A new method for bounding the complexity of modal logics

David Basin[1], Seán Matthews[2], Luca Viganò[2]

[1] Institut für Informatik, Universität Freiburg
Am Flughafen 17, D-79110 Freiburg, Germany
basin@informatik.uni-freiburg.de
[2] Max-Planck-Institut für Informatik
Im Stadtwald, D-66123 Saarbrücken, Germany
sean@mpi-sb.mpg.de, luca@mpi-sb.mpg.de

Abstract. We present a new proof-theoretic approach to bounding the complexity of the decision problem for propositional modal logics. We formalize logics in a uniform way as sequent systems and then restrict the structural rules for particular systems. This, combined with an analysis of the accessibility relation of the corresponding Kripke structures, yields decision procedures with bounded space requirements. As examples we give $O(n \log n)$ space procedures for the modal logics K and T.

1 Introduction

We present a new proof-theoretic approach to bounding the complexity of the decision problem for propositional modal logics. We formalize logics in a uniform way as cut-free labelled sequent systems and then restrict the structural rules for particular systems. This, combined with an analysis of the accessibility relation of the corresponding Kripke structures, yields decision procedures with space requirements that are easily bounded. As examples we give $O(n \log n)$ space decision procedures for the modal logics K and T.

This paper is based on previous work where we give a *labelled deduction* framework, based on Kripke semantics, in which we are able to formalize a large class of propositional modal logics (essentially those with accessibility relations axiomatizable using Horn-clauses; e.g. K, T, S4, S5, etc.) as labelled natural deduction systems [2]. There we show that modal logics in this class can be decomposed into two separated parts: a fixed base logic, and a relational theory, which we extend to generate particular logics in the class.

Now we use this framework to develop complexity results. We begin by showing a bijection between our labelled natural deduction systems and cut-free labelled sequent systems with a subformula property. This provides us with a bound on the number of different formulas that can appear in a proof. However it does not bound the number of times a formula can appear in a sequent. To do this we prove that we can bound applications of contraction. In general this is impossible (in the same way that it is sometimes necessary to contract universally quantified formulas in first-order logic [5], or implication in intuitionistic propositional logic [7]). However we show that bounds do exist for particular modal logics. Furthermore, our systems provide for restricted reasoning about the accessibility relation that we exploit to factor complexity questions about the accessibility relation out of our analysis. Taken together these results allow us to bound the depth of proofs and the size of sequents arising in them, and thus, by 'resource aware' programming, to provide PSPACE upper bounds.

The space bounds we arrive at are not new; they were recently discovered, using different techniques, by Hudelmaier [8]. What is new is the use of a labelled sequent calculus to provide a framework for complexity bounds combined with the analysis of contraction for particular logics in this general setting. We view this as a first step towards a general framework for both applying proof theory to the analysis of the decision problem for families of modal, and other similarly formalized non-classical, logics, see [1,14], and for implementing decision procedures for these logics.

The remainder of this paper is organized as follows. In §2 we review the essentials of our labelled natural deduction systems and show that they are intertranslatable with the cut-free labelled sequent systems we use here. In §3 we show how contraction can be bounded in our sequent systems for the modal logics K and T. In §4 we show that these results can be combined with bounds on relational reasoning to bound the space needed in the search for a proof. In §5 we discuss related work, and in §6 draw conclusions. Due to lack of space, proofs have been omitted or considerably shortened; see [14] for details.

2 Natural deduction and sequent systems

In this paper we use cut-free labelled sequent systems for modal logics. To show their soundness and completeness with respect to standard Kripke semantics, we use sound and complete natural deduction systems from earlier work [2] and show that our sequent systems are intertranslatable with them. In this way it follows that cut is admissible; i.e., rather than eliminating cut directly, we exploit results we already have for natural deduction systems.

2.1 Labelled natural deduction systems

Let W be a denumerable set of variables, called *labels*, and R a binary relation over W. We factor our presentations into two parts, a fixed *base* logic and a varying *relational theory*, corresponding to the two sorts of syntactic entities we consider: labelled well-formed formulas (*lwffs*), $x{:}A$, which pair a label x and a modal formula A, and relational well-formed formulas (*rwffs*), $x\,R\,y$. The lwff $x{:}A$ expresses that the formula A holds at world x, and the rwff $x\,R\,y$ expresses that (x, y) is in the accessibility relation R. The following rules define the base logic for the (functionally complete) $\bot/\!\!\to\!/\Box$ fragment of our natural deduction systems.[1]

[1] Other connectives can be defined in the usual manner, e.g. $\neg A$ as $A \to \bot$ and $\Diamond A$ as $\neg\Box\neg A$, and their corresponding rules derived.

$$\dfrac{\begin{array}{c}[x{:}A \to \bot]\\ \vdots \\ y{:}\bot\end{array}}{x{:}A}\ \bot E \qquad \dfrac{\begin{array}{c}[x{:}A]\\ \vdots \\ x{:}B\end{array}}{x{:}A \to B}\ {\to} I \qquad \dfrac{x{:}A \to B \quad x{:}A}{x{:}B}\ {\to} E \qquad \dfrac{\begin{array}{c}[x\,R\,y]\\ \vdots \\ y{:}A\end{array}}{x{:}\Box A}\ \Box I \qquad \dfrac{x{:}\Box A \quad x\,R\,y}{y{:}A}\ \Box E$$

