On the modal logic K plus theories

Alain Heuerding*, Stefan Schwendimann*

Institut für Informatik und angewandte Mathematik,
Universität Bern, Switzerland

Abstract. $\mathsf{K}+T$ is the propositional modal logic K with the elements of the finite set T as additional axioms.
We develop a sequent calculus that is suited for proof search in $\mathsf{K}+T$ and discuss methods to improve the efficiency. An implementation of the resulting decision procedure is part of the Logics Workbench LWB.
Then we show that – in contrast to K, KT, $\mathsf{S4}$ – there are theories T and formulas A where a counter-model must have a superpolynomial diameter in the size of T plus A.
In the last part we construct an embedding of $\mathsf{S4}$ in $\mathsf{K}+T$.

1 Introduction

A Hilbert-style calculus for (propositional) $\mathsf{K}+T$ is obtained from the usual Hilbert-style calculus for the modal logic K by adding the formulas of T as additional axioms. There is also a natural characterization of $\mathsf{K}+T$ from the point of view of Kripke structures: We restrict ourselves to Kripke structures whose worlds satisfy T.
One application of $\mathsf{K}+T$ is the proof of the equivalence of propositional normal modal logics ([5]). Another application is the well-known wise men puzzle, which can be solved with the multimodal variant of $\mathsf{K}+T$, whereas the multimodal variant of K alone is not sufficient. However, in many systems that offer decision procedures for modal logics, e.g. HLM [9] or Tableaux [1], as well as in discussions of methods for proof search in modal logics, e.g. [14], modal logics plus theories are not considered.
In the first part we develop a sequent calculus that ensures the termination of proof search. Making use of the fact that most rules are invertible and by adding rules for $\leftrightarrow$, the search tree can be considerably reduced. A further non-elementary improvement is obtained by eliminating useless branchings.
The length of the branches of the search tree plays an important role in proof search (see also the multiplicity problem in [14]) and in complexity questions ([8]), but also in the construction of embeddings ([3]). In the case of proof search for the formula A in K, KT or $\mathsf{S4}$, it is possible to give a polynomial upper bound in the size of A. Such a polynomial bound (in the size of A plus T) does not exist for $\mathsf{K}+T$. In our main theorem we prove that this is not a defect of our sequent

* Work supported by the Swiss National Science Foundation, SPP 5003-34279.

calculus, but that sometimes all counter-models must have a superpolynomial diameter in the size of A plus T.
In the last part we construct an embedding of $\mathsf{S4}$ in $\mathsf{K}+T$. The transitivity of the accessibility relation in the Kripke-structures that is present in $\mathsf{S4}$ but not in K is simulated by an appropriate theory T. The existence of such a natural embedding indicates that $\mathsf{K}+T$ is considerably more expressive than K.

2 Notation

Definition 1.
Var $:= \{p_0, p_1, p_2, \ldots\}$ is the set of the variables. The set Fml of the (modal) formulas is inductively defined: If $P \in$ Var, then $P \in$ Fml and $\neg P \in$ Fml; if $A, B \in$ Fml, then $(\Box A), (\Diamond A), (A \wedge B), (A \vee B) \in$ Fml.
If $A, B \in$ Fml, then $A \equiv B$ means that A and B are syntactically equal.
If $A, B \in$ Fml, then: $(\neg(\neg A)) :\equiv A$, $(\neg(\Box A)) :\equiv (\Diamond(\neg A))$, $(\neg(\Diamond A)) :\equiv (\Box(\neg A))$, $(\neg(A \wedge B)) :\equiv ((\neg A) \vee (\neg B))$, $(\neg(A \vee B)) :\equiv ((\neg A) \wedge (\neg B))$, and $(A \to B) :\equiv ((\neg A) \vee B)$, $(A \leftrightarrow B) :\equiv ((A \to B) \wedge (B \to A))$.
A theory is a finite set of formulas.

Usually we omit the outermost brackets. The unary connectives have the highest priority, followed by $\wedge$, $\vee$, $\to$, and $\leftrightarrow$. $\wedge$, $\vee$, and $\leftrightarrow$ are left associative.
Example: $p_2 \wedge p_0 \wedge p_1 \vee (p_2 \to p_3)$ stands for $(((p_2 \wedge p_0) \wedge p_1) \vee (p_2 \to p_3))$.

We use meta-variables as follows: P, Q, R for variables, A, B, C for formulas, Γ, Σ for (perhaps empty) multisets of formulas, T for theories, n for natural numbers (including 0).

Definition 2.
If Γ is the multiset $A_1, \ldots, A_n$, then $\Diamond\Gamma$ is the multiset $\Diamond A_1, \ldots, \Diamond A_n$.
$\Box^0 A :\equiv A$, $\Box^{n+1} A :\equiv \Box\,\Box^n A$.

Definition 3.
The length $|A|$ of a formula A is the number of variables and connectives in A.
$|T| := \sum_{A \in T} |A|$. (Note that theories are always finite.)
Example: $|p_0 \wedge (\neg p_1 \vee p_0)| = 6$.

Definition 4. $A\{B_1/P_1, \ldots, B_n/P_n\}$ is the formula obtained from A by simultaneously substituting P_1 by B_1, …, P_n by B_n.

