGL} \Box\Pi', \Pi'' \Rightarrow \Box A_p(\Box\Gamma', \Gamma', \Box A; A), \Lambda.$$

The line 2 or 3 of the table and invertibility of the $\vee$-l rule yields

$$\vdash_{GmGL} \Box A_p(\Box\Gamma', \Gamma', \Box A; A) \Rightarrow A_p(\Box\Gamma', \Gamma''; \Box A, \Delta').$$

We obtain (iii) again by cut admissibility. QED

Analogues of Corollaries 3.2.3, 3.2.4, 3.2.5 and 3.2.6 hold also for modal logic **GL** by similar proofs, so we obtain, from Theorem 3.4.1, the uniform interpolation and a simulation of propositional quantifiers.

Considering again the schema $(\Diamond\forall\bar{p}A)^* \leftrightarrow (\forall\bar{p}\Diamond A)^*$, it is not clear whether it holds in case of **GL** or not. Transitivity complicate things here. So far, we are able neither to prove it nor to provide a counterexample.

3.4.1 Fixed points

Uniform interpolation theorem for logic **GL** entails Sambin's and de Jongh's fixed point theorem. Our proof then presents an alternative constructive proof of the fixed point theorem:

Theorem 3.4.3. *Fixed point theorem: Suppose p is modalized in B (i.e., any occurrence of p is in the scope of a $\Box$). Then we can find a formula C in the variables of B without p such that*

$$\vdash_{GL} C \leftrightarrow B(C).$$

Uniform interpolation entails fixed point theorem. Already ordinary interpolation does the job: a fixed point of a formula B is an interpolant of a sequent obtained from a sequent expressing the uniqueness of the fixed point

$$\Box(p \leftrightarrow B(p)) \wedge \Box(q \leftrightarrow B(q)) \Rightarrow p \leftrightarrow q,$$

which is provable in **GL** - for a detailed proof see [46] and [8]. However, this method is not useful for implementations since first we would need to have a proof of the sequent expressing the uniqueness of the fixed point.

Direct proofs of fixed point theorem were given by Sambin [44], Sambin and Valentini in [46] (construction of explicit fixed points which is effective and implementable), Smoryński [48] from Beth's definability property, Reidhar-Olson [43], Gleit and Goldfarb [21]. A proof from Beth's property can be found also in Kracht's book [28], for three different proofs see Boolos' book [8].

The point of non-constructiveness of proofs of the existence of fixed point is that first the uniqueness is proved semantically, and from this is derived, using Beth's definability, that this explicit definition yields indeed a fixed point. Or the uniqueness is proved syntactically, and Craig interpolation of the statement of the uniqueness for a particular formula then yields the fixed point. This choice is constructive, but non-effective since first we need to have a (cut-free) proof of the uniqueness for the particular formula to construct an interpolant.

A different and effective constructive proof of fixed point theorem is the one by Sambin and Valentini in [46]. Our proof, based on uniform interpolation, is an alternative effective proof then. The point is that we do not need a proof of the uniqueness to construct the interpolants.

Proof of Theorem 3.4.3. Let us consider a formula $B(p, \bar{q})$ with p modalized in B. The fixed point of B then would be the simulation of

$$\exists p(\Box(p \leftrightarrow B(p)) \wedge B(p))$$

or, equivalently, of

$$\forall r(\Box(r \leftrightarrow B(r)) \rightarrow B(r)).$$

Let us denote them C_1 and C_2 and observe they are both interpolants of

$$(\Box(p \leftrightarrow B(p)) \wedge B(p) \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r))$$

and that neither of them contains p, r. We show that any of them is the fixed point of B and that they are indeed equivalent. What follows are a bit informal proof-trees which, to keep readability, express rather statements about provability in Gm_{GL} then proofs in Gm_{GL}.

First we show that $(\Box(p \leftrightarrow B(p)) \wedge B(p) \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r))$ is provable from the uniqueness statement:

$$\dfrac{\Box(p \leftrightarrow B(p)) \wedge \Box(r \leftrightarrow B(r)) \Rightarrow p \leftrightarrow r \qquad \dfrac{\vdots}{p \leftrightarrow r, p \leftrightarrow B(p), r \leftrightarrow B(r), B(p) \Rightarrow B(r)}}{\dfrac{\dfrac{\Box(p \leftrightarrow B(p)), \Box(r \leftrightarrow B(r)), B(p) \Rightarrow B(r)}{(\Box(p \leftrightarrow B(p)), B(p) \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r))}}{(\Box(p \leftrightarrow B(p)) \wedge B(p) \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r))}}\ \text{cut}$$

Now let us see that any of C_i is a fixed point and thus, by the uniqueness, $C_1 \leftrightarrow C_2$.

First observe, that whenever $(\Gamma(p) \Rightarrow \Delta(p))$ is provable, $(\Gamma[p/A] \Rightarrow \Delta[p/A])$ where we substitute A for p is provable as well (we just substitute everywhere in the proof, to treat $\Box_{GL}$ inferences can require some admissible weakenings, and we add proofs of sequents $(\Gamma, A \Rightarrow \Delta, A)$ in place of initial sequents). The label "subst." in the following proof-tree refers to such a substitution, the label "inv." refers to invertibility of a rule:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box(p \leftrightarrow B(p)) \wedge B(p) \Rightarrow C_i}{\Box(C_i \leftrightarrow B(C_i)) \wedge B(C_i) \Rightarrow C_i}\ \text{subst.}}{\Box(C_i \leftrightarrow B(C_i)), B(C_i) \Rightarrow C_i}\ \text{inv.}}{\Box(C_i \leftrightarrow B(C_i)) \Rightarrow \neg B(C_i), C_i}}{\Box(C_i \leftrightarrow B(C_i)) \Rightarrow B(C_i) \rightarrow C_i} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{C_i \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r)}{C_i \Rightarrow \Box(C_i \leftrightarrow B(C_i)) \rightarrow B(C_i)}\ \text{subst.}}{C_i \Rightarrow \neg\Box(C_i \leftrightarrow B(C_i)), B(C_i)}\ \text{inv.}}{C_i, \Box(C_i \leftrightarrow B(C_i)) \Rightarrow B(C_i)}}{\Box(C_i \leftrightarrow B(C_i)) \Rightarrow \neg C_i, B(C_i)}}{\Box(C_i \leftrightarrow B(C_i)) \Rightarrow C_i \rightarrow B(C_i)}}{\dfrac{\Box(C_i \leftrightarrow B(C_i)) \Rightarrow C_i \leftrightarrow B(C_i)}{\emptyset \Rightarrow \Box(C_i \leftrightarrow B(C_i))}\ \Box_{GL}}$$

Now by a cut

$$\dfrac{\emptyset \Rightarrow \Box(C_i \leftrightarrow B(C_i)) \qquad \Box(C_i \leftrightarrow B(C_i)) \Rightarrow C_i \leftrightarrow B(C_i)}{\emptyset \Rightarrow C_i \leftrightarrow B(C_i)}\ \text{cut}$$

From this proof one can see that already ordinary interpolation does the job. The point of using uniform interpolation here is that we do not need to have a proof of $(\Box(p \leftrightarrow B(p)) \wedge B(p) \Rightarrow \Box(r \leftrightarrow B(r)) \rightarrow B(r))$ to construct an interpolant - we just need to know that it is provable.

We learnt this simple proof from Albert Visser.

QED

3.5 Grzegorczyk's Logic S4Grz

Theorem 3.5.1. *Let Σ, Γ, Δ be finite multisets of formulas (Σ a multiset of boxed formulas). For every propositional variable p there exists a formula $A_p(\Sigma|\Gamma; \Delta)$ such that:*

- *(i)*

$$Var(A_p(\Sigma|\Gamma;\Delta)) \subseteq Var(\Sigma,\Gamma,\Delta)\backslash\{p\}$$

- *(ii)*

$$\vdash_{Gm^+_{Grz}} \emptyset|\Sigma,\Gamma,A_p(\Sigma|\Gamma;\Delta) \Rightarrow \Delta$$

- *(iii) moreover let* Π,Λ,Θ *be multisets of formulas not containing p and* $\vdash_{Gm^+_{Grz}}$ $\Theta,\Sigma|\Pi,\Gamma \Rightarrow \Lambda,\Delta$. *Then*

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta,\Pi \Rightarrow A_p(\Sigma|\Gamma;\Delta),\Lambda.$$

We define a formula $A_p(\Sigma|\Gamma;\Delta)$ inductively as in 3.3.1, changing the table as follows (again, q and r are propositional variables other then p, multisets Φ and Ψ contain only propositional variables and at least one of the multisets is required to be nonempty).

Also the multisets Υ,Θ in the line 2 contain only propositional variables.

The formula $A_p(\Sigma|\Gamma;\Delta)$ is defined recursively to equal $\bigwedge_{(\Omega|\Theta\Rightarrow\Xi)\in Cl(\Sigma|\Gamma;\Delta)} A_p(\Omega|\Theta;\Xi)$.

The recursive steps for the critical sequents are given by the following table:

	$\Box\Gamma'\|\Phi;\Box\Delta',\Psi$ matches	$A_p(\Box\Gamma'\|\Phi;\Box\Delta',\Psi)$ equals
1	if $p\in\Phi\cap\Psi$ or $\Gamma'\cap\Delta'\neq\emptyset$	$\top$
2	otherwise	$\bigvee_{q\in\Psi} q \bigvee_{r\in\Phi} \neg r$ $\bigvee_{B\in\Delta',(B\to\Box B)\notin\Gamma'} \Box A_p(\Box\Gamma',\Box(B\to\Box B)\|\Gamma';B)$ $\bigvee_{B\in\Delta',(B\to\Box B)\in\Gamma'} \Box A_p(\Box\Gamma'\|\emptyset;B))$ $\vee\Diamond(\bigwedge_{\substack{(\Box\Sigma\|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'\|\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ\\ \Sigma\cap\Omega=\emptyset}} (\bigvee_{q\in\Theta} q\vee \bigvee_{r\in\Upsilon}\neg r\vee$ $\bigvee_{B\in\Omega,(B\to\Box B)\notin\Sigma} \Box A_p(\Box\Sigma,\Box(B\to\Box B)\|\Sigma;B)\vee$ $\bigvee_{B\in\Omega,(B\to\Box B)\in\Sigma} \Box A_p(\Box\Sigma\|\emptyset;B))\wedge$ $\bigwedge_{\substack{(\Box\Sigma\|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'\|\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ}} A_p(\Box\Sigma\|\Upsilon;\Box\Omega,\Theta))$

PROOF OF THEOREM 3.5.1. The table follows similar ideas as the previous one, only now we deal with two loop preventing mechanisms: one is that used for **T** and the other is splitting the $\Box_{Grz}$ rule into two cases testing if the diagonal formula is already stored in the third multiset or not.

We adopt the same simplification as we have used proving termination of the calculus Gm_{Grz^+} - we restrict the $\Box_T^+$ rule and treat the third multiset as a set (i.e., we remove duplicate formulas).

Let us see that the definition terminates. Consider a run of the procedure for $A_p(\emptyset|\Pi;\Lambda)$. Let d be maximal box depth in Π, Λ, which is, as in the case of **GL**, maximal number of critical steps along one branch of the corresponding tree. Let $b(\Gamma)$ be the number of boxed subformulas of Γ counted as a set.

With each A_p argument $(\Sigma|\Gamma;\Delta)$ occurring during the run of the procedure, we associate an ordered pair $\langle e - |\Sigma^\circ|, w(\Gamma,\Delta)\rangle$. We recall that we use the size of the set Σ°.

Here $e = d.b(\Pi,\Lambda)$ is an upper bound of the number of formulas stored if we do not duplicate them.

The measure decreases in each step of the run of the procedure in terms of the lexicographical ordering.

For a noncritical argument $(\Sigma|\Gamma;\Delta)$, for each $(\Omega|\Theta \Rightarrow \Xi) \in Cl(\Sigma|\Gamma;\Delta)$, $w(\Theta,\Xi) < w(\Gamma,\Delta)$.

