FEASIBLE DISJUNCTION PROPERTY AND FEASIBLE INTERPOLATION IN MODAL LOGIC

MARTA BÍLKOVÁ

Abstract. We prove Feasible Disjunction Property for modal propositional logics **K**, **K4**, **K4Grz**, **GL**, **T**, **S4**, and **S4Grz**, by a uniform and simple proof based on modular modal sequent proof systems. We derive Feasible Interpolation Theorem for all the logics. Our results are weaker than Hrubeš' obtained in [9].

1. Introduction

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.

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 work on feasible disjunction property in case of modal logics was originally motivated by the fact that it can be used to derive feasible interpolation theorem and, 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 [9] that Frege calculi for modal logics **K**, **K4**, **S4**, **GL** satisfy the stronger interpolation property - monotone feasible interpolation - and therefore examples of hard modal tautologies can be obtained without assumptions.

Our complexity results are weaker and therefore our paper is rather a technical note whose aim is a didactic one - to present uniform and simple proofs of the two feasible properties in case of modal logics, which makes clear how to extract a computational (or a constructive) information from modal sequent proofs.

We concentrate on the general (nonmonotone) feasible interpolation theorem. We prove the theorem for modal propositional logics **K**, **K4**, **K4Grz**, **GL**, **T**, **S4**, and **S4Grz**.

Our proof is a simplification and generalization of the proof for logic **S4** in [1]. The proof technique comes from [4] and [5] where intuitionistic logic is considered. It derives feasible interpolation from so called *Feasible Disjunction Property* (FDP)

The work was supported by ITI research center 1M0021620808(1M0545).

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 [5] 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, to keep an analogy with intuitionistic propositional logic, Harrop. It is similar to the class defined in [7] or [1] 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 [16], which was overlooked in [7] where it was derived similarly as in [5] only using Harrop hypotheses and only for logic **S4**.

Ferrari, Fiorentini, and Fiorino in [7] 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 [7] 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 4.2, as well as well developed for modal logics.

Our approach yields a simple and transparent proof of feasible disjunction and interpolation properties in modal logics which we find, in case of normal modal logics, simpler than the one presented in [7]. However, [7] 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 [10] 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 [6]. From this viewpoint, our results generalize that for intuitionistic logic stated at [5].

2. Sequent calculi

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**. For basic information on modal logics consult e.g. [6, 2]

First we define modal sequent calculi extending the following classical system G:

Definition 2.1. 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 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. 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 $(p \Rightarrow p)$. So our results hold for calculi with the atomic version of initial sequents as well.

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 $d(A) = \Box(A \rightarrow \Box A)$.
For **S4Grz**, $\Gamma^\star = \Box\Gamma$ and $d(A) = \Box(A \rightarrow \Box A)$.
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 2.2. A *critical sequent* is a sequent of the form $\Box\Gamma \Rightarrow \Box A$ which is the conclusion of a $\Box_L$ inference.

3. 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.

3.1. **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).

In contrast to the case of intuitionistic logic treated in [5] 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.

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 3.1. 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.

For **S4Grz**, the closure is defined as follows:

Definition 3.2. 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.

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:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma \Rightarrow \Box A}{\Box\Gamma \Rightarrow \neg A, \Box A}\,\text{weak}}{\Box\Gamma \Rightarrow \neg A \vee \Box A}\,\vee\text{-r}}{\Box\Gamma, \Box D \Rightarrow \neg A \vee \Box A}\,\text{weak}}{\Box\Gamma \Rightarrow \Box(\neg A \vee \Box A)}\,\Box_{S4Grz}$$

and so we can always construct a proof of a sequent from the closure in polynomial time.

3.2. **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 [5], 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 3.3. 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 3.4. *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 3.4. For a cut elimination proof for classical logic based on sets see e.g. [19]. A proof for modal logics can be found in [18].

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.

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. [19].

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 $\Box A$).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4} \qquad A, \Gamma' \Rightarrow \Delta}{\Box\Gamma, A, (\Gamma'\backslash \Box A) \Rightarrow \Delta}\,\text{cut} \qquad \Box\Gamma \Rightarrow A}{(\Box\Gamma\backslash A), \Gamma'\backslash (\Box A, A) \Rightarrow \Delta}\,\text{cut}}{\Box\Gamma, (\Gamma'\backslash \Box A, A) \Rightarrow \Delta}\,\text{weak}$$

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

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 3.5. *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 3.5. 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 $\Box A$).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Box\Gamma, \Box D \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}\,\Box_{S4Grz} \qquad A, \Gamma' \Rightarrow \Delta}{\Box\Gamma, A, (\Gamma'\backslash \Box A) \Rightarrow \Delta}\,\text{cut} \qquad \Box\Gamma, \Box D \Rightarrow A}{(\Box\Gamma\backslash A), \Box D, (\Gamma'\backslash \Box A, A) \Rightarrow \Delta}\,\text{cut}}{\Box\Gamma, \Box D, (\Gamma'\backslash \Box A, A) \Rightarrow \Delta}\,\text{weak} \qquad \Box\Gamma \Rightarrow \Box D}{(\Box\Gamma\backslash \Box D), (\Gamma'\backslash \Box A, A, \Box D) \Rightarrow \Delta}\,\text{cut}}{\Box\Gamma, (\Gamma'\backslash \Box A, A) \Rightarrow \Delta}\,\text{weak}$$

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.