($\Box I$ has the side condition that y is different from x and does not occur in any assumption on which $y{:}A$ depends other than $x\,R\,y$.) We then generate natural deduction systems for modal logics by extending the base logic with a relational theory, i.e., by adding rules for the accessibility relation R. For instance, if we take the base logic alone we get the system K_{ND} formalizing the modal logic K, from which we can produce the system T_{ND} or $\mathrm{K4}_{ND}$ by adding respectively a rule for reflexivity or transitivity,

$$\dfrac{}{x\,R\,x} \qquad \text{or} \qquad \dfrac{x\,R\,y \quad y\,R\,z}{x\,R\,x}$$

This framework is based on a deliberate compromise where we restrict ourselves to modal logics with accessibility relation axiomatizable in terms of Horn-clauses. In return we have that the formalization of any logic in this class is both sound and complete with respect to the corresponding Kripke semantics and has proof-normalization properties. More specifically, in [2] we prove the following: (i) for logics where the theory of the binary accessibility relation characterizing the Kripke structure is Horn-clause axiomatizable (this is a very large class including almost all the Geach hierarchy, in particular the logics K, T, K4, S4, S5, etc.) the natural deduction systems are sound and complete with respect to the corresponding Kripke semantics, and (ii) proofs can be transformed into an equivalent normal form similar to that defined by Prawitz [12], suitably modified for labelled and relational formulas.

2.2 Labelled sequent systems

Let Γ and Δ (possibly annotated) vary over finite multisets of lwffs and rwffs respectively. The cut-free labelled sequent system K consists of the following axioms and rules, where $\Box R$ has the side condition that y does not occur in $\Gamma, \Delta \vdash \Gamma', x{:}\Box A$.

$$\dfrac{}{x{:}A \vdash x{:}A}\ AXl \qquad \dfrac{}{x\,R\,y \vdash x\,R\,y}\ AXr \qquad \dfrac{}{y{:}\bot \vdash x{:}A}\ \bot L$$

$$\dfrac{\Gamma, \Delta \vdash \Gamma', x{:}A \quad x{:}B, \Gamma, \Delta \vdash \Gamma'}{x{:}A \to B, \Gamma, \Delta \vdash \Gamma'}\ {\to} L \qquad \dfrac{x{:}A, \Gamma, \Delta \vdash \Gamma', x{:}B}{\Gamma, \Delta \vdash \Gamma', x{:}A \to B}\ {\to} R$$

$$\dfrac{\Delta \vdash x\,R\,y \quad y{:}A, \Gamma, \Delta \vdash \Gamma'}{x{:}\Box A, \Gamma, \Delta \vdash \Gamma'}\ \Box L \qquad \dfrac{\Gamma, \Delta, x\,R\,y \vdash \Gamma', y{:}A}{\Gamma, \Delta \vdash \Gamma', x{:}\Box A}\ \Box R$$

$$\dfrac{\Gamma, \Delta \vdash \Gamma'}{\Gamma, \Delta, x\,R\,y \vdash \Gamma'}\ WrL \qquad \dfrac{\Gamma, \Delta \vdash \Gamma'}{x{:}A, \Gamma, \Delta \vdash \Gamma'}\ WlL \qquad \dfrac{\Gamma, \Delta \vdash \Gamma'}{\Gamma, \Delta \vdash \Gamma', x{:}A}\ WlR$$

$$\frac{\Delta, x\,R\,y, x\,R\,y \vdash u\,R\,v}{\Delta, x\,R\,y \vdash u\,R\,v}\ CrL \qquad \frac{x{:}A, x{:}A, \Gamma, \Delta \vdash \Gamma'}{x{:}A, \Gamma, \Delta \vdash \Gamma'}\ ClL \quad \frac{\Gamma, \Delta \vdash \Gamma', x{:}A, x{:}A}{\Gamma, \Delta \vdash \Gamma', x{:}A}\ ClR$$

Analogously to the natural deduction systems, we can then, e.g., obtain the cut-free labelled sequent system T or K4 by extending the relational theory with reflexivity or transitivity, formalized by the rules

$$\frac{}{\Delta \vdash x\,R\,x}\ \mathit{refl} \qquad \text{or} \qquad \frac{\Delta \vdash x\,R\,y \quad \Delta \vdash y\,R\,z}{\Delta \vdash x\,R\,z}\ \mathit{trans}$$

Normalizing natural deduction systems and sequent systems without cut are closely related [4,12,13]. If we write $\Gamma, \Delta \vdash_{ND} x{:}A$ to indicate a derivation of $x{:}A$ from assumptions Γ, Δ in our natural deduction systems, then we have:

Theorem 1. *$\Delta \vdash_{ND} x\,R\,y$ iff $\Delta \vdash x\,R\,y$; and $\Gamma, y_1{:}\neg B_1, \ldots, y_n{:}\neg B_n, \Delta \vdash_{ND} x{:}A$ iff $\Gamma, \Delta \vdash x{:}A, y_1{:}B_1, \ldots, y_n{:}B_n$.*

Proof. (Sketch) We adapt and extend the proof given by Prawitz [12, App. A], to which the reader is referred for details.

Left to right: By induction on the length of normal natural deduction derivations. We consider an application of $\Box I$ as an illustrative case: suppose that from $\Gamma, y_1{:}\neg B_1, \ldots, y_n{:}\neg B_n, \Delta, x\,R\,y \vdash_{ND} y{:}A$ we infer $\Gamma, y_1{:}\neg B_1, \ldots, y_n{:}\neg B_n, \Delta \vdash_{ND} x{:}\Box A$. By the induction hypothesis we have $\Gamma, \Delta, x\,R\,y, \vdash y{:}A, y_1{:}B_1, \ldots, y_n{:}B_n$, and thus $\Gamma, \Delta \vdash x{:}\Box A, y_1{:}B_1, \ldots, y_n{:}B_n$ by $\Box R$ (the side condition for $\Box R$ holds by the side condition for $\Box I$).