For a critical argument $(\Box\Gamma'|\Phi;\Box\Delta',\Psi)$ let us see that, in the table, for each of the five recursively called arguments the measure decreases.

- $(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B)$ where $B \in \Delta'$ and $(B \to \Box B) \notin \Gamma'$: here obviously $|(\Box\Gamma' \cup \Box(B \to \Box B))^\circ| > |\Box\Gamma'^\circ|$.
- $(\Box\Gamma'|\emptyset; B)$ where $B \in \Delta'$ and $(B \to \Box B) \in \Gamma'$: In this case, $w(\emptyset, B) < w(\Phi, \Box\Delta', \Psi)$.
- $(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B)$ where $B \in \Omega$ and $(B \to \Box B) \notin \Sigma$, and $(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma'|\Gamma';\emptyset)$ and $\Sigma^\circ = \Gamma'^\circ$: Since $\Sigma^\circ = \Gamma'^\circ$, also $|\Box\Sigma^\circ| = |\Box\Gamma'^\circ|$. Hence $|(\Box\Sigma \cup \Box(B \to \Box B))^\circ| > |\Box\Gamma'^\circ|$.
- $(\Box\Sigma|\emptyset; B)$ where $B \in \Omega$ and $(B \to \Box B) \in \Sigma$, and $(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma'|\Gamma';\emptyset)$ and $\Sigma^\circ = \Gamma'^\circ$.
- $(\Box\Sigma|\Upsilon; \Box\Omega, \Theta)$ where $(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma'|\Gamma'\emptyset)$ and $\Sigma^\circ \supset \Gamma'^\circ$: Since $\Sigma^\circ \supset \Gamma'^\circ$, $|\Sigma^\circ| > |\Gamma'^\circ|$.

Before we continue proving the theorem, we prove the following lemma fully analogous to the previous one:

Lemma 3.5.2.

$$\vdash_{Gm^+_{Grz}} \Diamond(\bigwedge_{\substack{(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega,\Theta) \in Cl(\Box\Gamma'|\Gamma';\emptyset) \\ \Sigma^\circ = \Gamma'^\circ \\ \Sigma \cap \Omega = \emptyset}} (\bigvee_{q \in \Theta} q \vee \bigvee_{r \in \Upsilon} \neg r \vee$$

$$\bigvee_{B\in\Omega,(B\to\Box B)\notin\Sigma} \Box A_p(\Box\Sigma,\Box(B\to\Box B)|\Sigma;B)$$

$$\bigvee_{B\in\Omega,(B\to\Box B)\in\Sigma} \Box A_p(\Box\Sigma|\emptyset;B)) \qquad \bigwedge_{\substack{(\Box\Sigma|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'|\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ\\ \Sigma\cap\Omega=\emptyset}} A_p(\Box\Sigma|\Upsilon;\Box\Omega,\Theta))$$

$\Leftrightarrow$

$$\Diamond A_p(\Box\Gamma'|\Gamma';\emptyset)$$

PROOF OF LEMMA 3.5.2. The proof is fully analogous to that of Lemma 3.4.2. Again, since the form is the same as in the previous case, we show in Gm_{Grz^+} that the following holds:

$$\vdash_{Gm^+_{Grz}} \underbrace{\Diamond(\bigwedge_i(A_i\vee\Diamond D)\wedge\bigwedge_j B_j)}_{E} \Leftrightarrow \underbrace{\Diamond(\bigwedge_i A_i\wedge\bigwedge_j B_j)}_{D}.$$

Equivalently

$$\vdash_{Gm^+_{Grz}} \Box(\underbrace{\bigvee_i\neg A_i\vee\bigvee_j\neg B_j)}_{\neg D} \Leftrightarrow \Box(\underbrace{\bigvee_i(\neg A_i\wedge\Box\neg D)\vee\bigvee_j\neg B_j}_{\neg E}).$$

Since, as we have noted in Lemma 3.4.2, the diagonal formulas were introduced by weakening, we can use the same proof here. We only write it down to make it clear.

Consider the left-right direction first. Since

$$\forall i;\quad \vdash_{Gm^+_{Grz}} \emptyset|\Box\neg D,\neg A_i\Rightarrow\bigvee_i(\neg A_i\wedge\Box\neg D)$$

and

$$\forall j;\quad \vdash_{Gm^+_{Grz}} \emptyset|\neg B_j\Rightarrow\bigvee_j\neg B_j,$$

we obtain by $\vee$ inferences and weakening

$$\vdash_{Gm^+_{Grz}} \Box(\neg E\to\Box\neg E)|\Box\neg D,\underbrace{\bigvee_i\neg A_i\vee\bigvee_j\neg B_j}_{\neg D}\Rightarrow\underbrace{\bigvee_i(\neg A_i\wedge\Box\neg D)\vee\bigvee_j\neg B_j}_{\neg E},$$

which by $\Box^+_T$ inferences and admissibility of contraction yields

$$\vdash_{Gm^+_{Grz}} \Box\neg D,\Box(\neg E\to\Box\neg E)|\underbrace{\bigvee_i\neg A_i\vee\bigvee_j\neg B_j}_{\neg D}\Rightarrow\underbrace{\bigvee_i(\neg A_i\wedge\Box\neg D)\vee\bigvee_j\neg B_j}_{\neg E},$$

which, by a $\Box^{+}_{Grz1}$ inference, yields

$$\vdash_{Gm^{+}_{Grz}} \Box\neg D|\emptyset \Rightarrow \Box\neg E,$$

which by weakening and $\Box^{+}_{T}$ inferences yields

$$\vdash_{Gm^{+}_{Grz}} \emptyset|\Box\neg D \Rightarrow \Box\neg E.$$

Now consider the right-left direction. Since

$$\forall i; \quad \vdash_{Gm^{+}_{Grz}} \emptyset|\neg A_i \wedge \Box\neg D \Rightarrow \bigvee_i \neg A_i$$

and

$$\forall j; \quad \vdash_{Gm^{+}_{Grz}} \emptyset|\neg B_j \Rightarrow \bigvee_j \neg B_j,$$

we obtain by $\vee$ inferences and weakening

$$\vdash_{Gm^{+}_{Grz}} \Box\neg(D \to \Box D), \Box\neg E|\underbrace{\bigvee_i(\neg A_i \wedge \Box\neg D) \vee \bigvee_j \neg B_j}_{\neg E} \Rightarrow \underbrace{\bigvee_i \neg A_i \vee \bigvee_j \neg B_j}_{\neg D},$$

which, by a $\Box^{+}_{Grz1}$ inference, yields

$$\vdash_{Gm^{+}_{Grz}} \Box\neg E|\emptyset \Rightarrow \Box\neg D,$$

which by weakening and $\Box^{+}_{T}$ inferences yields

$$\vdash_{Gm^{+}_{Grz}} \emptyset|\Box\neg E \Rightarrow \Box\neg D.$$

QED

Let us continue proving the Theorem:
(i) follows easily by induction on $(\Sigma|\Gamma;\Delta)$ just because we never add p during the definition of the formula $A_p(\Sigma|\Gamma;\Delta)$.

(ii) Similarly as in Theorem 3.3.1 (ii), we proceed by induction on the complexity of $(\Sigma|\Gamma;\Delta)$ given by the terminating function.

Let $(\Sigma|\Gamma \Rightarrow \Delta)$ be a noncritical sequent. Then sequents $(\Omega_i|\Theta_i \Rightarrow \Xi_i) \in Cl(\Sigma|\Gamma;\Delta)$ are of lower complexity. By the induction hypotheses

$$\vdash_{Gm^{+}_{Grz}} \emptyset|\Omega_i, \Theta_i, A_p(\Omega_i|\Theta_i;\Xi_i) \Rightarrow \Xi_i$$

for each i.

Then by admissibility of weakening and by 2.3.5

$$\vdash_{Gm^+_{Grz}} \emptyset|\Sigma, \Gamma, A_p(\Omega_k|\Theta_1; \Xi_1), \ldots, A_p(\Omega_k|\Theta_k; \Xi_k) \Rightarrow \Delta,$$

and so

$$\vdash_{Gm^+_{Grz}} \emptyset|\Sigma, \Gamma, \bigwedge_{(\Omega_i|\Theta_i \Rightarrow \Xi_i) \in Cl(\Sigma|\Gamma;\Delta)} A_p(\Omega_i|\Theta_i; \Xi_i) \Rightarrow \Delta,$$

which is

$$\vdash_{Gm^+_{Grz}} \emptyset|\Sigma, \Gamma, A_p(\Sigma|\Gamma; \Delta) \Rightarrow \Delta.$$

Let $(\Sigma|\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 1. Then either (ii) is an initial sequent in the case that $p \in \Phi \cap \Psi$ or (ii) is provable in Gm^+_{Grz} in the case that $\Gamma' \cap \Delta' \neq \emptyset$.

Let $(\Sigma|\Gamma \Rightarrow \Delta)$ be a critical sequent matching the line 2. We have, similarly as in 3.3.1, the following:

- for each $B \in \Delta', (B \to \Box B) \notin \Gamma'$, we have

  $$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma', \Box(B \to \Box B), \Gamma', A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B) \Rightarrow B$$

  by the i.h., which gives

  $$\vdash_{Gm^+_{Grz}} \Box\Gamma', \Box(B \to \Box B), \Box A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B)|$$

  $$|\Gamma', (B \to \Box B), A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B) \Rightarrow B$$

  by $\Box^+_T$ inferences, contraction inferences, and weakening. To get rid of $(B \to \Box B)$, which is $(\neg B \vee \Box B)$, we apply invertibility of the $\vee$-l and $\neg$-l rules to obtain

  $$\vdash_{Gm^+_{Grz}} \Box\Gamma', \Box(B \to \Box B)|\Gamma', A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B) \Rightarrow B.$$

  This yields

  $$\vdash_{Gm^+_{Grz}} \Box\Gamma', \Box A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B)|\Phi, \Rightarrow \Box\Delta', \Psi$$

  by a $\Box^+_{Grz1}$ inference. Then by weakening and $\Box^+_T$ inferences

  $$\vdash_{Gm^+_{Grz}} \Box\Gamma'|\Box A_p(\Box\Gamma', \Box(B \to \Box B)|\Gamma'; B), \Phi \Rightarrow \Box\Delta', \Psi.$$

- for each $B \in \Delta', (B \to \Box B) \in \Gamma'$, we have

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma', A_p(\Box\Gamma'|\emptyset; B) \Rightarrow B$$

by the i.h., which gives

$$\vdash_{Gm^+_{Grz}} \Box\Gamma', \Box(B \to \Box B), \Box A_p(\Box\Gamma'|\emptyset; B)|\Gamma', A_p(\Box\Gamma'|\emptyset; B) \Rightarrow B$$

by $\Box^+_T$ inferences and weakening. Now we obtain

$$\vdash_{Gm^+_{Grz}} \Box\Gamma', \Box A_p(\emptyset|\Gamma'; B)|\Phi \Rightarrow \Box\Delta', \Psi$$

by a $\Box^+_{Grz1}$ inference. Then by weakening and $\Box^+_T$ inferences

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma', \Box A_p(\emptyset|\Gamma'; B), \Phi \Rightarrow \Box\Delta', \Psi.$$

- for each $(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma'|\Gamma'; \emptyset); \Sigma^\circ = \Gamma'^\circ; \Sigma \cap \Omega = \emptyset$
  - obviously $\vdash_{Gm^+_{Grz}} \emptyset|\Upsilon, \bigvee_{r\in\Upsilon} \neg r \Rightarrow \emptyset$, and by admissibility of weakening

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, \bigvee_{r\in\Upsilon} \neg r \Rightarrow \Box\Omega, \Theta.$$