3.3. **Feasible Disjunction Property.**

Theorem 3.6. *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 3.6. By Theorem 3.4 or Theorem 3.5, 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 $\Box_L$ inference 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

3.4. **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 [8], 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[1] to prove the feasible interpolation theorem, we include the proof here. It is going to be more complicated then the previous one.

Definition 3.7. **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.

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 3.8. 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 $(\Box A \Rightarrow \Box A)$,

[1]The disjunction property for modal logics as stated in this paper also holds for a class of formulas defined as below 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 below. 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.

- 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 3.9. *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 3.9. To construct a proof in polynomial time our strategy is to find the appropriate sequent in the closure of the proof π. By Theorem 3.4 or 3.5 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 3.6 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 3.6 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. Feasible interpolation

Theorem 4.1. *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 4.1. 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 3.6 - 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 $A_0(\vec{x}, \vec{y}) \vee A_1(\vec{x}, \vec{z})$ 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 4.2. *Let the sequent $(\emptyset \Rightarrow A_0(\vec{x}, \vec{y}) \vee A_1(\vec{x}, \vec{z}))$ be provable in the calculus G (with $\vec{y}$ and $\vec{z}$ disjoint sets of variables). Then the sequent*

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{x}, \vec{z})$$

is provable in the calculus G_L.

Proof of Lemma 4.2. 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 $(I(\vec{x}) \Rightarrow A_1(\vec{x}, \vec{z}))$ have G proofs. Then both $(\Box\neg I(\vec{x}) \Rightarrow \Box A_0(\vec{x}, \vec{y}))$ and $(\Box I(\vec{x}) \Rightarrow \Box A_1(\vec{x}, \vec{z}))$ are G_L provable and so is $(\Box I(\vec{x}) \vee \Box\neg I(\vec{x}) \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{x}, \vec{z}))$.

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

$$\Box x_1 \vee \Box\neg x_1, \ldots, \Box x_n \vee \Box\neg x_n \Rightarrow \Box A_0(\vec{x}, \vec{y}) \vee \Box A_1(\vec{x}, \vec{z})$$

provable in the calculus G_L. QED

4.1. **Complexity consequences.** It has been shown in much recent work of Hrubeš [9] 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.

However, we include some complexity remarks involving our weaker version of interpolation here.

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 ([12],[6]), 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 [17] method and obtain lower bounds under assumption that there exist pseudorandom generators, or the method from [3] and obtain lower bounds under assumption that factoring is hard to compute.

We present here a simple argument based on ideas of Mundici [13, 14], Krajíček [11] and taken from Pudlák [15]. 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. *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. 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 4.2, 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 4.1 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 4.4. *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 4.4. In [3], 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

4.2. **Concluding remarks.** Since feasible disjunction property for a wide class of modal logics, so called *extensible logics*, has been proved by Jeřábek [10] 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 [6]. 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 [10] 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.

REFERENCES

1. M. Bílková, *Feasible disjunction and interpolation properties in modal logic S4 - abstract*, The Bulletin of Symbolic Logic **9** (2003), 87.
2. P. Blackburn, M. de Rijke, and Y. Venema, *Modal logic*, Cambridge University Press, 2001.
3. M. L. Bonet, T. Pitassi, and R. Raz, *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.
4. 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.
5. S. R. Buss and P. Pudlák, *On the computational content of intuitionistic propositional proofs*, Annals of Pure and Applied Logic **109** (2001), 49–64.
6. A. Chagrov and M. Zakaryasschev, *Modal logic*, Oxford University Press, 1998.
7. 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.
8. 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.
9. P. Hrubeš, *Lower bounds for modal logics*, submitted (2006).
10. E. Jeřábek, *Frege systems for extensible modal logics*, to appear in Annals of Pure and Applied Logic (2005).
11. J. Krajíček, *Lower bounds to the size of constant-depth propositional proofs*, The Journal of Symbolic Logic **59** (1994), 73–86.
12. R. E. Ladner, *The computational complexity of provability in systems of modal propositional logic*, SIAM Journal of Computation **6** (1977), 3:467–480.
13. D. Mundici, *Complexity of Craig's interpolation*, Fundamenta Informaticae **5** (1982), 261–278.

14. ———, *A lower bound for the complexity of Craig's interpolants in sentential logic*, Archiv für Math. Logic **23** (1983), 27–36.
15. P. Pudlák, *Lower bounds for resolution and cutting planes proofs and monotone computations*, The Journal of Symbolic Logic **62** (1997), 981–998.
16. ———, *On the complexity of propositional calculus*, Sets and Proofs, Invited papers from Logic Colloquium'97, Cambridge Univ. Press, 1999, pp. 197–218.
17. 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.
18. G. Sambin and S. Valentini, *The modal logic of provability. the sequential approach*, Journal of Philosophical Logic **11** (1982), 311–342.
19. G. Takeuti, *Proof theory*, North-Holland, Amsterdam, 1987.

Department of Logic, Charles University in Prague, Celetna 20, 116 42 Prague 1, Czech Republic

Institute of Computer Science, Academy of Sciences of the Czech Republic, Pod Vodarenskou vezi 2, 182 07 Prague 8, Czech Republic

E-mail address: bilkova@cs.cas.cz