Right to left: By induction on the length of the proof of the sequent. We consider an application of $\Box R$ as an illustrative case. By the induction hypothesis, given $\Gamma, \Delta, x\,R\,y \vdash y{:}A, y_1{:}B_1, \ldots, y_n{:}B_n$ we have $\Gamma, y_1{:}\neg B_1, \ldots, y_n{:}\neg B_n, \Delta, x\,R\,y \vdash_{ND} y{:}A$, and we derive $\Gamma, y_1{:}\neg B_1, \ldots, y_n{:}\neg B_n, \Delta \vdash_{ND} x{:}\Box A$ by $\Box I$ (the side condition for $\Box I$ holds by the side condition for $\Box R$).

From Theorem 1 and previous results in [2], it follows that our sequent systems are sound and complete with respect to the corresponding Kripke semantics.

3 Contraction

In this section we show that for particular logics in our framework applications of the contraction rules can be eliminated (in K) or bounded (in T).

We begin by introducing some terminology. We call the formulas that pass through the application of a rule unchanged (they appear in the premises and in the conclusion) the *parametric formulas* of the rule; the formula contracted or introduced in the conclusion is the *principal formula* of the rule, and the formulas from which the principal formula derives are the *active formulas* of the rule. We call *lwff-rules* the rules that have an lwff as principal formula, namely *WlL*, *WlR*, *ClL*, *ClR*, $\to L$, $\to R$, $\Box L$ and $\Box R$. Suppose that a sequent S results from sequents $S_1, \ldots, S_n$ by first applying the lwff-rule ρ_1 and then applying the lwff-rule ρ_2, where (i) each of the premises of ρ_2 results from an application of

ρ_1, (ii) each application of ρ_1 introduces or contracts the same lwff, and (iii) the principal formula of ρ_1 is parametric in the application of ρ_2. We then say that ρ_1 is *permutable* with respect to ρ_2 (ρ_1 *permutes* with respect to ρ_2), if the original inference can be replaced by one in which the sequent S is derived from $S_1, \ldots, S_n$ by applying first ρ_2 and then ρ_1. By inspection of the rules, we have that:

Lemma 2. *Every lwff-rule is permutable with respect to any other lwff-rule, with the exception of* $\Box L$*, which is permutable with respect to every lwff-rule other than* $\Box R$*.*

For example:

$$\dfrac{\dfrac{u{:}A, \Gamma, \Delta, x\,R\,y \vdash \Gamma', u{:}B, y{:}C}{\Gamma, \Delta, x\,R\,y \vdash \Gamma', u{:}A \to B, y{:}C} \to R}{\Gamma, \Delta \vdash \Gamma', u{:}A \to B, x{:}\Box C} \Box R \quad \text{permutes to} \quad \dfrac{\dfrac{u{:}A, \Gamma, \Delta, x\,R\,y \vdash \Gamma', u{:}B, y{:}C}{u{:}A, \Gamma, \Delta \vdash \Gamma', u{:}B, x{:}\Box C} \Box R}{\Gamma, \Delta \vdash \Gamma', u{:}A \to B, x{:}\Box C} \to R$$

The reason that $\Box L$ is, in general, not permutable with respect to $\Box R$ is that $\Box L$ may have the same active rwff $x\,R\,y$ as $\Box R$; examples of this situation are given below, e.g. in the proof-fragment (1).

Before showing that we can eliminate *ClL* and *ClR* in K, we observe that:

Lemma 3. *The rule CrL is eliminable in* K *and* T*.*

This follows because contracted rwffs can be introduced in the antecedent of a sequent only by applications of the rule *WrL*; the principal rwff of *refl* is introduced in the succedent of the sequent. Therefore, we just need to delete both the *CrL* and the corresponding *WrL*. For example, we transform

$$\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\Pi_1\\ \Delta_1 \vdash u\,R\,v\end{array}}{\Delta_1, x\,R\,y \vdash u\,R\,v}\,WrL\\ \Pi_2\\ \Delta_2, x\,R\,y, x\,R\,y \vdash u\,R\,v\end{array}}{\Delta_2, x\,R\,y \vdash u\,R\,v}\,CrL \qquad \text{to} \qquad \begin{array}{c}\Pi_1\\ \Delta_1 \vdash u\,R\,v\\ \Pi_2^{\dagger}\\ \Delta_2, x\,R\,y \vdash u\,R\,v\end{array}$$

where, here and in the following, we use '$\dagger$' to denote that in the derivation $\Pi_i^{\dagger}$ we apply the same sequence of rules applied in the derivation Π_i; in other words, Π_i and $\Pi_i^{\dagger}$ differ only in their parametric formulas.

We define the *grade* of an lwff $x{:}A$ to be the number of connectives in A. We define the *rank* of a contraction of $x{:}A$ to be the largest number of steps immediately preceding the conclusion of the contraction and containing at least one of the two contracted instances of $x{:}A$. Since, by the permutability of the rules, we can always transform a proof so that the contraction of $x{:}A$ immediately follows the step introducing the second instance of $x{:}A$, the rank measures how many steps stand between the introduction of the first and that of the second instance of $x{:}A$. Thus, the minimum possible rank is 2.