Definition 5. $\mathsf{CPC} \vdash A$ means that $\Box$ and $\Diamond$ do not occur in the formula A and that A is provable in classical propositional logic.

Definition 6. $\langle x_0, \ldots, x_n \rangle$ is the $n+1$ tuple with the elements $x_0, \ldots, x_n$.

3 K: syntax and semantics

Definition 7. $\mathsf{K}_{\mathcal{H}}$ is the following Hilbert-style calculus:

$$A\{B_1/P_1,\dots,B_n/P_n\} \quad \text{if } \mathsf{CPC} \vdash A$$
$$\Box(A \to B) \to \Box A \to \Box B$$

$$\frac{A \quad A \to B}{B}\ (\text{mp}) \qquad\qquad \frac{A}{\Box A}\ (\Box)$$

Definition 8. The corresponding one-sided sequent calculus $\mathsf{K}_{\mathcal{S}}$ is defined as follows:

$$P, \neg P \qquad\qquad \frac{\Gamma}{A, \Gamma}\ (\text{weak})$$

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

$$\frac{A, \Gamma}{\Box A, \Diamond\Gamma}\ (\Box)$$

Note 9. We use multisets of formulas, so there is no contraction hidden in $\mathsf{K}_{\mathcal{S}}$.

Definition 10. A Kripke-structure $\mathcal{M}$ is a triple $\langle W_{\mathcal{M}}, \mathcal{R}_{\mathcal{M}}, I_{\mathcal{M}}\rangle$, where $W_{\mathcal{M}}$ is a non-empty set, $\mathcal{R}_{\mathcal{M}} \subset {W_{\mathcal{M}}}^2$, and $I_{\mathcal{M}} : W_{\mathcal{M}} \times \mathrm{Var} \to \{0,1\}$. We call the elements of $W_{\mathcal{M}}$ the worlds of $\mathcal{M}$.

Usually we omit the subscript ${}_{\mathcal{M}}$. We use $\mathcal{M}$ as a meta-variable for Kripke-structures.

Definition 11. Let $\mathcal{M}$ be a Kripke-structure. For all $w \in W$ the relation $w \models A$ is inductively defined:

$w \models P \ :\Leftrightarrow\ I(w,P) = 1, \qquad w \models \neg P \ :\Leftrightarrow\ I(w,P) = 0$
$w \models \Box A \ :\Leftrightarrow\ \forall w' \in W : (w\mathcal{R}w' \Rightarrow w' \models A)$
$w \models \Diamond A \ :\Leftrightarrow\ \exists w' \in W : (w\mathcal{R}w' \text{ and } w' \models A)$
$w \models A \wedge B \ :\Leftrightarrow\ w \models A \text{ and } w \models B, \qquad w \models A \vee B \ :\Leftrightarrow\ w \models A \text{ or } w \models B$

$\mathcal{M} \models A \ :\Leftrightarrow\ \forall w \in W : w \models A$

$\models A$ iff for all Kripke-structures $\mathcal{M}$ we have $\mathcal{M} \models A$.

Theorem 12.

$$K_{\mathcal{H}} \vdash A \quad\Leftrightarrow\quad \models A \quad\Leftrightarrow\quad K_{\mathcal{S}} \vdash A$$

Proof. Left equivalence: see e.g. [12]; right equivalence: see e.g. [2] or [4].

Definition 13. $\langle w_0,\dots,w_n\rangle \in W^{n+1}$ is a path in $\mathcal{M}$ iff

$$\forall i \in \{0,\dots,n-1\} : w_i\mathcal{R}w_{i+1} \text{ and } \forall i,j \in \{0,\dots,n\} : (i \neq j \Rightarrow w_i \neq w_j)$$

Definition 14.
$|w,w'| := \min\{n+1 | \langle w_0,\dots,w_n\rangle \text{ path in } \mathcal{M}, w_0 = w, w_n = w'\}$ $(\forall w,w' \in W)$.
$\mathrm{diam}(\mathcal{M}) := \max\{|w,w'| \mid w,w' \in W\}$. We call $\mathrm{diam}(\mathcal{M})$ the diameter of $\mathcal{M}$.

4 $\mathsf{K}+T$: syntax and semantics

Definition 15. The Hilbert-style calculus $(\mathsf{K}+T)_{\mathcal{H}}$ is the calculus $\mathsf{K}_{\mathcal{H}}$ plus for all $B \in T$ the axiom B.