  - obviously $\vdash_{Gm^+_{Grz}} \emptyset| \bigvee_{q\in\Theta} q \Rightarrow \Theta$, and by admissibility of weakening

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, \bigvee_{q\in\Theta} q \Rightarrow \Box\Omega, \Theta.$$

  - for each $B \in \Omega, (B \to \Box B) \notin \Sigma$, by the induction hypotheses,

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Sigma, \Sigma, \Box(B \to \Box B), A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \Rightarrow B.$$

    By $\Box^+_T$ inferences and contractions,

$$\vdash_{Gm^+_{Grz}} \Box\Sigma, \Box(B \to \Box B)|\Sigma, B \to \Box B, A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \Rightarrow B.$$

    To get rid of $(B \to \Box B)$, which is $(\neg B \vee \Box B)$, we apply invertibility of $\vee$-l rule and contraction to obtain

$$\vdash_{Gm^+_{Grz}} \Box\Sigma, \Box(B \to \Box B)|\Sigma, A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \Rightarrow B.$$

    By weakening $\vdash_{Gm^+_{Grz}}$

$$\Box\Sigma, \Box(B \to \Box B), \Box A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B)|\Sigma, A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \Rightarrow B.$$

Now we can apply the $\Box^+_{Grz1}$ rule to obtain

$$\vdash_{Gm^+_{Grz}} \Box\Sigma, \Box A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B)|\Upsilon \Rightarrow \Box\Omega, \Theta.$$

By weakening and a $\Box^+_T$ inference

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, \Box A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \Rightarrow \Box\Omega, \Theta.$$

– for each $B \in \Omega, (B \to \Box B) \in \Sigma$, by the induction hypotheses,

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Sigma, A_p(\Box\Sigma|\emptyset; B) \Rightarrow B.$$

By $\Box^+_T$ inferences,

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Sigma, A_p(\Box\Sigma|\emptyset; B) \Rightarrow B.$$

By weakening

$$\vdash_{Gm^+_{Grz}} \Box\Sigma, \Box A_p(\Box\Sigma|\emptyset; B)|\Sigma, A_p(\Box\Sigma|\emptyset; B) \Rightarrow B.$$

Now we use the $\Box^+_{Grz1}$ rule to obtain

$$\vdash_{Gm^+_{Grz}} \Box\Sigma, \Box A_p(\Box\Sigma|\emptyset; B)|\Upsilon \Rightarrow \Box\Omega, \Theta.$$

By weakening and a $\Box^+_T$ inference

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, \Box A_p(\Box\Sigma|\emptyset; B) \Rightarrow \Box\Omega, \Theta.$$

Together this yields using $\vee$-l inferences

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, \bigvee_{q\in\Theta} q \vee \bigvee_{r\in\Upsilon} \neg r \vee$$

$$\bigvee_{B\in\Omega,(B\to\Box B)\notin\Sigma} \Box A_p(\Box\Sigma, \Box(B \to \Box B)|\Sigma; B) \vee \bigvee_{B\in\Omega,(B\to\Box B)\in\Sigma} \Box A_p(\Box\Sigma|\emptyset; B) \Rightarrow \Box\Omega, \Theta.$$

For each $(\Box\Sigma|\Upsilon \Rightarrow \Box\Omega, \Theta) \in Cl(\Box\Gamma'|\Gamma'; \emptyset); \Sigma^\circ \supset \Gamma'^\circ$ we have by the induction hypotheses

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Sigma, \Upsilon, A_p(\Box\Sigma|\Upsilon; \Box\Omega, \Theta) \Rightarrow \Box\Omega, \Theta.$$

Let us denote the conjunction

$$\bigwedge_{\substack{(\Box\Sigma|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'|\Gamma';\emptyset)\\ \Sigma^\circ=\Gamma'^\circ\\ \Sigma\cap\Omega=\emptyset}} (\bigvee_{q\in\Theta} q \vee \bigvee_{r\in\Upsilon} \neg r$$

$$\vee \bigvee_{B\in\Omega,(B\to\Box B)\notin\Sigma} \Box A_p(\Box\Sigma,\Box(B\to\Box B)|\Sigma;B) \vee \bigvee_{B\in\Omega,(B\to\Box B)\in\Sigma} \Box A_p(\Box\Sigma|\emptyset;B))\wedge$$

$$\bigwedge_{\substack{(\Box\Sigma|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'|\Gamma';\emptyset)\\ \Sigma^\circ\supset\Gamma'^\circ}} A_p(\Box\Sigma|\Upsilon;\Box\Omega,\Theta)$$

by C. Then for each $(\Box\Sigma|\Upsilon\Rightarrow\Box\Omega,\Theta)\in Cl(\Box\Gamma'|\Gamma';\emptyset)$,

$$\vdash_{Gm^+_{Grz}} \Box\Sigma|\Upsilon, C\Rightarrow\Box\Omega,\Theta$$

by weakening and $\wedge$-l inferences. Thus by Lemma 2.3.5

$$\vdash_{Gm^+_{Grz}} \Box\Gamma'|\Gamma', C\Rightarrow\emptyset$$

and by negation and weakening inferences,

$$\vdash_{Gm^+_{Grz}} \Box\Gamma',\Box(\neg C\to\Box\neg C)|\Gamma'\Rightarrow\neg C.$$

Now by a $\Box^+_{Grz1}$ inference

$$\vdash_{Gm^+_{Grz}} \Box\Gamma'|\Phi\Rightarrow\Box\neg C,\Box\Delta',\Psi$$

and by a negation inference

$$\vdash_{Gm^+_{Grz}} \Box\Gamma'|\Phi,\Diamond C\Rightarrow\Box\Delta',\Psi.$$

- for each $r\in\Phi$ obviously $\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma',\Phi,\neg r\Rightarrow\Box\Delta',\Psi$.
- for each $q\in\Psi$ obviously $\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma'\Phi, q\Rightarrow\Box\Delta',\Psi$.

Together this yields, using $\vee$-l inferences,

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma'\Phi, \bigvee_{q\in\Psi} q \bigvee_{r\in\Phi}\neg r \bigvee_{B\in\Delta',(B\to\Box B)\notin\Gamma'} \Box A_p(\Box\Gamma',\Box(B\to\Box B)|\Gamma';B)$$

$$\bigvee_{B\in\Delta',(B\to\Box B)\in\Gamma'} \Box A_p(\Box\Gamma'|\emptyset;B))\vee\Diamond C\Rightarrow\Box\Delta',\Psi.$$

This yields, by the line 2 of the table,

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box\Gamma',\Phi, A_p(\Box\Gamma'|\Phi;\Box\Delta',\Psi)\Rightarrow\Box\Delta',\Psi.$$

(iii) We proceed by induction on the height of the proof of sequent $(\Theta,\Sigma|\Pi,\Gamma\Rightarrow\Lambda,\Delta)$

in Gm^+_{Grz}. Again, we can restrict ourselves to initial sequents and critical steps ($\Box_{Grz1}$ and $\Box_{Grz2}$ inferences). For invertible parts of the proof the task reduces to appropriate critical sequents as in 3.3.1.

So let us first consider the last step of the proof of $(\Sigma, \Theta|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is an initial sequent. It works similarly as in 3.2.1, the third multiset has no influence here.

Let us consider that the last inference of the proof of $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is a $\Box^+_{Grz1}$ inference.

- Consider the principal formula $\Box A \in \Delta$. Then the proof ends with:

$$\frac{\Theta, \Sigma, \Box(A \to \Box A)|\Theta^{\Box}, \Sigma^{\Box} \Rightarrow A}{\Theta, \Sigma|\Gamma, \Pi \Rightarrow \Box A, \Delta', \Lambda}\ \Box^+_{Grz1}$$

  where $\Box A, \Delta'$ is Δ. Consider $\Sigma \cap \Delta = \emptyset$ (otherwise $A_p(\Gamma; \Delta) \equiv \top$ and (iii) holds).

  Then by the induction hypotheses

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta^{\Box}, \Theta \Rightarrow A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A).$$

  By $\Box^+_T$ inferences, contraction inferences, and weakening

$$\vdash_{Gm^+_{Grz}} \Theta, \Box(D \to \Box D)|\Theta^{\Box} \Rightarrow A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A),$$

  where D is $A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A)$. Now, by a $\Box^+_{Grz1}$ inference, we obtain

$$\vdash_{Gm^+_{Grz}} \Theta|\Pi \Rightarrow \Box A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A), \Lambda.$$

  By weakening inferences

$$\vdash_{Gm^+_{Grz}} \Theta|\Theta^{\Box}, \Pi \Rightarrow \Box A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A), \Lambda.$$

  By $\Box^+_T$ inferences we obtain

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta, \Pi \Rightarrow \Box A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A), \Lambda.$$

  By the line 2 of the table and invertibility of the $\vee$-l rule we have

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box A_p(\Sigma, \Box(A \to \Box A)|\Sigma^{\Box}; A) \Rightarrow A_p(\Sigma|\Gamma; \Box A, \Delta').$$

  The two sequents above yield (iii+) by admissibility of the cut rule in Gm^+_{Grz}.

- Consider the principal formula $\Box A \in \Lambda$, i.e., A doesn't contain p. Then the proof ends with:

$$\frac{\Theta, \Sigma, \Box(A \to \Box A) | \Theta^{\Box}, \Sigma^{\Box} \Rightarrow A}{\Theta, \Sigma | \Gamma, \Pi \Rightarrow \Delta, \Box A, \Lambda'} \Box^{+}_{Grz1}$$

where $\Box A, \Lambda'$ is Λ.

Then by the induction hypotheses

$$\vdash_{Gm^{+}_{Grz}} \emptyset | \Box(A \to \Box A), \Theta, \Theta^{\Box} \Rightarrow A_p(\Sigma|\Sigma^{\Box}; \emptyset), A.$$

By $\Box^{+}_{T}$ inferences and contraction inferences we obtain

$$\vdash_{Gm^{+}_{Grz}} \Box(A \to \Box A), \Theta | (A \to \Box A), \Theta^{\Box} \Rightarrow A_p(\Sigma|\Sigma^{\Box}; \emptyset), A.$$

To get rid of $(A \to \Box A)$, which is $(\neg A \vee \Box A)$, we use invertibility of the $\vee$-l and $\neg$-l rules, and contraction, to obtain

$$\vdash_{Gm^{+}_{Grz}} \Box(A \to \Box A), \Theta | \Theta^{\Box} \Rightarrow A_p(\Sigma|\Sigma^{\Box}; \emptyset), A.$$

By a $\neg$-l inference and weakening

$$\vdash_{Gm^{+}_{Grz}} \Box(A \to \Box A), \Theta, \Box\neg A_p(\Sigma|\Sigma^{\Box}; \emptyset) | \Theta^{\Box}, \neg A_p(\Sigma|\Sigma^{\Box}; \emptyset) \Rightarrow A.$$

By a $\Box^{+}_{Grz1}$ inference

$$\vdash_{Gm^{+}_{Grz}} \Theta, \Box\neg A_p(\Sigma|\Sigma^{\Box}; \emptyset) | \Pi \Rightarrow \Box A, \Lambda'.$$

Since weakening is admissible in Gm^{+}_{Grz}, we obtain

$$\vdash_{Gm^{+}_{Grz}} \Theta, \Box\neg A_p(\Sigma|\Sigma^{\Box}; \emptyset) | \Theta^{\Box}, \neg A_p(\Sigma|\Sigma^{\Box}; \emptyset), \Pi \Rightarrow \Box A, \Lambda'$$

and now $\Box^{+}_{T}$ inferences and a $\neg$-l inference yield

$$\vdash_{Gm^{+}_{Grz}} \emptyset | \Theta, \Pi \Rightarrow \Diamond A_p(\Sigma|\Sigma^{\Box}; \emptyset), \Box A, \Lambda'.$$

By weakening inferences

$$\vdash_{Gm^{+}_{Grz}} \Theta | \Theta^{\Box}, \Pi \Rightarrow \Diamond A_p(\Sigma|\Sigma^{\Box}; \emptyset), \Box A, \Lambda'.$$

By $\Box^{+}_{T}$ inferences

$$\vdash_{Gm^{+}_{Grz}} \emptyset | \Theta, \Pi \Rightarrow \Diamond A_p(\Sigma|\Sigma^{\Box}; \emptyset), \Box A, \Lambda'.$$

By the line 2 of the table, invertibility of the $\vee$-l rule, and Lemma 3.5.2 we have

$$\vdash_{Gm^{+}_{Grz}} \emptyset | \Diamond A_p(\Sigma|\Sigma^{\Box}; \emptyset) \Rightarrow A_p(\Sigma|\Gamma; \Box A, \Delta').$$

The two sequents above yield (iii+) by admissibility of the cut rule in Gm^{+}_{Grz}.