3.1 Contraction elimination in K

Theorem 4. *The rules ClL and ClR are eliminable in* K*, i.e., every theorem provable in* K *has a proof in which there are no applications of ClL and ClR.*

Proof. (Sketch) We adapt and extend the proof for classical propositional logic given by Zeman [16], and, given a proof Π of $\vdash d{:}D$ in K, proceed by three nested inductions. The first induction is on the number of contractions in Π. Suppose that Π contains $i+1$ contractions, and pick a 'highest' contraction in Π, i.e. consider a subproof of Π that ends with a contraction of $x{:}A$ and such that the proof above the contraction is contraction-free. We show how to eliminate this contraction to obtain a proof Π' of $\vdash d{:}D$ that contains i contractions; we proceed first by induction on the grade of $x{:}A$ and then by induction on the rank of the contraction. The base case, $grade(x{:}A) = 0$ is straightforward; for example, if one instance of $x{:}A$ is introduced by weakening, then we conclude by deleting this weakening and the contraction. There is one step for each rule introducing $x{:}A$, and we consider an illustrative case; the other cases follow similarly. Suppose that A is $\Box B$, both instances of $x{:}\Box B$ are introduced by applications of $\Box L$, and the contraction is an application of *ClL* with rank $j+1$. Then the only interesting subcase is when the rwff $x\,R\,z$, active in the uppermost application of $\Box L$, is active also in an application of $\Box R$ before the lowest application of $\Box L$, i.e.

$$
\begin{array}{c}
\dfrac{\dfrac{\begin{array}{c}\dfrac{}{x\,R\,y \vdash x\,R\,y}\,AXr \\ \vdots\; WrL \\ \Delta, x\,R\,y \vdash x\,R\,y\end{array} \qquad \begin{array}{c} \dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\dfrac{}{x\,R\,z \vdash x\,R\,z}\,AXr \\ \vdots\; WrL \\ \Delta_1, x\,R\,z \vdash x\,R\,z\end{array} \qquad \begin{array}{c}\Pi_1 \\ z{:}B, \Gamma_1, \Delta_1, x\,R\,z \vdash \Gamma_1'\end{array}}{x{:}\Box B, \Gamma_1, \Delta_1, x\,R\,z \vdash \Gamma_1'}\,\Box L \\ \Pi_2 \\ x{:}\Box B, \Gamma_2, \Delta_2, x\,R\,z \vdash z{:}C, \Gamma_2'\end{array}}{x{:}\Box B, \Gamma_2, \Delta_2 \vdash x{:}\Box C, \Gamma_2'}\,\Box R \\ \Pi_3 \\ y{:}B, x{:}\Box B, \Gamma, \Delta, x\,R\,y \vdash \Gamma'\end{array}}{x{:}\Box B, x{:}\Box B, \Gamma, \Delta, x\,R\,y \vdash \Gamma'}\,\Box L}{x{:}\Box B, \Gamma, \Delta, x\,R\,y \vdash \Gamma'}\,ClL \\
\Pi_0 \\
\vdash d{:}D
\end{array}
\tag{1}
$$

(Vertical dots labelled with *WrL* denote a sequence of applications of *WrL*.)

As explained for Lemma 2, we cannot, in general, reduce the rank of *ClL* by permuting the uppermost $\Box L$ with respect to the rule following it, since, if Π_2 is empty, the uppermost $\Box L$ is not permutable with respect to the $\Box R$ with active rwff $x\,R\,z$. We can however permute this $\Box R$ with respect to the lowest $\Box L$. To show this, we reason as follows. Since we are proving $\vdash d{:}D$, Π_0 must contain an application of $\Box R$ with active rwff $x\,R\,y$, and for this to be possible y must be an arbitrary world accessible from x. In particular, $y \neq x$. Thus, since $x\,R\,y$ and since there are no relational rules, $x{:}\Box C$ cannot follow from $y{:}B$, i.e. $x{:}\Box C$ and $y{:}B$ are independent. Then $x{:}\Box C$ must follow from some formula in Γ or Γ', and Π_3 can be divided into two separate subproofs, Π_4 and Π_5. Π_4 introduces $y{:}B$

and $x\,R\,y$, and $x{:}\Box C$ is active in Π_5. (If $y{:}B$ and $x\,R\,y$ are contained in Γ_2 and Δ_2, then Π_4 is empty and $\Pi_5 = \Pi_3$.) Given this separation, we can transform (1) to:

$$
\begin{array}{c}
\dfrac{
\begin{array}{c}
\dfrac{}{x\,R\,y \vdash x\,R\,y}\,AXr \\
\vdots\; WrL \\
\Delta_3, x\,R\,y, x\,R\,z \vdash x\,R\,y
\end{array}
\qquad
\begin{array}{c}
\dfrac{
\begin{array}{c}
\dfrac{}{x\,R\,z \vdash x\,R\,z}\,AXr \\
\vdots\; WrL \\
\Delta_1, x\,R\,z \vdash x\,R\,z
\end{array}
\qquad
\begin{array}{c}
\Pi_1 \\
z{:}B, \Gamma_1, \Delta_1, x\,R\,z \vdash \Gamma_1'
\end{array}
}{x{:}\Box B, \Gamma_1, \Delta_1, x\,R\,z \vdash \Gamma_1'}\,\Box L \\
\Pi_2 \\
x{:}\Box B, \Gamma_2, \Delta_2, x\,R\,z \vdash z{:}C, \Gamma_2' \\
\Pi_4^{\dagger} \\
y{:}B, x{:}\Box B, \Gamma_3, \Delta_3, x\,R\,y, x\,R\,z \vdash z{:}C, \Gamma_3'
\end{array}
}{
\dfrac{x{:}\Box B, x{:}\Box B, \Gamma_3, \Delta_3, x\,R\,y, x\,R\,z \vdash z{:}C, \Gamma_3'}{x{:}\Box B, x{:}\Box B, \Gamma_3, \Delta_3, x\,R\,y \vdash \Gamma_3'}\,\Box R
}\,\Box L \\
\Pi_5^{\dagger} \\
\dfrac{x{:}\Box B, x{:}\Box B, \Gamma, \Delta, x\,R\,y \vdash \Gamma'}{x{:}\Box B, \Gamma, \Delta, x\,R\,y \vdash \Gamma'}\,ClL \\
\Pi_0 \\
\vdash d{:}D
\end{array}
\qquad (2)
$$