Definition 16. The one-sided sequent calculus $(\mathsf{K}+T)_{\mathcal{S}}$ is the calculus $\mathsf{K}_{\mathcal{S}}$ plus for all $B \in T$ the rule

$$\frac{\neg B, \Gamma}{\Gamma}\ (\mathrm{th})$$

Example 1. $T := \{p_1, \Box(p_1 \to p_0)\}$. Then $\Box p_0$ is provable in $(\mathsf{K}+T)_{\mathcal{H}}$ and in $(\mathsf{K}+T)_{\mathcal{S}}$.

$$\dfrac{\dfrac{p_1}{\Box p_1}\ (\Box) \qquad \dfrac{\Box(p_1 \to p_0) \quad \Box(p_1 \to p_0) \to \Box p_1 \to \Box p_0}{\Box p_1 \to \Box p_0}\ (\mathrm{mp})}{\Box p_0}\ (\mathrm{mp})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p_1, \neg p_1}{p_0, p_1, \neg p_1}\ (\mathrm{weak})}{p_0, p_1}\ (\mathrm{th}) \qquad p_0, \neg p_0}{p_0, p_1 \wedge \neg p_0}\ (\wedge)}{\Box p_0, \Diamond(p_1 \wedge \neg p_0)}\ (\Box)}{\Box p_0}\ (\mathrm{th})$$

Definition 17.
$T \models A \ :\Leftrightarrow\ \forall \mathcal{M} : (\mathcal{M} \models T \Rightarrow \mathcal{M} \models A)$.
$\mathcal{M} \not\models \langle T, A\rangle \ :\Leftrightarrow\ (\mathcal{M} \models T$ and $\mathcal{M} \not\models A)$.
If $\mathcal{M} \not\models \langle T, A\rangle$, then we call $\mathcal{M}$ a counter-model of $\langle T, A\rangle$.

Theorem 18.

$$(\mathsf{K}+T)_{\mathcal{H}} \vdash A \quad \Leftrightarrow \quad T \models A \quad \Leftrightarrow \quad (\mathsf{K}+T)_{\mathcal{S}} \vdash A$$

Proof. Left equivalence: see e.g. [12]; right equivalence: see e.g. [2].

In the following we write $\mathsf{K}+T \vdash A$ instead of $(\mathsf{K}+T)_{\mathcal{H}} \vdash A$.

Theorem 19. *If* $T = \{B_1, \ldots, B_n\}$, $C :\equiv B_1 \wedge \ldots \wedge B_n$, *then*

$$\mathsf{K}+T \vdash A \quad \Leftrightarrow \quad \exists k \in I\!N : \mathsf{K} \vdash \Box^0 C \wedge \Box^1 C \wedge \ldots \wedge \Box^k C \to A$$

Proof. See [3].

Remark. With $\Box^0 C \wedge \Box^1 C \wedge \ldots \wedge \Box^k C$ we express that the formulas in T must be satisfied in the actual world and in the following k worlds. The same mechanism is used in the (th) rule of $(\mathsf{K}+T)_{\mathcal{S}}$, however without the limit k.

Note 20. $\mathsf{K} \nvdash \Diamond(p_0 \vee \neg p_0)$, but $\mathsf{K} + \{\Diamond p_1\} \vdash \Diamond(p_0 \vee \neg p_0)$.
It is surprising that $\Diamond p_1$ can help to prove a formula with p_0 as its only variable. If we do backward proof search in $(\mathsf{K} + T)_{\mathcal{S}}$, then $\Diamond p_1$ enables the backward application of $(\Box)$. From the point of view of Kripke semantics, $\Diamond(p_0 \vee \neg p_0)$ does not hold for worlds without successor; the addition of $\Diamond p_1$ ensures the existence of successors.

5 Proof search in sequent calculi

Although we consider only finite theories, the backward proof search in $(\mathsf{K} + T)_{\mathcal{S}}$ does not terminate in general, since the (th) rule is always applicable.

Because $(\mathsf{K} + T)_{\mathcal{S}}$ enjoys the subformula property, and $(K + T)_{\mathcal{S}} \vdash A, \Gamma$ iff $(K + T)_{\mathcal{S}} \vdash A, A, \Gamma$, backward proof search can be restricted such that only a finite number of sequents occurs. Consequently each branch either loops or ends in an axiom.

The calculus $(\mathsf{K} + T)_{\mathcal{S},2}$ uses a variant of this restriction. A built-in loop check ensures the termination of the backward proof search. A sequent in $(\mathsf{K} + T)_{\mathcal{S},2}$ consists of a multiset and the history H. H is a set of pairs of a formula and a multiset. Such a pair represents a sequent on which the $(\Box)$ rule has already been applied.

Definition 21. $(\mathsf{K} + T)_{\mathcal{S},2}$

$T = \{B_1, \ldots, B_n\}$, Δ contains no duplicate elements

$$P, \neg P, \Gamma; H$$

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

$$\frac{A, \Delta, \neg B_1, \ldots, \neg B_n; H \cup \{\langle A; \Delta\rangle\}}{\Box A, \Diamond\Delta, \Sigma; H}\langle A; \Delta\rangle \notin H \qquad (\Box)$$

Note 22. The weakening rule is now integrated in $(\Box)$ and in the axioms.

Theorem 23. *If* $T = \{B_1, \ldots, B_n\}$, *then*

$$(\mathsf{K} + T)_{\mathcal{S},2} \vdash A, \neg B_1, \ldots, \neg B_n; \emptyset \quad \Leftrightarrow \quad (\mathsf{K} + T)_{\mathcal{S}} \vdash A$$

Proof. From the invertibility of the $(\vee)$ and $(\wedge)$ rules of $\mathsf{K} + T_{\mathcal{S}}$ we can conclude that it is enough to apply (th) backwards right after applying $(\Box)$ backwards in $(\mathsf{K} + T)_{\mathcal{S}}$. The equivalence follows with an induction on proof length.