Let us consider that the last inference of the proof of $(\Theta, \Sigma|\Pi, \Gamma \Rightarrow \Lambda, \Delta)$ is a $\Box^+_{Grz2}$ inference.

- Consider the principal formula $\Box A \in \Delta$. Then the proof ends with:

$$\frac{\Theta, \Sigma|\emptyset \Rightarrow A}{\Theta, \Sigma|\Gamma, \Pi \Rightarrow \Box A, \Delta', \Lambda}\ \Box^+_{Grz2}$$

  where $\Box A, \Delta'$ is Δ. Consider $\Sigma \cap \Delta = \emptyset$ (otherwise $A_p(\Gamma; \Delta) \equiv \top$ and (iii) holds).

  Then by the induction hypotheses

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta \Rightarrow A_p(\Sigma|\emptyset; A).$$

  By $\Box^+_T$ inferences, contraction inferences, and weakening

$$\vdash_{Gm^+_{Grz}} \Theta, \Box(D \to \Box D)|\Theta^{\Box} \Rightarrow A_p(\Sigma|\emptyset; A),$$

  where D is $A_p(\Sigma|\emptyset; A)$. Now, by a $\Box^+_{Grz1}$ inference, we obtain

$$\vdash_{Gm^+_{Grz}} \Theta|\Pi \Rightarrow \Box A_p(\Sigma|\emptyset; A), \Lambda.$$

  By weakening inferences

$$\vdash_{Gm^+_{Grz}} \Theta|\Theta^{\Box}, \Pi \Rightarrow \Box A_p(\Sigma|\emptyset; A), \Lambda.$$

  By $\Box^+_T$ inferences we obtain

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta, \Pi \Rightarrow \Box A_p(\Sigma|\emptyset; A), \Lambda.$$

  By the line 2 of the table and invertibility of the $\vee$-l rule we have

$$\vdash_{Gm^+_{Grz}} \emptyset|\Box A_p(\Sigma|\emptyset; A) \Rightarrow A_p(\Sigma|\Gamma; \Box A, \Delta').$$

  The two sequents above yield (iii+) by admissibility of the cut rule in Gm^+_{Grz}.

- Consider the principal formula $\Box A \in \Lambda$, i.e., A doesn't contain p. Then the proof ends with:

$$\frac{\Theta, \Sigma|\emptyset \Rightarrow A}{\Theta, \Sigma|\Gamma, \Pi \Rightarrow \Delta, \Box A, \Lambda'}\ \Box^+_{Grz2}$$

where $\Box A, \Lambda'$ is Λ.

Then by the induction hypotheses

$$\vdash_{Gm^+_{Grz}} \emptyset|\Theta \Rightarrow A_p(\Sigma|\emptyset;\emptyset), A.$$

Notice that $(\Sigma|\emptyset;\emptyset)$ is a critical sequent with all but one multisets empty, and by the table defining A_p, $A_p(\Sigma|\emptyset;\emptyset) \equiv \bot$. Thus we have in fact $\vdash_{Gm^+_{Grz}} \emptyset|\Theta \Rightarrow A$. By $\Box^+_T$ inferences we obtain

$$\vdash_{Gm^+_{Grz}} \Theta|\Theta^\Box \Rightarrow A$$

and by weakening

$$\vdash_{Gm^+_{Grz}} \Theta, \Box(A \to \Box A)|\Theta^\Box \Rightarrow A.$$

By a $\Box^+_{Grz1}$ inference

$$\vdash_{Gm^+_{Grz}} \Theta|\Pi \Rightarrow \Box A, \Lambda'.$$

By admissibility of weakening we obtain

$$\vdash_{Gm^+_{Grz}} \Theta|\Pi \Rightarrow A_p(\Sigma|\Gamma;\Delta), \Box A, \Lambda'.$$

QED

Again, analogues of Corollaries 3.2.3, 3.2.4, 3.2.5 and 3.2.6 hold also for modal logic **GL** by similar proofs, so we obtain, from Theorem 3.5.1, the uniform interpolation and a simulation of propositional quantifiers.

With the schema $(\Diamond\forall\bar{p}A)^* \leftrightarrow (\forall\bar{p}\Diamond A)^*$, the situation is the same as in the case of **GL**. So far, we are able neither to prove it nor to provide a counterexample.

3.6 Concluding remarks

We have presented a nearly uniform method of a constructive proof of uniform interpolation in propositional modal logics, based on a terminating sequent proof system. Two main points are to treat reflexivity, which is done using a simple loop preventing mechanism built-in the syntax, and to treat transitivity, which is rather tricky and to prevent looping, the presence of a diagonal formula is substantial. We conjecture a similar proof should work also for logic **K4Grz** but we decided not to give it here since it is much similar to that for **S4Grz**.

Observe that from our results it follows that a formula A is provable if and only if the simulation of its universal closure (where we quantify over all propositional variables of A) equals $\top$. So our construction contains, as a special case, a decision procedure.

However, our procedure is not in PSPACE - an easy example shows that it constructs formulas of exponential size in some cases. A simple reason is that closing under invertible rules we in fact construct a conjunctive normal form which is not always of polynomial size. This is not so interesting from the point of view of modal logics since it is present already in the classical propositional logic.

Even in the classical case, the complexity of interpolation is open. It was showed by Mundici in [36, 37] that, assuming $NP \cap co - NP \not\subseteq P/poly$, not all (Craig) interpolants in classical propositional logic are of polynomial size. (We use this ideas in 4.3.1 to derive lower bounds on size of proofs in modal logics.)

An interesting question remains - to understand what complexity brings the presence of modalities.

Chapter 4

Feasible interpolation

In the proof complexity area, a version of the Craig's interpolation theorem, so called feasible interpolation, is concerned to derive lower bounds on size of proofs. Feasible interpolation theorem states that, given a proof of an implication, we are able to extract from it a boolean interpolation circuit whose size is polynomial in the size of the proof. Its stronger monotone version states that we are able to extract an interpolation circuit which is moreover monotone.

In this chapter, we concentrate on the general feasible interpolation theorem. We prove the theorem for modal propositional logics **K**, **K4**, **K4Grz**, **GL**, **T**, **S4**, and **S4Grz**. The choice of logics. however natural, is also motivated by the method we use which is based on modular modal sequent calculi. So we restrict ourselves to logics for which such calculi are known and can be defined uniformly.

It is convenient in proof complexity of classical logic to formulate feasible interpolation rather for a proof of a disjunction instead of an implication. This is no more equivalent in some nonclassical logics as for example intuitionistic logic. Then it is rather a restricted form of an interpolation theorem. In case of modal logics, we deal with a special form of disjunctions - a disjunction of boxed formulas.

Our proof is a simplification and generalization of the proof for logic **S4** in [4]. Our proof technique comes from [11] and [12]. It derives feasible interpolation from so called *Feasible Disjunction Property* (FDP) which, for a modal logic, states that whenever a disjunction of the form $(\Box A \vee \Box B)$ is provable, one of the disjuncts $\Box A$, $\Box B$ has to be provable as well. The method of [12] is based on sequent calculus and uses SLD resolution to extract required information from proofs. FDP holds also for a suitable class of formulas as assumptions. We define such a class and call the formulas, in an analogy with intuitionistic propositional logic, Harrop. It is similar to the class defined in [15] or [4] for **S4**, but here it applies to all non-reflexive (reflexive) logics respectively.

We shall show that already FDP without hypotheses entails feasible interpolation theorem [41], which was overlooked in [15] where it was derived similarly as in [12] only using Harrop hypotheses and only for logic **S4**.

Ferrari, Fiorentini, and Fiorino in [15] use method based on so-called extraction calculi applied to Hilbert calculi or Natural deduction calculi to extract information from proofs. The method considers itself independent on structural properties of a particular formulation of a logic, as e.g. cut-elimination or normalization.

We would like to stress that feasible disjunction property is a property of a calculus rather then a property of a logic. So one should be careful about choosing as general calculus as possible in the sense of polynomial simulation.

We shall work with sequent calculi for modal logics. The motivation of using natural deduction calculi in some cases in [15] rather then sequent calculi is that there is no need of cut elimination which is difficult in case of provability logics. However, we show that we can manage with a simple cut elimination in our proofs - it eliminates classical cuts only. Moreover, we consider sequent calculi a sufficiently general tool formalizing logic from the complexity point of view, see also 4.3.2, as well as well developed for modal logics.

Our approach yields a simple and transparent proof of feasible interpolation in modal logics which we find, in case of normal modal logics, simpler than the one presented in [15]. However, [15] treats also logics we have not considered here, as e.g. **S4.1** and intuitionistic modal logic **K**.

FDP for a wide class of modal logics, so called extensible logics, has been proved recently by Jeřábek [27] using Frege proof systems. Hence feasible interpolation theorem and its consequences automatically apply to all these logics as well.

It is natural to relate our results to intuitionistic logic using well known translations from intuitionistic logic to logic **S4**, **S4Grz** which can be found e.g. in [13]. From this viewpoint, our results generalize that for intuitionistic logic stated at [12].

As a consequence of feasible interpolation theorem we obtain, under an assumption that $NP \cap co - NP \not\subseteq P/poly$, the existence of hard modal tautologies.

However, recently it has been shown by Hrubeš in [26] that modal logics **K**, **K4**, **S4**, **GL** satisfy monotone feasible interpolation theorem and therefore hard tautologies can be obtained without assumptions.

For all this chapter, we consider **L** to be one of nonreflexive (i.e. not containing the schema T) modal logics **K**, **K4**, **K4Grz**, and **GL**, or one of reflexive modal logics **T**, **S4**, and **S4Grz**.

The chapter 4 is organized as follows:

- Section 4.1: we uniformly define sequent calculi for modal logics **K**, **K4**, **K4Grz**, **GL**, **T**, **S4**, and **S4Grz** based on sets instead of multisets. Also following proofs are to be treated uniformly for all modal logics considered in this chapter.

- Section 4.2: we define the disjunction property for modal logic and overview our method of proving feasible disjunction property using modal sequent calculi with the cut rule.
    - Subsection 4.2.1: we introduce the concept of the closure of a proof to treat information contained in the proof of modal disjunction which is relevant to decide which disjunct is true. The closure consists of the critical sequents and is closed under the cut rule. The closure can be managed in polynomial time.
    - Subsection 4.2.2: we prove a restricted form of cut-elimination where we do not eliminate strong modal cuts. The cut elimination does not extend the closure of the original proof. We need a certain "almost cut-free" proof to reason about the closure of the original proof.
    - Subsection 4.2.3: we prove the main Theorem 4.2.6 - feasible disjunction property.
    - Subsection 4.2.4: although it is not necessary for proving feasible interpolation theorem, we prove feasible disjunction property also for a suitable class of modal formulas as assumptions. In an analogy with intuitinistic logic we call them Harrop.
- Section 4.3: as a consequence of Theorem 4.2.6 we obtain a form of feasible interpolation theorem for modal logics.
    - Subsection 4.3.1: we discuss its complexity consequences - the existence of hard tautologies.
    - Subsection 4.3.2: we conclude with some remarks.