(During the transformation it might be necessary to rename some labels to avoid clashes.) The rank of *ClL* is now less than $j+1$ and we can then conclude by applying the induction hypothesis. Reasoning similarly, we can eliminate all applications of *ClL* and *ClR*, and thus conclude the proof of the theorem.

Theorem 4 provides the basis for showing that K is decidable (see §4). Furthermore, the proof of Theorem 4 is extensible: when we add relational rules to K, we only need to consider the new cases that are generated by these rules. In particular, we must only investigate the eliminability of *ClL* when applied with principal formula of the form $x{:}\Box B$; by Lemma 3 and Theorem 4 it immediately follows that in T we can eliminate *ClR*, as well as all applications of *ClL* with principal formula different from $x{:}\Box B$. This generalization holds also for other logics extending K, as shown in [14]. However, it turns out that, even for a simple logic like T, applications of *ClL* with principal formula $x{:}\Box B$ are not eliminable; for example, the T-theorem $x{:}\neg\Box\neg(A \to \Box A)$ cannot be proved in our system without one application of *ClL* with principal formula $x{:}\Box\neg(A \to \Box A)$.

3.2 Bounded contraction in T

Although applications of *ClL* with principal formula $x{:}\Box B$ are needed in T, if we can bound their use then we need not give up decidability. To this end, we show that when proving a theorem in T, we need not contract each lwff $x{:}\Box B$ more than once in every branch. This amounts to restricting *ClL* with two side conditions: that the contracted lwff has the form $x{:}\Box B$, and that $x{:}\Box B$ can be contracted only once in a branch. We enforce the second condition by marking every $x{:}\Box B$ with a bit, a 1 or a 0, depending on whether a contraction has already been applied or not. We call this index the *contraction index* of the lwff, and we introduce the convention that when, in a forwards proof, we introduce a new instance of $x{:}\Box B$ in the antecedent of a sequent, we set its contraction index to 0; symmetrically, when in a backwards proof we first obtain $x{:}\Box B$ in the antecedent of a sequent, we set its contraction index to 1. Thus we restrict *ClL* to the rule

$$\frac{x{:}(\Box B)^0, x{:}(\Box B)^0, \Gamma, \Delta \vdash \Gamma'}{x{:}(\Box B)^1, \Gamma, \Delta \vdash \Gamma'}\ \mathit{ClL}_T,$$

which explicitly requires that both contracted lwffs have contraction index 0. The following theorem shows that these restrictions preserve completeness.

Theorem 5. *Every theorem provable in* T *has a proof in which there are no contractions, except for applications of ClL with principal formula of the form* $x{:}\Box B$*. However, ClL need not be applied more than once with the same principal formula* $x{:}\Box B$ *in every branch, and we can restrict ClL to be* ClL_T*.*

Proof. (Sketch) We extend Theorem 4 by considering the additional cases that arise in T when *ClL* is applied with principal formula $x{:}\Box B$. In particular, to show that *ClL* can be restricted to ClL_T, we show that if *ClL* is applied with principal formula $x{:}\Box B$ more than once in a branch $\mathcal{B}$ of a proof of $\vdash d{:}D$, then $\vdash d{:}D$ has a proof in which there is at most one application of *ClL* with principal formula $x{:}\Box B$ in $\mathcal{B}$. By the permutability of the rules, we can assume that if *ClL* is applied n times with principal formula $x{:}\Box B$ in $\mathcal{B}$, then these n contractions are performed as an uninterrupted sequence of steps immediately following the rule that introduces the n-th instance of $x{:}\Box B$. Then for each branch $\mathcal{B}$ we proceed as follows. If lwffs of different grade are contracted in $\mathcal{B}$, then we pick a 'lowest' sequence of n applications of *ClL* with contracted lwff of greatest grade. If $n = 1$, we move on to the next sequence of contractions. If $n > 1$, we consider the first two applications in the sequence, and we either eliminate the uppermost one, or we transform it into an application of *ClL* with principal formula of smaller grade. By iterating this transformation, we obtain the desired proof.