Note 24. From the point of view of Kripke semantics, the combination of the rules $(\Box)$ and (th) of $\mathsf{K}_{\mathcal{S}}$ to one rule means: Add the theory only after moving to a new world.

If we do backward proof search in $(\mathsf{K}+T)_{\mathcal{S},2}$, we first apply the invertible rule $(\vee)$ as often as possible, and then the invertible rule $(\wedge)$. Afterwards we have to apply $(\Box)$ backwards in all possible ways until the provability is established or all these possibilities failed. Of course we always choose Σ as small as possible.

In this article we use $\leftrightarrow$ only as an abbreviation, what produces sometimes a superfluous blow up of the formula (consider e.g. the formulas $p_0 \leftrightarrow p_1 \leftrightarrow \ldots \leftrightarrow p_n \leftrightarrow p_0 \leftrightarrow p_1 \leftrightarrow \ldots \leftrightarrow p_n$ of [13]). Using a two-sided sequent calculus with special rules for $\leftrightarrow$ solves this problem.

A serious problem is the superfluous backward application of $(\wedge)$. Consider the following example of backward proof search in $(\mathsf{K}+\{P \vee Q\})_{\mathcal{S},2}$ (we omit the history in the sequents):

$$
\dfrac{
\dfrac{\dfrac{\dfrac{P,Q,R,\neg P \quad P,Q,R,\neg Q}{P,Q,R,\neg P \wedge \neg Q}(\wedge)}{P \vee Q \vee R, \neg P \wedge \neg Q}(\vee),(\vee)}{\Box(P \vee Q \vee R), \neg P}(\Box)
\qquad
\dfrac{\dfrac{\dfrac{P,Q,R,\neg P \quad P,Q,R,\neg Q}{P,Q,R,\neg P \wedge \neg Q}(\wedge)}{P \vee Q \vee R, \neg P \wedge \neg Q}(\vee),(\vee)}{\Box(P \vee Q \vee R), \neg Q}(\Box)
}{\Box(P \vee Q \vee R), \neg P \wedge \neg Q}(\wedge)
$$

The right subproof is almost equal to the left subproof, because the subformulas of the main formula $\neg P \wedge \neg Q$ of the first backward application of $(\wedge)$ disappear unused. However, we cannot do without the two remaining applications of $(\wedge)$.

Of course this problem also occurs in classical propositional logic (see e.g. [10]), but in the case of $(\mathsf{K}+T)_{\mathcal{S},2}$ the problem is more serious since the formulas of the theory are added again and again. The so-called use-checking proposed in [11] for intuitionistic propositional logic can be modified such that it fits $\mathsf{K}+T$.

Theorem 25. *If $\mathcal{P}$ is a proof of the sequent $A, \Gamma; H$ in $(K+T)_{\mathcal{S},2}$, and no subformula of A is the main formula of an axiom or of a $(\Box)$ application in $\mathcal{P}$, then $(K+T)_{\mathcal{S},2} \vdash A \wedge B, \Gamma; H$ for all $B \in Fml$.*

Proof. Induction on proof length of $\mathcal{P}$.

For the formula $\Box^n(p_0 \vee p_1 \vee p_2)$, use-checking leads to an exponential speed-up of backward proof search in $(\mathsf{K}+T)_{\mathcal{S},2}$.

6 Sometimes counter-models must have large diameter

An important property of a calculus is the length of the branches resp. loops that can occur. If backward proof search fails in $(\mathsf{K}+T)_{\mathcal{S},2}$ then a counter-model can be directly derived from the search tree. Each application of $(\Box)$ corresponds to a world in the counter-model or, if a loop occurs, to a connection with an already existing world.

In the case of the sequent calculi for K, KT, $\mathsf{S4}$ (cf. section 7), the diameter of the resulting counter-model is limited by a polynomial in $|A|$. These polynomial bounds immediately show that these decision problems are solvable in PSPACE (see [8] for details).

It is easy to obtain an exponential upper bound for $\mathrm{diam}(\mathcal{M})$. We know that $(\mathsf{K}+T)_{\mathcal{S},2} \vdash A, \Gamma$ iff $(\mathsf{K}+T)_{\mathcal{S},2} \vdash A, A, \Gamma$, and $(\mathsf{K}+T)_{\mathcal{S},2}$ satisfies the subformula property. Since the number of different subformulas in A and T is at most $|A| + |T|$, the following lemma holds:

Lemma 26. *If $\mathsf{K}+T \not\vdash A$, then there is a Kripke-structure $\mathcal{M}$ such that $\mathcal{M} \not\models \langle T, A\rangle$ and $\mathrm{diam}(\mathcal{M}) \leq 2^{|A|+|T|}$.*

In this section we show that there is no polynomial upper bound for $\mathrm{diam}(\mathcal{M})$ in the size of A plus T.