4.1 Sequent calculi

First we define modal sequent calculi used in this part of thesis. They extend the following classical system G:

Definition 4.1.1. Sequent calculus G:

$$A \Rightarrow A$$

$$\frac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}\wedge\text{-l} \qquad \frac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow A \vee B, \Delta}\vee\text{-r}$$

$$\frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta}\,\neg\text{-r} \qquad \frac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta}\,\neg\text{-l}$$

$$\frac{\Gamma \Rightarrow A, \Delta \qquad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow A \wedge B, \Delta}\,\wedge\text{-r} \qquad \frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\,\vee\text{-l}$$

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow A, \Delta}\,\text{weak-r} \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma, A \Rightarrow \Delta}\,\text{weak-l}$$

$$\frac{\Gamma \Rightarrow \Delta, A \qquad A, \Pi \Rightarrow \Lambda}{\Gamma, (\Pi \backslash A) \Rightarrow (\Delta \backslash A), \Sigma}\,\text{cut}$$

There are few points to remark. First is that, from now below, we consider cedents to be *sets* of formulas and the comma is to be read as the set union. The reason we have chosen sets is that we are interested rather in size of proofs than in their structural properties. In this context it is easier to do without the contraction rules. However, one should be careful to check all cases in cut-elimination. Therefore we stress in our notation that, in the cut rule, the cut formula is really cut away. The other rules are also to be understood this way - in fact we should write them as e.g.

$$\frac{\Gamma, A, B \Rightarrow \Delta}{(\Gamma \backslash A, B), A \wedge B \Rightarrow \Delta}\,\wedge\text{-l}$$

Second point is that the initial sequents are of the form $(A \Rightarrow A)$ for arbitrary formula A rather then $(p \Rightarrow p)$ where p is a propositional variable. Note that the version with initial sequents $(A \Rightarrow A)$ for arbitrary formula A trivially polynomially simulates the one with $(p \Rightarrow p)$ (while the other direction is not in general polynomial). So our results hold for calculi with the atomic version of initial sequents as well.

The last point is that we have included weakening rules in the definition. The reason why we haven't built them into initial sequents and $\Box_L$ rules is technical - since we are going to use SLD resolution we need critical sequents to contain only one formula in the antecedent (see below).

A modal sequent calculus G_L results from adding, if **L** extends **T**, the $\Box_T$ rule:

$$\frac{\Gamma, A \Rightarrow \Delta}{\Gamma, \Box A \Rightarrow \Delta}\,\Box_T$$

and the $\Box_L$ rule of the form:

$$\frac{\Gamma^\star, d(A) \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_L$$

where $\Gamma^\star$ is a modification of Γ and $d(A)$ is a so called *diagonal formula*.
In the $\Box_L$ rule, all formulas from $\Box\Gamma, \Box A$ are principal.

For **K** and **T**, $\Gamma^\star = \Gamma$ and $d(A) = \top$ (or is just empty).
For **K4** and **S4**, $\Gamma^\star = \Box\Gamma, \Gamma$ and $d(A) = \top$ (or is just empty).
For **GL**, $\Gamma^\star = \Box\Gamma, \Gamma$ and $d(A) = \Box A$.
For **K4Grz**, $\Gamma^\star = \Box\Gamma, \Gamma$ and $d(A) = \Box(A \to \Box A)$.
For **S4Grz**, $\Gamma^\star = \Box\Gamma$ and $d(A) = \Box(A \to \Box A)$.
So for example the $\Box_{GL}$ rule is the following:

$$\frac{\Box\Gamma, \Gamma, \Box A \Rightarrow \ A}{\Box\Gamma \Rightarrow \Box A}\ \Box_{GL}$$

The reason why we have presented the $\Box_L$ rules uniformly is that proofs that follow run for all the logics similarly (except **S4Grz** where we need to change the definitions and proofs slightly).

Definition 4.1.2. A *critical sequent* is a sequent of the form $\Box\Gamma \Rightarrow \Box A$ which is the conclusion of a $\Box_L$ inference.

4.2 Disjunction property

Disjunction property for a modal logic **L** states that whenever a disjunction of the form $\Box A_0 \vee \Box A_1$ is a tautology of **L**, one of the disjunct $\Box A_i$ must be a tautology as well.

The standard proof-theoretic argument proving DP uses a cut-free sequent proof system complete for **L**. We start with a cut-free proof of the sequent $(\emptyset \Rightarrow \Box A_0 \vee \Box A_1)$ and consider it backwards. An easy observations leads to the conclusion that a sequent $(\emptyset \Rightarrow \Box A_i)$ for some i must occur in the same proof. The absence of the cut rule is substantial here.

Feasible Disjunction property for a modal calculus **L** states that whenever a disjunction of the form $\Box A_0 \vee \Box A_1$ has a proof π in **L**, one of the disjunct $\Box A_i$ has a proof in **L** which can be constructed in time polynomial in the size of π.

Since we are bounded by the size of the original proof, FDP is no more just a property of a logic but it is a property of a particular proof system. It is important to keep this in mind.

Trivially FDP holds for cut-free analogues of modal sequent calculi G_L defined above by the standard argument described above. But since cut-elimination is highly noneffective even in the classical case (the size of a proof can increase exponentially) this is not so interesting from the complexity point of view, especially when one is interested in lower bounds on size of proofs. We would like to prove it for a formulation of sequent calculi with cuts which usually polynomially simulate usual Frege systems for the same logic.

We present a simple proof of feasible disjunction property for sequent calculi G_L (including the cut rule) defined above. Given a proof of a sequent $(\emptyset \Rightarrow \Box A_0 \vee \Box A_1)$ we want to decide for which disjunct $(\emptyset \Rightarrow \Box A_i)$ is provable. Now it has to be done in time polynomial in the size of the original proof.

The proof of FDP for G_L goes as follows:

- consider a G_L proof π of $(\emptyset \Rightarrow \Box A_0 \vee \Box A_1)$
- extract from π information sufficient for deciding the disjunction so that it can be treated in polynomial time (the information is the closure of the critical sequents of π under the cut rule)
- prove that there is an G_L almost-cut-free-proof π' of $(\emptyset \Rightarrow \Box A_0 \vee \Box A_1)$ such that its closure does not extend the closure of π (we need this since π' can be of exponential size and so we cannot construct it and we have to do only with the closure of π)
- consider π' backwards to conclude that $(\emptyset \Rightarrow \Box A_i)$, for some i, is in the closure of π', and hence in the closure of π. This means that $(\emptyset \Rightarrow \Box A_i)$ is provable in G_L.

4.2.1 The closure

To extract, from a proof of a disjunction, information that is relevant for deciding which disjunct is provable, we concentrate on critical sequents which constitute modal information contained in the proof (since there a modality is introduced to the succedent).

First we define the closure of a proof for all logics except **S4Grz** where we need to capture slightly more than the critical sequents:

Definition 4.2.1. The *closure* of a proof π, denoted $Cl(\pi)$, is the smallest set containing the critical sequents from π and closed under cuts.

The size of the set of all the critical sequents from π is obviously polynomial in the size of π. Since the closure contains sequents with just one formula in the succedent we can test presence of a sequent in the closure in polynomial time using SLD resolution (simulating the closure under cut).

Also a proof of any sequent from the closure $Cl(\pi)$ can be obtained in polynomial time. We only need to consider the critical sequents of π together with their proofs (i.e., subproofs of π) for this argument: First we construct a proof of the considered sequent from some critical sequents of π using the closure. Then we add the proofs (taken from π) of those critical sequents which were used.

In contrast to the case of intuitionistic logic treated in [12] where the closure of a proof contains all sequents from the proof, we keep in the closure only information which is relevant in the modal sense, which means, only the critical sequents.

For **S4Grz**, the closure is defined as follows:

Definition 4.2.2. The *closure* of a G_{S4Grz} proof π, denoted $Cl(\pi)$, is the smallest set containing the critical sequents from π, and for each critical sequent $(\Box\Gamma \Rightarrow \Box A)$ also the sequent $(\Box\Gamma \Rightarrow \Box(A \to \Box A))$, and closed under cuts.

So for each critical sequent $(\Box\Gamma \Rightarrow \Box A)$, we moreover consider the sequent $(\Box\Gamma \Rightarrow \Box(A \to \Box A))$. Now we close all these critical and added sequents under cuts as before.

As before, we can test presence of a sequent in the closure in polynomial time using SLD resolution.

Note that the added sequents can be proved polynomially from the appropriate critical sequents:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma \Rightarrow \Box A}{\Box\Gamma \Rightarrow \neg A, \Box A}\text{weak}}{\Box\Gamma \Rightarrow \neg A \vee \Box A}\vee\text{-r}}{\Box\Gamma, \Box D \Rightarrow \neg A \vee \Box A}\text{weak}}{\Box\Gamma \Rightarrow \Box(\neg A \vee \Box A)}\Box_{S4Grz}$$

and so we can always construct a proof of a sequent from the closure in polynomial time.

4.2.2 Cut elimination

The next step is to eliminate cuts. We need to consider a certain 'almost-cut-free' proof backwards to show that feasible disjunction property holds, but all we have in hands is just the closure of the original proof. Therefore we prove the following form of cut elimination which does not extend the closure of the original proof. This means that all relevant information obtained in the almost-cut-free proof is already present in the original proof with cuts.

In the case of modal logics, in contrast to [12], we do not need to eliminate all cuts. In fact, the cuts with the cut formula boxed and principal in both premisses of a $\Box_L$ inference, which are usually most difficult to eliminate (in the case of **GL** and **Grz**), need not be eliminated. This makes our argument simpler. Notice that cuts left in a proof are cuts on two critical sequents, which means that both premisses as well as the conclusion of such a cut inference are in the closure of the proof.

First we consider **L** to be one of nonreflexive logics **K**, **K4**, **GL**, **K4Grz**, or one of **T** and **S4**. The case of **S4Grz** needs some minor changes.

Definition 4.2.3. An *almost-cut-free proof* is a proof in which all cuts are with the cut formula boxed and principal of a $\Box_L$ inference in both premisses.

Theorem 4.2.4. *Cut elimination for **L** either nonreflexive or one of **T** or **S4**: Let π be a Gm_L proof of the sequent $\Gamma \Rightarrow \Delta$. Then there is an almost-cut-free G_L proof π' of the sequent $\Gamma \Rightarrow \Delta$ such that $Cl(\pi') \subseteq Cl(\pi)$.*

PROOF OF THEOREM 4.2.4. For a cut elimination proof for classical logic based on sets see e.g. [50]. A proof for modal logics can be found in [46].

The *rank* of a cut inference is an ordered pair $\langle w, h \rangle$, where w is the weight of the cut formula, and h is the sum of the heights of the proofs of the premisses of a cut.

We consider the pairs lexicographically ordered.

The *rank* of a proof is the maximal rank of a cut occurring in the proof. There can be more then one such cut in a proof.

The proof is by induction on the rank of the proof. The induction step is to eliminate all the cuts of the maximal rank.

We start with a cut of the maximal rank. The main step is the following: Given proofs of the premisses of the cut where all cuts are of lower rank, we have to show that there is a proof of the conclusion using only cuts where the sum of the heights of the proofs of the premisses is lower or cuts with the rank lower than the rank of the cut we consider, which is, the rank of the proof.

First we consider the cut formula not starting with the $\Box$ modality. There are the following cases to distinguish:
(i) The cut formula not principal in one premiss : we permute the cut inference upwards.
(ii) The cut formula introduced by weakening in one premiss: then the cut inference is replaced by weakening inferences.
(iii) One premiss is an initial sequent: then this cut inference does nothing and can be just removed from the proof.
(iv) The cut formula principal in both premisses: then we use by induction hypothesis a cut(s) with the cut formula(s) of lower weight.
All these classical steps are standard, for a reference see e.g. [].

Eliminating cuts with a not boxed cut formula doesn't change the closure of the proof. Since neither of these steps adds a $\Box_L$ inference it cannot add any new critical sequent.