As an illustrative case, let both instances of $x{:}\Box B$ be introduced by an application of $\Box L$ with active rwff $x\,R\,x$, and consider the following branch where Π_1 and Π_2 do not contain applications of *ClL* with principal formula $x{:}\Box B$ or an lwff of grade greater than the grade of $x{:}\Box B$.

$$\dfrac{\dfrac{}{\Delta \vdash x\,R\,x}\,\mathit{refl} \qquad \begin{matrix} \dfrac{\dfrac{}{\Delta_1 \vdash x\,R\,x}\,\mathit{refl} \qquad \begin{matrix}\Pi_1 \\ x{:}B, x{:}\Box B, \Gamma_1, \Delta_1 \vdash \Gamma_1'\end{matrix}}{x{:}\Box B, x{:}\Box B, \Gamma_1, \Delta_1 \vdash \Gamma_1'}\,\Box L \\ \Pi_2 \\ x{:}B, x{:}\Box B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma' \end{matrix}}{\dfrac{x{:}\Box B, x{:}\Box B, x{:}\Box B, \Gamma, \Delta, \vdash \Gamma'}{\dfrac{x{:}\Box B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}{\begin{matrix} x{:}\Box B, \Gamma, \Delta \vdash \Gamma' \\ \Pi_0 \\ \vdash d{:}D \end{matrix}}\,\mathit{ClL}}\,\mathit{ClL}}\,\Box L \tag{3}$$

Since applications of $\Box L$ with active rwff introduced by *refl* are permutable with respect to every rule (even with respect to $\Box R$), we can transform (3) to:

$$
\dfrac{\dfrac{}{\Delta \vdash x\,R\,x}\,\mathit{refl} \qquad \dfrac{\dfrac{\dfrac{}{\Delta \vdash x\,R\,x}\,\mathit{refl} \qquad \begin{array}{c}\Pi_1\\ x{:}B, x{:}\Box B, \Gamma_1, \Delta_1 \vdash \Gamma_1'\\ \Pi_2^{\dagger}\\ x{:}B, x{:}B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'\end{array}}{x{:}B, x{:}\Box B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}\,\Box L}{x{:}B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}\,\mathit{ClL}}{\begin{array}{c}\dfrac{x{:}\Box B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}{x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}\,\mathit{ClL}\\ \Pi_0\\ \vdash d{:}D\end{array}}\,\Box L \tag{4}
$$

Then, we transform (4) by replacing the uppermost applications of $\Box L$ and *ClL* with principal formula $x{:}\Box B$ with an application of *ClL* with principal formula $x{:}B$, which has smaller grade, i.e.

$$
\dfrac{\dfrac{}{\Delta \vdash x\,R\,x}\,\mathit{refl} \qquad \dfrac{\begin{array}{c}\Pi_1\\ x{:}B, x{:}\Box B, \Gamma_1, \Delta_1 \vdash \Gamma_1'\\ \Pi_2^{\dagger}\\ x{:}B, x{:}B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'\end{array}}{x{:}B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}\,\mathit{ClL}}{\begin{array}{c}\dfrac{x{:}\Box B, x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}{x{:}\Box B, \Gamma, \Delta \vdash \Gamma'}\,\mathit{ClL}\\ \Pi_0\\ \vdash d{:}D\end{array}}\,\Box L
$$

4 Complexity of proof search

In this section we show the decidability of our sequent systems by combining bounds on contraction with bounds on the number of worlds and relational formulas that can be generated in proofs. In particular, we show that contraction elimination for K and bounded contraction elimination for T give rise to a proof procedure for these logics that uses $O(n \log n)$ space. Hence, these results, combined with the soundness and completeness of our systems with respect to the standard Kripke semantics for the modal logics K and T, tell us that the provability (validity) problems for these logics are decidable in Polynomial Space.

For clarity, we first consider labelled propositional logic, and then extensions to K and T.

4.1 Propositional logic

Labelled propositional logic, PL, consists of the axioms and rules AXl, $\bot L$, $\rightarrow L$, $\rightarrow R$, *WlL* and *WlR*, operating over sequents that contain only lwffs (i.e., Δ is always empty). The rules can be applied backwards to build a proof 'top-down', starting with the end-sequent and working towards the axioms (leaves) of the proof. To show that provability is in Polynomial Space, we employ the following definitions and facts.

Let the degree of an lwff $x{:}A$ simply be the size of A, $|A|$ (the number of symbols in its string representation), and the degree of a sequent the sum of the degrees of its lwffs. We say that $y{:}B$ is a subformula of $x{:}A$ if B is a subformula of A according to the standard definition in [12].

Fact 6. *In each rule of* PL*, each premise has smaller degree then the conclusion.*

Fact 7. *The subformula property holds:* PL *proofs of a sequent S generate only sequents that contain subformulas of S.*

Fact 6 tells us that every proof of a sequent S is bounded in length by the degree of S, which is in turn bounded by its size $n = |S|$. Fact 7 tells us that we can represent any generated sequent in $O(n^2)$ space, since there are at most $O(n)$ subformulas of size $O(n)$. We can reduce this to $O(n \, log \, n)$ space, since we can represent a subformula by an index into the end-sequent S, which requires only $log \, n$ bits.[2]

To test provability in Polynomial Space, we must first overcome problems related to two kinds of branching in the search space for proofs.

Conjunctive branching: applying rules with multiple premises builds a branching tree, where all branches must be proven.

Disjunctive branching: more than one rule may be applicable and a given rule may be applicable in different ways.

Conjunctive branching, caused by rules like $\to L$, leads to proofs that are exponential in size. Disjunctive branching arises when more than one rule may be applied to a sequent or when a single rule can be applied in different ways (e.g., a weakening).[3] This is reflected by a branching point in the search space for proofs rather than in proofs themselves.

To bound space requirements, we adapt and extend standard techniques [7,8]. In particular, rather than storing entire proofs, we store a sequent and a stack that maintains information sufficient to reconstruct branching points. Each stack entry is a triple: the name of the rule applied, the principal formula of the sequent, and an index. The index records sufficient information such that on return to the branching point another branch (if one remains) can be generated. For example, for $\to L$, the index is a bit indicating the first or second premise; for weakening, the index is a pointer indicating which premise is weakened.