Definition 27. If $m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$ and $P, Q_1, \ldots, Q_m, R$ are different variables, then $\forall i \in \{1, \ldots, m\} : \forall j \in I\!N : A_{ij} :\equiv \Box^j Q_i \wedge \bigwedge_{k=1}^{j-1} \Box^k \neg Q_i$ and

$$T_{\langle b_1,\ldots,b_m\rangle} := \{\Diamond R, \neg Q_1 \vee A_{1,b_1}, \ldots, \neg Q_m \vee A_{m,b_m}, P \vee A_{1,b_1} \wedge \ldots \wedge A_{m,b_m}\}$$

Example 2. $m = 2$, $b_1 = 3$, $b_2 = 5$.
Then $\langle\{w_0, \ldots, w_{15}, \mathcal{R}, I\rangle$, where $w_0 \mathcal{R} w_1$, $\ldots$, $w_{14} \mathcal{R} w_{15}$, $w_{15} \mathcal{R} w_1$, and where I is given by the following table, is a typical counter-model of $\langle T_{\langle 3,5\rangle}, P\rangle$. (A '?' in the table means that the value does not matter.)

I	w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	w_{11}	w_{12}	w_{13}	w_{14}	w_{15}
P	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Q_1	?	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
Q_2	?	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
R	?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Because of the formula $\Diamond R$ there must always exist a successor world. In a counter-model of $\langle T_{\langle 3,5\rangle}, P\rangle$ there must be a world where P is false, called w_0 in this example. The formula $P \vee A_{1,3} \wedge A_{2,5}$ at the beginning and afterwards the formulas $\neg Q_1 \vee A_{1,3}$ resp. $\neg Q_2 \vee A_{2,5}$ effect that Q_1 is exactely true in every third world resp. that Q_2 is exactely true in every fifth world. This leads to a loop of $3 \cdot 5$ different worlds.

Lemma 28. *If $m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$, then $T_{\langle b_1,\ldots,b_m\rangle} \not\vdash P$.*

Proof. It is always possible to construct a counter-model of $\langle T_{\langle b_1,\ldots,b_m\rangle}, P\rangle$ analogous to the one in the example above.

Note 29. $T_{\langle b_1,\ldots,b_m\rangle} \cup \{\neg Q_1 \vee \ldots \vee \neg Q_m\} \vdash P$.

Definition 30. If $m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$, then $G(b_1, \ldots, b_m)$ stands for

$$\forall i, j \in \{1, \ldots, m\} : (i < j \rightarrow \gcd(b_i, b_j) = 1)$$

Lemma 31. *If* $m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$ *and* $G(b_1, \ldots, b_m)$, *then:*

$$\mathcal{M} \not\models \langle T_{\langle b_1,\ldots,b_m\rangle}, P\rangle \quad \Rightarrow \quad \mathrm{diam}(\mathcal{M}) \geq \prod_{i=1}^{m} b_i$$

Proof. Assume that $\mathcal{M} \models T_{\langle b_1,\ldots,b_m\rangle}$ $(*)$, $\mathcal{M} \not\models P$.

(1) $\mathcal{M} \models T_{\langle b_1,\ldots,b_m\rangle} \;\Rightarrow\; \forall w \in W : w \models \Diamond R \;\Rightarrow\; \forall w \in W : \exists w' \in W : w\mathcal{R}w'$.
(2) $\mathcal{M} \not\models P \;\Rightarrow\; \exists w_0 \in W : w_0 \models \neg P$
$\stackrel{(*)}{\Rightarrow}\; \exists w_0 \in W : w_0 \models \neg P \wedge (P \vee A_{1,b_1} \wedge \ldots \wedge A_{m,b_m})$
$\Rightarrow\; \exists w_0 \in W : w_0 \models A_{1,b_1} \wedge \ldots \wedge A_{m,b_m}$.
(3) Assume $w, w' \in W$ and $d_1 \in \{1, \ldots, b_1\}$, $\ldots$, $d_m \in \{1, \ldots, b_m\}$ such that $w\mathcal{R}w'$ and $w \models A_{1,d_1} \wedge \ldots \wedge A_{m,d_m}$.
Then we have for all $i \in \{1, \ldots, m\}$:
  – $d_i > 1$: $w \models A_{i,d_i} \;\Rightarrow\; w \models \Box^{d_i} Q_i \wedge \bigwedge_{k=1}^{d_i-1} \Box^k \neg Q_i$
  $\Rightarrow\; w' \models \Box^{d_i-1} Q_i \wedge \bigwedge_{k=1}^{d_i-2} \Box^k \neg Q_i \;\Rightarrow\; w' \models A_{i,d_i-1}$.
  – $d_i = 1$: $w \models A_{i,d_i} \;\Rightarrow\; w \models \Box Q_i \;\Rightarrow\; w' \models Q_i$
  $\stackrel{(*)}{\Rightarrow}\; w' \models Q_i \wedge (\neg Q_i \vee A_{i,b_i}) \;\Rightarrow w' \models A_{i,b_i}$.
(4) Assume $w \in W$, $i \in \{1, \ldots, m\}$ and $d_i, d'_i \in \{1, \ldots, b_i\}$, $d_i \leq d'_i$ such that $w \models A_{i,d_i}$ and $w \models A_{i,d'_i}$.
If $d_i < d'_i$, then $w \models \Box^{d_i} Q_i$ and $w \models \Box^{d_i} \neg Q_i$. With (1) follows $\exists w' \in W$: $(w' \models Q_i$ and $w' \models \neg Q_i)$. Contradiction.
Thus $d_i = d'_i$.