Now we consider the cut formula starting with the $\Box$ modality. We distinguish the following cases:

Elimination of a cut with the cut formula boxed and not principal of a $\Box_L$ inference in one premiss: there are following cases to distinguish:

(i) The cut formula boxed and not principal in one premiss (of any inference other then $\Box_L$ - this cannot occur with a nonprincipal boxed formula): we permute the cut inference upwards. This step doesn't add any new critical sequent.

(ii) The cut formula boxed and introduced by weakening in one premiss: then the cut inference is replaced by weakening inferences.

(iii) The cut formula boxed and one premiss is an initial sequent: then this cut inference does nothing and can be just removed from the proof.

(iv) The cut formula boxed and principal of a $\Box_T$ inference in one premiss and principal of a $\Box_L$ inference in the other (only for **T** and **S4**).

In the case of **T**, i.e. a $\Box_K$ inference:

$$\dfrac{\dfrac{\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_K \qquad \dfrac{A, \Gamma' \Rightarrow \Delta}{\Box A, (\Gamma'\backslash A) \Rightarrow \Delta}\,\Box_T}{\Box\Gamma, (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\text{cut}$$

we transform it as follows: (note that Γ' can possibly contain $\Box A$).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_K \qquad A, \Gamma' \Rightarrow \Delta}{\Box\Gamma, A, (\Gamma'\backslash\Box A) \Rightarrow \Delta}\,\text{cut} \qquad \Gamma \Rightarrow A}{\Gamma, (\Box\Gamma\backslash A), (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\text{cut}}{\Gamma, \Box\Gamma, (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\text{weak}}{\Box\Gamma, (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\Box_T\text{ inferences}$$

In the case of **S4**, i.e. a $\Box_{S4}$ inference:

$$\dfrac{\dfrac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4} \qquad \dfrac{A, \Gamma' \Rightarrow \Delta}{\Box A, (\Gamma'\backslash A) \Rightarrow \Delta}\,\Box_T}{\Box\Gamma, (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\text{cut}$$

we transform it as follows: (again Γ' can possibly contain $\Box A$).

$$\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4} \qquad A, \Gamma' \Rightarrow \Delta}{\Box\Gamma, A, (\Gamma'\backslash\Box A) \Rightarrow \Delta}\,\text{cut} \qquad \Box\Gamma \Rightarrow A}{(\Box\Gamma\backslash A), \Gamma'\backslash(\Box A, A) \Rightarrow \Delta}\,\text{cut}}{\Box\Gamma, (\Gamma'\backslash\Box A, A) \Rightarrow \Delta}\,\text{weak}$$

Neither of transformations above adds any new critical sequent and therefore it does not extend the closure of the proof.

Cuts with the cut formula boxed and principal of $\Box_L$ inferences in both premisses are not eliminated. QED

The main point which makes our argument simple is that eliminating cuts (using a pretty standard argument) we do not use any new $\Box_L$ inference and therefore we do not add any new critical sequent and do not extend the closure.

Note that only cuts on sequents from the closure of the original proof π can occur in an almost-cut-free proof π'.

To obtain a similar cut elimination in the case of **S4Grz**, we change the concept of an almost-cut-free proof as follows:

An almost-cut-free proof in G_{S4Grz} may, besides the cuts on critical sequents, contain also cuts on sequents $(\Box\Gamma \Rightarrow \Box(A \rightarrow \Box A))$ treated as added axioms.

Theorem 4.2.5. *Cut elimination for **S4Grz**: Let π be a G_{S4Grz} proof of the sequent $\Gamma \Rightarrow \Delta$. Then there is an almost-cut-free G_{S4Grz} proof π' of the sequent: $\Gamma \Rightarrow \Delta$ such that $Cl(\pi') \subseteq Cl(\pi)$.*

PROOF OF THEOREM 4.2.5. The argument runs precisely as before. The only change is the following step:

Elimination of a cut with the cut formula boxed and principal of a $\Box_T$ inference in one premiss and principal of a $\Box_{S4Grz}$ inference in the other (D denotes $\Box(A \rightarrow \Box A)$):

$$\dfrac{\dfrac{\Box\Gamma, \Box D \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4Grz} \qquad \dfrac{A, \Gamma' \Rightarrow \Delta}{\Box A, (\Gamma' \backslash A) \Rightarrow \Delta}\,\Box_T}{\Box\Gamma, (\Gamma' \backslash \Box A, A) \Rightarrow \Delta}\,\text{cut}$$

we transform it as follows: (again Γ' can possibly contain $\Box A$).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma, \Box D \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4Grz} \qquad A, \Gamma' \Rightarrow \Delta}{\Box\Gamma, A, (\Gamma' \backslash \Box A) \Rightarrow \Delta}\,\text{cut} \qquad \Box\Gamma, \Box D \Rightarrow A}{(\Box\Gamma \backslash A), \Box D, (\Gamma' \backslash \Box A, A) \Rightarrow \Delta}\,\text{cut}}{\Box\Gamma, \Box D, (\Gamma' \backslash \Box A, A) \Rightarrow \Delta}\,\text{weak} \qquad \Box\Gamma \Rightarrow \Box D}{\dfrac{(\Box\Gamma \backslash \Box D), (\Gamma' \backslash \Box A, A, \Box D) \Rightarrow \Delta}{\Box\Gamma, (\Gamma' \backslash \Box A, A) \Rightarrow \Delta}\,\text{weak}}\,\text{cut}$$

Here $(\Box\Gamma \Rightarrow \Box D)$ is added as a new axiom. The transformation does not add any new critical sequents and therefore it does not extend the closure of the proof. QED

Again, all cuts in the almost-cut-free proof π' are cuts on sequents form the closure of the proof π.

4.2.3 Feasible Disjunction Property

Theorem 4.2.6. *Feasible disjunction property: Let π be a G_L proof of $(\emptyset \Rightarrow \Box A_0 \vee \Box A_1)$. Then we can construct in polynomial time a G_L proof σ of $(\emptyset \Rightarrow \Box A_i)$ for some $i \in \{0,1\}$.*

PROOF OF THEOREM 4.2.6. By Theorem 4.2.4 or Theorem 4.2.5, there is an G_L almost-cut-free-proof π' of the same sequent. We consider π' backwards using the fact that cuts that can occur in π' are of the restricted form (both premisses of a cut are of the form $(\Box\Lambda \Rightarrow \Box C)$).

Consider the last step of the proof π'.

- It cannot be a cut, since then the succedent $\Box A_0 \vee \Box A_1$ would be the succedent of one of the premisses of the cut, but it is not a single boxed formula. Neither it can be a cut (in case of **S4Grz**) of the other form, the same reason applies here.

- It cannot be a weakening inference since the empty sequent has no proof.

- So it can be only a $\vee$ inference and the sequent $(\emptyset \Rightarrow \Box A_0,\ \Box A_1)$ is in π'.

Now consider the sequent $(\emptyset \Rightarrow \Box A_0,\ \Box A_1)$ and the step above it.

- If it is a weakening inference, we have a sequent $(\emptyset \Rightarrow \Box A_1)$ for some i in π'.

- If it is a cut then the cut formula must be one of $\Box A_i$. Otherwise the succedent $(\Box A_0,\ \Box A_1)$ would be the succedent of one of the premisses of the cut, but it is not a single boxed formula. It cannot be the case that $\Box A_0$ is in the succedent of one premiss of the cut while $\Box A_1$ is in the other, unless one of them is the cut formula. But then we have a sequent $(\emptyset \Rightarrow \Box A_1)$ in π' (it is a premiss of the cut).

Consider the sequent $(\emptyset \Rightarrow \Box A_i)$. Again, consider the step above it.

The step above can either be a $\Box_L$ infernce and hence $(\emptyset \Rightarrow \Box A_i)$ is a critical sequent and therefore it is in the closure $Cl(\pi')$ and hence in the closure $Cl(\pi)$ and we are done. Or the step above can be a cut. But both premisses of such a cut are critical sequents from the closure $Cl(\pi')$ and hence in the closure $Cl(\pi)$. Then so is $(\emptyset \Rightarrow \Box A_i)$ by the closure on the cut rule.

We have shown that $(\emptyset \Rightarrow \Box A_i)$ is in $Cl(\pi)$ for some i. Now we can construct its proof in time polynomial in the size of π.

QED

4.2.4 Harrop hypotheses

Feasible disjunction property also holds for a suitable class of formulas as assumptions. In an analogy with Harrop-Rasiowa formulas for intuitionistic logic [23], we define the following class of modal formulas and call them Harrop. We do not claim that they are the only formulas with this property. As in intuitionistic logic, this is an open problem to describe the class of all formulas under which disjunction property holds.

Although we do not need the FDP with Harrop hypotheses to prove the feasible interpolation theorem, we include the proof here. It is going to be more complicated then the previous one.

Definition 4.2.7. **L**-Harrop formulas for a logic **L** are defined as follows: for a logic **L** extending **T**:

$$H := p|\bot|\Box H|\Box A \to H|H \wedge H$$

for a logic **L** non-extending **T**:

$$H := p|\bot|\Box A|\Box A \to H|H \wedge H$$

where A is an arbitrary formula and p is any propositional variable.

Remark 4.2.8. The disjunction property for modal logics as stated in this paper also holds for a class of formulas defined as above where we allow, instead of any propositional variable, any propositional non-modal formula. In that case we are not able to prove that it is feasible. Consider we have an almost cut-free proof of $(\Gamma \Rightarrow \Box A_0 \vee \Box A_1)$, Γ a set of formulas as defined above. It can be the case that propositional non-modal part of Γ is inconsistent and the disjunction was, in the original proof, introduced by weakening. We are not able to recognize this case inspecting the closure of the original proof which captures the modal information contained in the proof. Neither we are able to check in polynomial time whether a set of formulas is classically inconsistent.

Stated in our language, Harrop formulas read as follows:
for a logic **L** extending **T**:

$$H := p|\Box H|\neg\Box A|\neg\Box A \vee H|H \wedge H$$

for a logic **L** non-extending **T**:

$$H := p|\Box A|\neg\Box A|\neg\Box A \vee H|H \wedge H$$

The proof of FDP proceeds as in the previous case without hypotheses, we only extend our notion of the closure as follows:

Definition 4.2.9. The *extended closure* of a proof π in G_L, denoted $Cl^+(\pi)$, is the smallest set containing

- the critical sequents from π,
- the initial sequents of the form $(\Box A \Rightarrow \Box A)$,
- the sequents $(\Box H \Rightarrow H)$ for all Harrop subformulas occurring in π, if L extends **T**,
- the sequents $(H_1 \wedge H_2 \Rightarrow H_i)$ for $i = 1, 2$ and for H_i a Harrop subformula occurring in π
- the sequents $(\neg\Box B \vee H, \Box A \Rightarrow H)$ for $(\neg\Box B \vee H)$ a subformula occurring in π
- $(\Box H, \neg\Box H \Rightarrow \emptyset)$ for H a Harrop subformula occurring in π if L extends **T**, or $(\Box A, \neg\Box A \Rightarrow \emptyset)$ for $\Box A$ a Harrop subformula occurring in π if L does not.

and closed under cuts, left weakenings (of course only by subformulas occurring in π to keep the closure finite), and right weakenings such that the conclusion have just one formula in the succedent.

Inspecting previous proofs of cut-elimination one can observe that eliminating cuts we do not extend the extended closure of a proof.

Lemma 4.2.10. *Feasible disjunction property with hypotheses: Let π be a G_L proof of $(\Gamma \Rightarrow \Box A_0 \vee \Box A_1)$ where Γ is a set of Harrop formulas. Then we can construct in polynomial time a G_L proof σ of $(\Gamma \Rightarrow \Box A_i)$ for some $i \in \{0, 1\}$.*

Proof of Lemma 4.2.10. To construct a proof in polynomial time our strategy is to find the appropriate sequent in the closure of the proof π. By Theorem 4.2.4 or 4.2.5 there is an almost-cut-free proof π' of the same sequent.