A proof begins with the end-sequent S and the empty stack. Each rule application (we assume rules are ordered and we apply them in order) generates

[2] Formulae are labelled but since there are no modality rules, $\Box L$ and $\Box R$, the labels play no essential role and do not change during proofs.

[3] If we are concerned with average time complexity, as opposed to space complexity, we can exploit the fact that all PL rules, other than weakening, are invertible and permute with each other. Thus we can apply rules in some fixed order (without backtracking) and apply weakening only before axioms.

a new sequent and appropriately extends the stack. If the generated sequent is an axiom and the stack contains no conjunctive branching points that still need to be explored, then S is provable. Otherwise we pop entries off the stack until we find a conjunctive branching point that must be further explored and then generate the next branch (first incrementing the index on the stack to record this). Alternatively, if we arrive at a sequent that is not an axiom and no rule applies, then we pop stack entries and continue at the first available disjunctive branching point with the choices that remain (e.g., apply a different weakening, determined by the index, or apply the next available rule). If no such branching point remains, then S is not provable.

This procedure terminates since the stack depth is $O(n)$ and the branching is bounded (by n, the number of rules, and the maximum number of premises). Furthermore, since each entry requires $O(log\, n)$ space (we can store the principal formula as an index into the end-sequent S), the algorithm requires $O(n \log n)$ space. Since a formula A of propositional logic is provable iff the sequent $\vdash x{:}A$ is provable in PL, we have the following lemma:

Lemma 8. *Provability for propositional logic is decidable in $O(n \log n)$ space.*

4.2 Extension to K

The sequent system K extends PL with rules for $\Box$, as well as AXr and the weakening rule for rwffs, WrL. This proof system also admits an $O(n \log n)$ space provability procedure, but the details are a bit different.

Fact 6 no longer applies since WrL, although it eliminates an rwff, does not reduce the number of connectives. So we define instead the degree of an lwff $x{:}A$ to be twice the size of A, $2 \times |A|$, and the degree of a sequent S to be the sum of the degrees of the lwffs in S plus the number of rwffs in S. Now we can extend Fact 6 for the rules of K, and since the degree function is linear, any proof will have depth $O(n)$, where $n = |S|$.

Fact 7 holds for K, although subformulas may be labelled differently. Unlike for PL we now must take labels seriously, since applications of $\Box R$ introduce new labels (and rwffs) and applications of $\Box L$ label subformulas with different (currently in existence) labels. Note that we can only generate a new label and a new rwff for each application of $\Box R$. This is bounded above in any branch by the number of $\Box$ operators appearing in the end-sequent S, i.e., $O(n)$. Hence the number of lwffs and rwffs in the generated sequent is also $O(n)$, since it can contain $O(n)$ lwffs and $O(n)$ rwffs. Moreover, since there are only $O(n)$ labels, we can represent a label using $O(log\, n)$ bits. Thus, each lwff and rwff can be represented using $O(log\, n)$ bits and any generated sequent can be represented using $O(n\, log\, n)$ space.

The proof procedure for K is essentially the same as for PL. The only interesting difference is that the rule for $\Box L$ introduces disjunctive branching: if the goal is $x{:}\Box A$, any label y currently in existence is a possible candidate for producing $y{:}A$ in the generated sequent. We use the index to record which label we choose so that on backtracking we can generate the next possible candidate.

Note that we can determine what the possible candidates are by looking into the stack and examining previous applications of $\Box R$ and WrL. Note also that $\Box L$ is not invertible, and its application introduces a choice point and other rules can be tried on backtracking. From the soundness and completeness of K and the fact that the entire search space is navigated, if need be, on backtracking, this proof procedure is complete. Termination is analogous to PL and the space requirement is the same. Thus we have:

Theorem 9. *Provability for the modal logic* K *is decidable in* $O(n \log n)$ *space.*

The essence of this result is that contraction elimination, the subformula property, and a linear number of rwffs give us linear depth proofs as for propositional logic. Moreover, given our bound on the number of worlds, the space complexity to represent sequents remains $O(n \log n)$. Hence we get an identical overall upperbound.

Note that K is possibly harder then PL given that provability for the former is PSPACE complete whereas the latter is co-NP complete. One intuition for this is that the $\Box L$ rule introduces a necessary disjunctive branching point in the search space; all such branching points for PL are eliminable by analysis of permutabilities, as indicated above.

4.3 Extension to T

The proof system for T differs from K in two respects:

1. Rwffs used in applications of $\Box L$ arise not only from applications of $\Box R$ but also from applications of *refl.*
2. We need possibly a single instance of contraction on the left for an lwff $x{:}\Box A$ in every branch (Theorem 5).

Since the number of worlds is still bounded to be linear in n, the size of the end-sequent S, the first difference means that we can have up to n additional rwffs in generated sequents, namely $x\ R\ x$ for each of the n possible labels x. This does not change the $O(n\, log\, n)$ space bound required to store sequents.

As described in §3 we can introduce controlled contraction by associating a bit with each lwff $x{:}\Box A$ indicating if it has been contracted or not (this also does not change the above space complexity for storing sequents), and thus restrict *ClL* to only contract lwffs $x{:}\Box A$ that have not yet been contracted. To accommodate possibly longer proofs, we modify the measure for K such that the degree of an lwff $x{:}A$ is four times the size of A plus 1, $(4 \times |A|) + 1$, when it has not been contracted and twice the size of A, $2 \times |A|$, when it has. Then every rule, including ClL_T, reduces this measure; this means that the length of branches of proofs is still $O(n)$. Thus it follows that:

Theorem 10. *Provability for the modal logic* T *is decidable in* $O(n \log n)$ *space.*

5 Related work

Modal logics are typically shown to be decidable semantically, by showing that they possess the finite model property. However, for many logics, including K and T, there are classes of satisfiable formulas in which every satisfying structure contains exponentially many worlds [6]. Thus it is necessary to analyze the complexity of particular proof procedures to get more refined complexity results.