Conclusion:
We define $c := \prod_{i=1}^{m} b_i$. Because of (1), (2) there are $w_0, w_1, \ldots, w_{c-1} \in W$ such that $w_0\mathcal{R}w_1\mathcal{R}\ldots\mathcal{R}w_{c-1}$ and $w_0 \models A_{1,b_1} \wedge \ldots \wedge A_{m,b_m}$.
With (2),(3),(4) together with $G(b_1, \ldots, b_m)$ follows that $\langle w_0, \ldots, w_{c-1}\rangle$ is a path in $\mathcal{M}$ and that there are no short-cuts, i.e. $|w_0, w_{c-1}| = c$, thus $\mathrm{diam}(\mathcal{M}) \geq c$.

Lemma 32. $\forall e \in \{1, 2, \ldots\} : \exists m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$ *with* $b_1 < \ldots < b_m$ *such that:*

$$b_m \geq 7 \quad \textit{and} \quad G(b_1, \ldots, b_m) \quad \textit{and} \quad \prod_{i=1}^{m} b_i > {b_m}^{4e}$$

Proof. Let prim_i be the ith prime number ($\mathrm{prim}_1 = 2$) and choose $m := 8e$.
$a := \prod_{i=1}^{m} \mathrm{prim}_i$, $\forall i \in \{1, \ldots, m\} : b_i := a + \mathrm{prim}_i$.
Assume c prim, $c|b_i$, $c|b_j$, where $i, j \in \{1, \ldots, m\}$ and $i < j$.
Then: $c|((a + \mathrm{prim}_j) - (a + \mathrm{prim}_i)) \Rightarrow c|(\mathrm{prim}_j - \mathrm{prim}_i) \Rightarrow c < \mathrm{prim}_j \Rightarrow c|a$.
With $c|b_j$ follows $c|\mathrm{prim}_j$, and since $c < \mathrm{prim}_j$ we have $c = 1$. Contradiction.
Thus $G(b_1, \ldots, b_m)$ is satisfied.
$\prod_{i=1}^{m} b_i > a^m = (a^2)^{\frac{m}{2}} > (2a)^{4e} > (a + \mathrm{prim}_m)^{4e} = {b_m}^{4e}$.

Lemma 33. *If* $m, b_1, \ldots, b_m \in \{2, 3, \ldots\}$, $b_m \geq 7$, $b_1 < \ldots < b_m$, $G(b_1, \ldots, b_m)$, *then* $|T_{\langle b_1,\ldots,b_m\rangle}| + |P| < {b_m}^4$.

Proof. $|T_{\langle b_1,\ldots,b_m\rangle}| + |P|$
$= 2 + \sum_{i=1}^{m}(3 + |A_{i,b_i}|) + (1 + \sum_{i=1}^{m}(1 + |A_{i,b_i}|)) + 1$
$< 4+4m+2m|A_{m,b_m}| = 4+m({b_m}^2+7b_m-4) < b_m+b_m({b_m}^2+{b_m}^2) < {b_m}^4.$

Theorem 34. *$\forall e \in I\!N : \exists T, A$ with $T \not\vdash A$:*

$$(\mathcal{M} \models T \text{ and } \mathcal{M} \not\models A) \quad \Rightarrow \quad \mathrm{diam}(\mathcal{M}) \geq (|T| + |A|)^e$$

Proof. We combine the lemmas 28, 31, 32 and 33.

7 Embeddings

Because the accessibility relation in the Kripke structures of $\mathsf{S4}$ is transitive, $\Box B$ means that B is true in the actual world and in all the worlds in the future. This leads to the following theorem:

Theorem 35.

$$\mathit{S4} + \{B_1, \ldots, B_n\} \vdash A \quad \Leftrightarrow \quad \mathit{S4} \vdash \Box B_1 \wedge \ldots \wedge \Box B_n \to A$$

Proof. See e.g. [2].

Definition 36. $\mathsf{KT}_{\mathcal{S}}$ (resp. $(\mathsf{KT} + T)_{\mathcal{S}}$) is the calculus $\mathsf{K}_{\mathcal{S}}$ (resp. $(\mathsf{K} + T)_{\mathcal{S}}$) plus the rule

$$\frac{A, \Diamond A, \Gamma}{\Diamond A, \Gamma}\ (\Diamond)$$

Definition 37. $\mathsf{S4}_{\mathcal{S}}$ is the calculus $\mathsf{KT}_{\mathcal{S}}$ with the rule ($\Box$) replaced by

$$\frac{A, \Diamond\Gamma}{\Box A, \Diamond\Gamma}\ (\Box)$$

We extend the notation for substitution:

Definition 38. Let A be a formula, $Q_1, \ldots, Q_n$ pairwise different variables that do not occur in A, and $B_1, \ldots, B_n$ subformulas of A.
We construct a function $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $\pi(i) < \pi(j)$ implies $|B_{\pi(i)}| \geq |B_{\pi(j)}|$. First we substitute in A the variable $Q_{\pi(1)}$ for $B_{\pi(1)}$, in the result we substitute the variable $Q_{\pi(2)}$ for $B_{\pi(2)}$, ..., and finally the variable $Q_{\pi(n)}$ for $B_{\pi(n)}$ (in this order, not in parallel!). We write $A\{Q_1/B_1, \ldots, Q_n/B_n\}$ for the result.
Example: If $A \equiv \Diamond(p_0 \vee \Diamond\Box p_1) \wedge \Diamond\Box p_1$, $B_1 \equiv \Diamond\Box p_1$, $B_2 \equiv \Diamond(p_0 \vee \Diamond\Box p_1)$. Then $\pi(1) = 2$, $\pi(2) = 1$, $A\{Q_1/B_1, Q_2/B_2\} \equiv Q_2 \wedge Q_1$ (i.e. $A\{Q_1/B_1, Q_2/B_2\} \not\equiv \Diamond(p_0 \vee Q_1) \wedge Q_1$).

Theorem 39. *If A is a formula, $\Diamond C_1, \ldots, \Diamond C_n$ are the $\Diamond$ subformulas of A, $Q_1, \ldots, Q_n$ are variables that do not occur in A,*
for all $i \in \{1, \ldots n\}$: $C_i' :\equiv C_i\{Q_1 / \Diamond C_1, \ldots, Q_n / \Diamond C_n\}$,
$A' :\equiv A\{Q_1 / \Diamond C_1, \ldots, Q_n / \Diamond C_n\}$,
$T' := \{Q_1 \vee \neg(\Diamond Q_1 \vee \Diamond C_1'), \ldots, Q_n \vee \neg(\Diamond Q_n \vee \Diamond C_n')\}$,
then:

$$\mathsf{S4} \vdash A \quad \Leftrightarrow \quad \mathsf{KT} + T' \vdash A'$$

Proof.
'$\Rightarrow$': Let $\mathcal{P}$ be a proof of A in $\mathsf{S4}_{\mathcal{S}}$. We construct a proof $\mathcal{P}'$ of A' in $(\mathsf{KT} + T)_{\mathcal{S}}$. The root of $\mathcal{P}'$ is A'. An application of a rule in $\mathcal{P}$ becomes in $\mathcal{P}'$ an application of the corresponding rule of $(\mathsf{KT} + T)_{\mathcal{S}}$.
If Q_i occurs in a sequent in $\mathcal{P}'$, then we insert just above this sequent the part

$$\dfrac{\dfrac{Q_i, \neg Q_i}{Q_i, \neg Q_i, \Gamma}\,(\text{weak}) \qquad \dfrac{\dfrac{\dfrac{\Diamond Q_i, \Diamond C_i', \Gamma}{Q_i, \Diamond Q_i, \Diamond C_i', \Gamma}\,(\text{weak})}{Q_i, \Diamond Q_i \vee \Diamond C_i', \Gamma}\,(\vee)}{}}{\dfrac{Q_i, \neg Q_i \wedge (\Diamond Q_i \vee \Diamond C_i'), \Gamma}{Q_i, \Gamma}\,(\text{th})}\,(\wedge)$$

The inserted part has two purposes:

- If $\Diamond C_i$ occurs for the first time on a branch in $\mathcal{P}$ (seen from the root), then it makes sure that $\Diamond C_i'$ occurs in the corresponding sequent in $\mathcal{P}'$.
- In contrast to $\mathsf{S4}_{\mathcal{S}}$, a backward application on $(\Box)$ in $(\mathsf{KT} + T)_{\mathcal{S}}$ destroys leading $\Diamond$ connectives. The inserted part regenerates them by 'replacing' Q_i by $\Diamond Q_i$.

Thus we know that if $\Diamond C_i$ occurs in a sequent in $\mathcal{P}$, then $\Diamond C_i'$ occurs in the corresponding sequent in $\mathcal{P}'$, i.e. we can continue with the construction.
'$\Leftarrow$': Let $\mathcal{P}'$ be a proof of A' in $(\mathsf{KT} + T)_{\mathcal{S}}$. We construct a proof $\mathcal{P}$ of A in $\mathsf{S4}_{\mathcal{S}}$. The root of $\mathcal{P}$ is A.
Because the rules (th), $(\Diamond)$, $(\wedge)$, $(\vee)$ of $(\mathsf{KT} + T')_{\mathcal{S}}$ are invertible, we can assume that the (th) rule is applied in $\mathcal{P}'$ only in the context displayed above. (If a $(\Box)$ rule is used on the left branch, then the (th) application in $\mathcal{P}'$ is superfluous.) These parts can be omitted in $\mathcal{P}$. Applications of $(\Diamond)$ with the main formula $\Diamond Q_i$ in $\mathcal{P}'$ can be omitted in $\mathcal{P}$ as well.
Axioms of the form $Q_i, \neg Q_i$ can only occur in the situation displayed above, since there is no negative occurrence of Q_i in A' and only one positive occurrence of Q_i in T'. The remaining rules resp. axioms in $\mathcal{P}'$ are replaced by the corresponding rules resp. axioms of $\mathsf{S4}_{\mathcal{S}}$.