Consider the proof π' backwards. We claim that either of $(\Gamma \Rightarrow \Box A_i)$ is in the closure of π', and hence in the closure of π.

Any inference we reach before we reach a $\Box_L$ inference, a cut, or an initial sequent without passing a $\Box_L$ inference or a cut (let us call this part of π' the lower part of π') has the property that its premiss(es) has (have) in antecedent again only Harrop formulas . So we can always continue considering a premiss.

At the top of the lower part of π', we finally reach at each branch on the level before a $\Box_L$ inference or a cut, or on the level of an initial sequent, either of following situations:

- $(\Box\Gamma' \Rightarrow \Box A_i)$ where $\Box\Gamma'$ are Harrop subformulas of Γ.
  Then by a similar argument as used in Theorem 4.2.6 we conclude that $(\Box\Gamma' \Rightarrow \Box A_i) \in Cl^+(\pi')$.

- $(\Box\Gamma' \Rightarrow \Box B)$, where $\Box\Gamma'$ are Harrop subformulas of Γ and $\Box B$ a subformula of a Harrop disjunction $(\neg\Box B \vee H)$ or of $\neg\Box B$ occurring as a subformula in Γ. Then by a similar argument as used in Theorem 4.2.6 we conclude that $(\Box\Gamma' \Rightarrow \Box B) \in Cl^+(\pi')$.

- $(\Box B \Rightarrow \Box B)$ where $\Box B$ is a Harrop subformula of Γ. It is an initial sequent and it cannot have other form because of restriction to Harrop formulas. $(\Box B \Rightarrow \Box B) \in Cl^+(\pi')$.

We have shown that all sequents from the top of the lower part of π' are in $Cl^+(\pi')$.

Now we use the extended closure to conclude that $(\Gamma \Rightarrow \Box A_i)$ is in the closure of π' (to "restore" Γ in the antecedent using sequents from the top of the lower part of π', the left inferences of the lower part of π', and the closure of π').

We reason by induction on number of left inferences in the lower part of π'.

- First step is there is no left inference in the lower part of π'. In this case there must be at least $\vee$-r inference introducing $\Box A_0 \vee \Box A_1$ followed by a weakening inference introducing say $\Box A_0$ and we have $(\Gamma \Rightarrow \Box A_1)$ at the top of the lower part of π' and hence in the closure of π' (or other way round); or a weakening inference introducing $\Box A_0 \vee \Box A_1$ and we have both $(\Gamma \Rightarrow \Box A_i)$ at the top of the lower part of π' and hence in the closure of π'.

- Consider there are some left inferences in the lower part of π'.

  Observe that one-premiss inferences of the lower part of π' have the following property: if its premiss is in $Cl^+(\pi')$ then the conclusion is in $Cl^+(\pi')$ as well.

  - For weakening it is obvious from definition of the extended closure.
  - For a $\Box_T$ inference with $\Box C$ principal we use a cut on its premiss and a sequent $(\Box C \Rightarrow C)$ from $Cl^+(\pi')$ to conclude that its conclusion is in $Cl^+(\pi')$ as well.
  - For a $\wedge$-l inference with $C \wedge D$ principal we use two cuts on its premiss and sequents $(C \wedge D \Rightarrow C)$ and $(C \wedge D \Rightarrow D)$ from $Cl^+(\pi')$ to conclude that its conclusion is in $Cl^+(\pi')$ as well.
  - For a $\neg$-l inference with $\neg\Box C$ principal we use a cut on its premiss and a sequent $(\Box C, \neg\Box C \Rightarrow \emptyset)$ from $Cl^+(\pi')$ to conclude that its conclusion is in $Cl^+(\pi')$ as well.

  So if the last inference of π' is one of these, we apply the induction hypotheses to its premiss and the result applies to its conclusion as well.

Consider the last inference of π' is a left disjunction inference with $(\neg\Box B \vee H)$ principal:

$$\frac{\Gamma', \neg\Box B \Rightarrow \Box A_0 \vee \Box A_1 \qquad \Gamma', H \Rightarrow \Box A_0 \vee \Box A_1}{\Gamma', \neg\Box B \vee H \Rightarrow \Box A_0 \vee \Box A_1}$$

We first briefly show that if $(\Delta, \neg\Box B \Rightarrow \Box C) \in Cl^+(\pi')$ then either $(\Delta \Rightarrow \Box C) \in Cl^+(\pi')$ or $(\Delta \Rightarrow \Box B) \in Cl^+(\pi')$:

Obviously, thanks the occurrence of $\neg\Box B$, $(\Delta, \neg\Box B \Rightarrow \Box C)$ is not a critical sequent. Consider possibilities how $\neg\Box B$ can have appeared: if closing under weakening, we have that $(\Delta \Rightarrow \Box C) \in Cl^+(\pi')$. If closing under cut, the other premiss cannot be a critical sequent for the same reason - the occurrence of $\neg\Box B$. So it must be one of added sequents and the only possibility is $(\Box B, \neg\Box B \Rightarrow \emptyset)$. In that case $\Box C$ must have been introduced by weakening and we have $(\Delta \Rightarrow \Box B) \in Cl^+(\pi')$.

Now we apply the induction hypothesis to the premisses of the left disjunction inference to obtain $(\Gamma', \neg\Box B \Rightarrow \Box A_i) \in Cl^+(\pi')$ and $(\Gamma', H \Rightarrow \Box A_j) \in Cl^+(\pi')$. As we have shown, there are two possibilities:

- If $(\Gamma' \Rightarrow \Box A_i) \in Cl^+(\pi')$ we obtain by the closure under weakening $(\Gamma', \neg\Box B \vee H \Rightarrow \Box A_i) \in Cl^+(\pi')$ and we are done.
- If $(\Gamma' \Rightarrow \Box B) \in Cl^+(\pi')$, we use a sequent $(\neg\Box B \vee H, \Box B \Rightarrow H)$ from the extended closure and obtain, by a cut,

  $$(\Gamma', \neg\Box B \vee H \Rightarrow H) \in Cl^+(\pi').$$

  By another cut with $(\Gamma', H \Rightarrow \Box A_j) \in Cl^+(\pi')$ we obtain

  $$(\Gamma', \neg\Box B \vee H, \Rightarrow \Box A_j) \in Cl^+(\pi').$$

QED

4.3 Feasible interpolation

Theorem 4.3.1. *Feasible interpolation theorem for modal logic L: Let π be a G_L proof of*

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0 \vee \Box A_1$$

Then it is possible to construct a circuit $C(x)$ whose size is polynomial in the size of π such that for every input $a \in \{0,1\}^n$, if $C(a) = i$, then $\Box A_i$ where we substitute for variables x_j $\bot$, if $a_j = 0$, and $\top$, if $a_j = 1$, is a L tautology.

PROOF OF THEOREM 4.3.1. For given input a consider a proof resulting from π by substituting for variables x_j $\bot$, if $a_j = 0$, and $\top$, if $a_j = 1$. The new proof ends with the sequent $(\Box\top \vee \Box\bot \Rightarrow \Box A_0[\bar{x}/a] \vee \Box A_1[\bar{x}/a])$. $(\Box\top \vee \Box\bot)$ is provable by a proof of constant size and thus by a cut we easily obtain a proof of $(\emptyset \Rightarrow \Box A_0[\bar{x}/a] \vee \Box A_1[\bar{x}/a])$ of size polynomial in the size of the original proof. Now the corollary follows from the theorem 4.2.6 - we can decide in polynomial time which disjunct is true and hence it can be computed by a circuit of polynomial size. QED

The intuitive meaning of our version of the interpolation theorem is: if we fix truth values of common variables of A_0 and A_1 by $\Box$ (this means in all the accesible worlds) and we know the values, than, having a proof of

$$(\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0 \vee \Box A_1),$$

we can check which of the disjuncts is true.

The variables x_i are not required to be the only common variables of A_0 and A_1, but the other cases do not seem to be applicable.

Moreover, if x_i are the only common variables and $A_0(\vec{x}, \vec{y}) \vee A_1(\vec{y}, \vec{z})$ is a classical tautology with $\vec{x}, \vec{y}$ and $\vec{z}$ disjoint sets of variables, then

$$(\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0 \vee \Box A_1)$$

is a L tautology:

Lemma 4.3.2. *Let the sequent $(\emptyset \Rightarrow A_0(\vec{x}, \vec{y}) \vee A_1(\vec{y}, \vec{z}))$ be provable in the calculus G (with $\vec{y}$ and $\vec{z}$ disjoint sets of variables). Then the sequent*

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{y}, \vec{z})$$

is provable in the calculus G_L.

PROOF OF LEMMA 4.3.2. It follows from the Craig's interpolation theorem that there is an interpolant $I(\vec{x})$ such that sequents $(\neg I(\vec{x}) \Rightarrow A_0(\vec{x}, \vec{y}))$ and $(I(\vec{x}) \Rightarrow A_1(\vec{y}, \vec{z}))$ have G proofs. Then both $(\Box\neg I(\vec{x}) \Rightarrow \Box A_0(\vec{x}, \vec{y}))$ and $(\Box I(\vec{x}) \Rightarrow \Box A_1(\vec{y}, \vec{z}))$ are G_L provable and so is $(\Box I(\vec{x}) \vee \Box\neg I(\vec{x}) \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{y}, \vec{z}))$.

Because

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box I(\vec{x}) \vee \Box\neg I(\vec{x})$$

is G_L provable (it can be easily proved by induction on the weight of I), we have by a cut

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{y}, \vec{z})$$

provable in the calculus G_L. QED

4.3.1 Complexity consequences

The main aim of proving feasible interpolation theorems for a proof system is that it can be applied to prove lower bounds on size of proofs for the proof system. Sometimes lower bounds are obtained under plausible complexity assumptions like that factoring is hard to compute. Since we have proved a general feasible interpolation theorem and not a monotone interpolation theorem, we cannot omit some complexity assumptions to obtain lower bounds for proof systems we consider.

Since all modal logics we consider here are known to be PSPACE-complete ([33],[13]), we could use an assumption PSPACE$\not\subseteq$NP/poly to derive the existence of modal tautologies that have not polynomial size proofs. The point of using feasible interpolation instead, however together with some complexity assumptions, is that it enables to construct concrete examples of hard modal tautologies.

We can use either Razborov's [42] method and obtain lower bounds under assumption that there exist pseudorandom generators, or the method from [7] and obtain lower bounds under assumption that factoring is hard to compute.

We present here a simple argument based on ideas of Mundici [36, 37], Krajíček [29] and taken from Pudlák [40]. It uses a cryptographical assumption that there are two disjoint NP sets which cannot be separated by a set in P/poly (this assumption follow e.g. from the one that factoring is not in P). Mundici used his argument to conclude that not all Craig interpolants in classical propositional logic are of polynomial size. Modifying his argument using Krajíček's idea we may use it to conclude that not all tautologies have polynomial size proofs.

Corollary 4.3.3. *Let L be one of modal logics* ***K****,* ***T****,* ***K4****,* ***S4****,* ***GL****,* ***K4Grz****,* ***S4Grz****. Suppose $NP \cap co-NP \not\subseteq P/poly$. Then there are tautologies which do not have proofs in G_L of size polynomial in the size of the proved formula.*

PROOF OF COROLLARY 4.3.3. Suppose there are two NP disjoint sets X and Y which cannot be separated by a set in *P/poly*. Let n be a natural number. Now define the disjoint sets $X \cap \{0,1\}^n$ and $y \cap \{0,1\}^n$ by $\{\bar{a} | \exists \bar{b} \neg A_0(\bar{a}, \bar{b})\}$ and $\{\bar{a} | \exists \bar{c} \neg A_1(\bar{a}, \bar{c})\}$ where A_0, A_1 are propositional formulas of size polynomial in n. Since the sets are disjoint, $A_0 \vee A_1$ is a classical tautology and the sequent $(\emptyset \Rightarrow A_0(\bar{x}, \bar{y}) \vee A_1(\bar{x}, \bar{z}))$ is provable in G. By Lemma 4.3.2, the sequent

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0(\bar{x}, \bar{y}) \vee \Box A_1(\bar{x}, \bar{z})$$

is provable in G_L. If it had a polynomial size proof, we would have by Theorem 4.3.1 a polynomial size circuit separating $X \cap \{0,1\}^n$ and $Y \cap \{0,1\}^n$, which is a contradiction. QED

Another consequence of feasible interpolation theorem is a speed-up between classical propositional calculus and modal calculi. Such a speed up would follow already from the assumption that PSPACE$\not\subseteq$NP/poly but without concrete examples of tautologies that separate the two systems in this sense.