Ladner [11], building upon the decision procedures of Kripke [10], showed that K and T have respective space complexity of n^2 and n^3. Improved bounds (identical to ours) have been recently given by Hudelmaier [8]. He starts with standard sequent calculi (related to those found in [3,16]) in which cut is admissible and contraction is built into the rules for the modalities. He then uses proof transformations to obtain equivalent systems with new modality rules, which are measure decreasing. Although we end up with the same complexity results, our systems and, in particular, the analysis behind them, are completely different from his; for example, unlike Hudelmaier, we do not need to introduce new modalities.

Labelling has often been used as a way to introduce additional information that can be exploited in the presentation of modal logics and in the analysis of their decidability. For instance, Fitting [3] generalizes the procedures described in [9] to give systematic decision procedures for a wide variety of prefixed modal tableaux systems, including K and T. Although our labelled sequent systems share characteristics with Fitting's systems (the main difference is that in Fitting's systems the different properties of the accessibility relation are expressed procedurally as side conditions on the application of the same set of rules, while we use relational rules to extend the fixed base logic), the analysis of decidability relies on different mechanisms. We show that contraction can be eliminated in K and bounded to a single application in T. Fitting avoids explicit repetitions (contractions) of formulas of the form $x{:}\Box A$ in the antecedent of a sequent (i.e., in his notation, formulas of the form $x\ \top \Box A$ in a tableau) by having a $\Box L$ rule that does not delete $x{:}\Box A$ but prevents its further use until a new y such that $x\,R\,y$ is introduced in the tableau; termination of the decision procedure is then argued by exploiting König's Lemma. Aside from this difference, this kind of procedure leads to implementations based on loop-checking, as opposed to measure-decreasing rule applications (as in Hudelmaier's and our work). Finally, this analysis, although it establishes decidability, does not result in good complexity bounds.

Other work on proof-theoretic decision procedures for modal logic, related to that of Fitting, is that of Wallen [15], who uses matrix-characterizations to investigate a range of standard modal logics, where duplication is achieved by increasing an index associated to the formulas. However, while he stresses the importance of 'computationally sensitive' characterizations of logics, he does not explicitly address the complexity bounds associated with the systems he investigates. Also, the central point of his work concerns identifying pairs of complementary terms that can be used as the basis of a search procedure, rather than analyzing the structural rules.

6 Conclusion and further work

We have presented a new proof-theoretic approach to bounding the complexity of the decision problem for propositional modal logics. As examples, we have given $O(n \log n)$ space decision procedures for the modal logics K and T, by combining restrictions on the structural rules of labelled sequent systems with an analysis of the accessibility relation of the corresponding Kripke structures. This work is a first step towards a general framework for both applying proof theory to the analysis of complexity of families of modal, and other similarly formalized non-classical, logics, see [1,14], and for implementing decision procedures for these logics. Current work includes extending this approach to other modal logics (extensions to K4 and S4 are given in [14]) and to substructural, e.g. relevance, logics, as well as exploring implementation issues.

References

1. D. Basin, S. Matthews, and L. Viganò. Implementing modal and relevance logics in a logical framework. In L. Carlucci Aiello, J. Doyle, and S. Shapiro, editors, *Proceedings of KR'96*, pages 386–397. Morgan Kaufmann, San Francisco, 1996.
2. D. Basin, S. Matthews, and L. Viganò. Labelled propositional modal logics: theory and practice. *Journal of Logic and Computation*, 1997. To appear.
3. M. Fitting. *Proof methods for modal and intuitionistic logics.* Kluwer, Dordrecht, 1983.
4. G. Gentzen. Investigations into logical deduction. In M. Szabo, editor, *The collected papers of Gerhard Gentzen*, pages 68–131. North Holland, Amsterdam, 1969.
5. J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and types.* Cambridge University Press, Cambridge, 1989.
6. J. Y. Halpern and Y. O. Moses. A guide to the completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54(3):319–379, 1992.
7. J. Hudelmaier. A $O(n\ log\ n)$-space decision procedure for intuitionistic propositional logic. *Journal of Logic and Computation*, 3(1):63–75, 1993.
8. J. Hudelmaier. Improved decision procedures for the modal logics K, T and S4. In H. Kleine Büning, editor, *Proceedings of CSL'95*, LNCS 1092, pages 320–334. Springer, Berlin, 1996.
9. G. Hughes and M. Cresswell. *An introduction to modal logic.* Routledge, London, 1972.
10. S. Kripke. Semantical analysis of modal logic I. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963.
11. R. E. Ladner. The computational complexity of provability in systems of modal propositional logics. *SIAM Journal of Computing*, 6(3):46–65, 1977.
12. D. Prawitz. *Natural deduction.* Almqvist and Wiksell, Stockholm, 1965.
13. A. S. Troelstra and H. Schwichtenberg. *Basic proof theory.* Cambridge University Press, Cambridge, 1996.
14. L. Viganò. *A framework for non-classical logics.* PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1997. Forthcoming.
15. L. Wallen. *Automated deduction in non-classical logics.* MIT Press, Cambridge, Massachusetts, 1990.
16. J. J. Zeman. *Modal logic: the Lewis-modal systems.* Oxford University Press, Oxford, 1973.