Corollary 4.3.4. *Let L be one of modal logics* ***K****,* ***T****,* ***K4****,* ***S4****,* ***GL****,* ***K4Grz****,* ***S4Grz****. Then, assuming that factoring is not computable in polynomial time, there is more then polynomial speed-up between proofs in propositional classical calculus and proofs in L.*

PROOF OF COROLLARY 4.3.4. In [7], concrete examples of propositional tautologies are constructed that have polynomial size proofs in classical propositional logic and cannot have polynomial size proofs in any system admitting feasible interpolation theorem. QED

4.3.2 Concluding remarks

Since feasible disjunction property for a wide class of modal logics, so called *extensible logics*, has been proved by Jeřábek [27] using Frege proof systems, feasible interpolation theorem and its consequences automatically apply to all these logics as well.

Our results also relate to intuitionistic logic using well known translations from intuitionistic logic to logics **S4**, **S4Grz** which can be found e.g. in [13]. We only use the following form of the translation:

- $p^\Box \equiv \Box p$; $\bot^\Box \equiv \bot$
- $(A \wedge B)^\Box \equiv (A^\Box \wedge B^\Box)$
- $(A \vee B)^\Box \equiv (\Box A^\Box \vee \Box B^\Box)$
- $(A \to B)^\Box \equiv \Box(A^\Box \to B^\Box)$

The sequent calculi we have chosen are, from the complexity point of view, as general as possible. In particular, they polynomially simulate various other structural formulations of sequent calculi (e.g. versions with atomic axioms, with multisets instead of sets, cut free versions), as well as appropriate standard Frege systems. It has been shown by Jeřábek [27] that all Frege systems for a wide class of modal logics, called extensible logics, are polynomially equivalent. So our results apply to most of proof systems for modal logics that are used.

A natural and desired next step would be to prove a monotone version of feasible interpolation theorem.

From our proof of uniform interpolation, one cannot guess how the circuit looks like. We only use the fact that polynomial time computations can be treated by polynomial size circuits (see e.g. [?]). So we did not go further to investigate the possibility to prove monotone feasible interpolation theorem using the same method, where a monotone circuit of polynomial size is required to be extracted from a proof. This would enable to remove complexity assumptions from lower bounds statement.

However, it has been shown in much recent work of Hrubeš [26] using a different method that modal logics **K**, **K4**, **S4**, **GL** satisfy monotone feasible interpolation theorem, and concrete examples of hard tautologies has been presented that require Frege proofs with exponential number of proof lines.

Bibliography

[1] A. Avron, *On modal systems having arithmetical interpretations*, The Journal of Symbolic Logic **49** (1984), 935–942.

[2] P. Beam, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, *Lower bounds on Hilbert's Nullstellensatz and propositional proofs*, Proc. London Math. Soc. **73** (1996), no. 3, 1–26.

[3] M. Bílková, *Uniform interpolation and propositional quantifiers in modal logics*, to appaer in Studia Logica.

[4] ———, *Feasible disjunction and interpolation properties in modal logic S4 - abstract*, The Bulletin of Symbolic Logic **9** (2003), 87.

[5] P. Blackburn, M. de Rijke, and Y. Venema, *Modal logic*, Cambridge University Press, 2001.

[6] M. L. Bonet, T. Pitassi, and R. Raz, *Lower bounds for cutting planes proofs with small coeficients*, The Journal of Symbolic Logic **62** (1997), no. 3, 708–728.

[7] ———, *No feasible interpolation for TC^0-frege proofs*, Proceedings of the 38th Annual Symposium on Foundations of Computer Science, Piscataway, NJ, IEEE Computer Society Press, Silver Spring (1997), 254-263.

[8] G. Boolos, *The logic of provability*, Cambridge University Press, New York and Cambridge, 1993.

[9] R.A. Bull, *On modal logic with propositional quantifiers*, The Journal of Symbolic Logic **34** (1969), 257–263.

[10] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A.A. Razborov, and J. Sgall, *On constant depth frege systems with a modular counting connective*, Computational Complexity **6** (1996/97), 256–298.

[11] S. R. Buss and G. Mints, *The complexity of the disjunction and existence properties in intuitionistic logic*, Annals of Pure and Applied Logic **99** (1999), 93–104.

[12] S. R. Buss and P. Pudlák, *On the computational content of intuitionistic propositional proofs*, Annals of Pure and Applied Logic **109** (2001), 49–64.

[13] A. Chagrov and M. Zakaryasschev, *Modal logic*, Oxford University Press, 1998.

[14] W. Craig, *Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory*, The Journal of Symbolic Logic **22** (1957), no. 3, 269–285.

[15] M. Ferrari, C. Fiorentini, and G. Fiorino, *On the complexity of the disjunction property in intuitionistic and modal logics*, ACM Transactions on Computational Logic (TOCL) **6** (2005), no. 3, 519–538.

[16] K. Fine, *Propositional quantifiers in modal logic*, Theoria **36** (1970), 336–346.

[17] D.M. Gabbay and L. Maksimova, *Interpolation and definability: Modal and intuitionistic logics*, Oxford University Press, 2005.

[18] G. Gentzen, *Collected works*, North-Holland, Amsterdam, 1969.

[19] S. Ghilardi and M. Zawadovski, *A sheaf representation and duality for finitely presented heyting algebras*, The Journal of Symbolic Logic **60** (1995), 911–939.

[20] ———, *Undefinability of propositional quantifiers in the modal system S4*, Studia Logica **55** (1995), 259–271.

[21] Z. Gleit and W. Goldfarb, *Characters and fixed points in provability logic*, Notre Dame Journal of Formal Logic **31** (1990), no. 1, 26–36.

[22] A. Goerdt, *Efficient interpolation for the intuitionistic sequent calculus*, Technische Universität Chemnitz preprint **CSR-00-02** (2000).

[23] R. Harrop, *Concerning formulas of the types $A \to B \vee C, A \to (\exists x B(x))$ in intuitionistic formal systems*, The Journal of Symbolic Logic **25** (1960), no. 1, 27–32.

[24] A. Heuerding, *Sequent calculi for proof search in some modal logics*, Ph.D. thesis, University of Bern, Switzerland, 1998.

[25] A. Heuerding, M. Seyfried, and H. Zimmermann, *Efficient loop-check for backward proof search in some non-classical propositional logics*, Tableaux (1996), 210–225.

[26] P. Hrubeš, *Lower bounds for modal logics*, submitted (2006).

[27] E. Jeřábek, *Frege systems for extensible modal logics*, to appear in Annals of Pure and Applied Logic (2005).

[28] M. Kracht, *Tools and techniques in modal logic*, Elsevier, 1999.

[29] J. Krajíček, *Lower bounds to the size of constant-depth propositional proofs*, The Journal of Symbolic Logic **59** (1994), 73–86.

[30] ———, *Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic*, The Journal of Symbolic Logic **62** (1997), 457–486.

[31] P. Kremer, *Quantifying over propositions in relevance logics: Non-axiomatizibility of* $\forall$ *and* $\exists$, The Journal of Symbolic Logic **58** (1993), 334–349.

[32] ———, *On the complexity of propositional quantification in intuitionistic logic*, The Journal of Symbolic Logic **62** (1997), 529–544.

[33] R. E. Ladner, *The computational complexity of provability in systems of modal propositional logic*, SIAM Journal of Computation **6** (1977), 3:467–480.

[34] L. Maksimova, *The Beth properties, interpolation, and amalgamability in varieties of modal algebras*, Soviet Matematics Doklady **44** (1992), 327–331.

[35] ———, *Definability and interpolation in classical modal logics*, Contemporary Mathematics **131** (1992), 583–599.

[36] D. Mundici, *Complexity of Craig's interpolation*, Fundamenta Informaticae **5** (1982), 261–278.

[37] ———, *A lower bound for the complexity of Craig's interpolants in sentential logic*, Archiv für Math. Logic **23** (1983), 27–36.

[38] S. Negri and J. von Plato, *Structural proof theory*, Cambridge University Press, 2001.

[39] A. Pitts, *On an interpretation of second order quantification in first order intuitionistic propositional logic*, The Journal of Symbolic Logic **57** (1992), 33–52.

[40] P. Pudlák, *Lower bounds for resolution and cutting planes proofs and monotone computations*, The Journal of Symbolic Logic **62** (1997), 981–998.

[41] ———, *On the complexity of propositional calculus*, Sets and Proofs, Invited papers from Logic Colloquium'97, Cambridge Univ. Press, 1999, pp. 197–218.

[42] A. Razborov, *Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic*, Izvestiya of the R.A.N. **59** (1995), no. 2, 201–224.

[43] L. Reidhaar-Olson, *A new proof of the fixed point theorem of provability logic*, Notre Dame Journal of Formal Logic **31** (1990), no. 1, 37–43.

[44] G. Sambin, *An effective fixed-point theorem in intuitionistic diagonalizable algebras*, Studia Logics **35** (1976), 345–361.

[45] G. Sambin and G. Boolos, *Provability: The emergence of a mathematical modality*, Studia Logica **50** (1991), 1–23.

[46] G. Sambin and S. Valentini, *The modal logic of provability. the sequential approach*, Journal of Philosophical Logic **11** (1982), 311–342.

[47] V. Yu. Shavrukov, *Subalgebras of diagonalizable algebras of theories containing arithmetic*, Ph.D. thesis, Dissertationes Mathematicae CCCXXIII, Polska Akademia Nauk, Mathematical Institute, Warszawa, 1993.

[48] C. Smoryński, *Beth's theorem and self-referential sentences*, Logic Colloquium 77 (1978), 253–261.

[49] R. Solovay, *Provability interpretations of modal logics*, Israel Journal of Mathematics **25** (1976), 287–304.

[50] G. Takeuti, *Proof theory*, North-Holland, Amsterdam, 1987.

[51] A. S. Troelstra and H. Schwichtenberg, *Basic proof theory*, Cambridge University Press, 1996.

[52] A. Visser, *Bisimulations, model descriptions and propositional quantifiers*, Logic Group Preprint Series, Utrecht University **161** (1996).

[53] V. Švejdar, *On provability logic*, Nordic Journal of Philosophical Logic **4** (2000), no. 2, 95–116.

[54] H. Wansing, *Sequent proof systems for modal logics*, Handbook of Philosophical Logic (D. Gabbay and F. Guenthner, eds.), vol. 8, Kluwer Academic Publishers, 2002.

[55] F. Wolter, *Independent fusions of modal logics revisited*, Advances in Modal Logic (M. Kracht, M. de Rijke, H. Wansing, and M. Zakaryaschev, eds.), Stanford CSLI, 1997.

Errata.

- p. 25 Proof of Corollary 2.2.14. the removed symbol should be "|".
- p. 94 the missing reference reads:
  C. Papadimitriu, *Computational complexity*, Addison-Wesley, 1994.
- p. 91 $\Box A_0(\vec{x},\vec{y}) \vee \Box A_1(\vec{y},\vec{z})$ should be $\Box A_0(\bar{x},\bar{y}) \vee \Box A_1(\bar{x},\bar{z})$ instead.