Example 3. $A \equiv \Diamond(p_0 \vee \Box \Diamond \neg p_0) \wedge p_0$.
Thus $n = 2$, $C_1 \equiv p_0 \vee \Box \Diamond \neg p_0$, $C_2 \equiv \neg p_0$. We choose $Q_1 \equiv p_1$, $Q_2 \equiv p_2$.
$C_1' \equiv p_0 \vee \Box Q_2$, $C_2' \equiv \neg p_0$.
$A' \equiv Q_1 \wedge p_0$.
$T' = \{Q_1 \vee \neg(\Diamond Q_1 \vee \Diamond C_1'), Q_2 \vee \neg(\Diamond Q_2 \vee \Diamond C_2')\}$.

The accessibility relation of the Kripke structures of KT must be reflexive, thus $\Diamond A$ is also satisfied if A is satisfied in the actual world. The embedding k used in [3] simulates this interpretation. We extend it to theories.

Definition 40. $\mathrm{k}(P) :\equiv P$, $\mathrm{k}(\neg P) :\equiv \neg P$, $\mathrm{k}(\Box A) :\equiv \Box\mathrm{k}(A)$, $\mathrm{k}(\Diamond A) :\equiv \mathrm{k}(A) \vee \Diamond\mathrm{k}(A)$, $\mathrm{k}(A \wedge B) :\equiv \mathrm{k}(A) \wedge \mathrm{k}(B)$, $\mathrm{k}(A \vee B) :\equiv \mathrm{k}(A) \vee \mathrm{k}(B)$.
If $T = \{B_1, \ldots, B_n\}$, then $\mathrm{k}(T) := \{\neg\mathrm{k}(\neg B_1), \ldots, \neg\mathrm{k}(\neg B_n)\}$.

Theorem 41.

$$\begin{aligned} \mathsf{K} \vdash k(A) \quad &\Leftrightarrow \quad \mathsf{KT} \vdash A \\ \mathsf{K} + k(T) \vdash k(A) \quad &\Leftrightarrow \quad \mathsf{KT} + T \vdash A \end{aligned}$$

Proof. Induction on proof length.

Note 42. In spite of the simple definition, $|\mathrm{k}(A)|$ can be much longer than $|A|$, for example $|\mathrm{k}(\Diamond^n p_0)| > 2^n$. This problem is diminished if structure sharing is used (provided that $\Box$, $\Diamond$, $\neg$, $\wedge$, $\vee$ are the only connectives of the language).

The same ideas that lead to lemma 26 immediately give an – of course very inefficient – embedding of $\mathsf{K} + T$ in K.

Theorem 43. *If T is finite, C is the conjunction of the elements of T, then:*

$$K + T \vdash A \ \Leftrightarrow\ \mathsf{K} \vdash C \wedge \Box C \wedge \ldots \wedge \Box^{2^{|A|+|T|}} C \to A$$

Summary:

$$\begin{tikzcd} \mathsf{S4} + T \arrow[r, dash, "\text{Th. 35}"] & \mathsf{S4} \arrow[d, dash, "\text{Th. 39}"] & \\ & \mathsf{KT} + T \arrow[d, dash, "\text{Th. 41}"] & \mathsf{KT} \arrow[d, dash, "\text{Th. 41}"] \\ & \mathsf{K} + T \arrow[r, dash, "\text{Th. 43}"] & \mathsf{K} \end{tikzcd}$$

8 Implementation

Decision procedures for K, $\mathsf{K} + T$, KT, $\mathsf{KT} + T$, $\mathsf{S4}$, and $\mathsf{S4} + T$ are implemented in the Logics Workbench LWB ([7]). These decision procedures were intensively used in [5] to prove the equivalence of propositional normal modal logics.
It is possible to use these decision procedures via WWW. Start a WWW browser, open `http://lwbwww.unibe.ch:8080/LWBinfo.html` and choose the item `run a session`.
If you want to run the example from section 4, type

```
load(k);
provable(box p0, [p1, box(p1 -> p0)]);
```

and press the `send` button. After a while you obtain the result.

9 Conclusion

After discussing methods for efficient backward proof search in $\mathsf{K}+T$, we proved that in $K+T$ the construction of a counter-model and therefore backward proof search is (in a certain sense) harder than in K. We did not investigate the complexity of $\mathsf{K}+T$. (From [8] one obtains the lower bound PSPACE, and from [6] the upper bound EXPTIME.)
Another sign of a considerable expressiveness of $\mathsf{K}+T$ is the existence of the natural embedding of $\mathsf{S4}$ in $\mathsf{K}+T$ we constructed in the last section.

To typeset the proof trees we used a macro package by Dirk Roorda. Thanks to Wolfgang Heinle and Werner Wolff for some helpful remarks.

References

1. Laurent Catach. Tableaux: A general theorem prover for modal logics. *Journal of Automated Reasoning*, 7:489–510, 1991.
2. Melvin Fitting. *Proof Methods for Modal and Intuitionistic Logics.* Reidel, Dordrecht, 1983.
3. Melvin Fitting. First-order modal tableaux. *Journal of Automated Reasoning*, 4:191–213, 1988.
4. Rajeev Goré. Tableau methods for modal and temporal logics. Technical report, TR-15-95, Automated Reasoning Project, Australian National University, Canberra, Australia, 1995. To appear in Handbook of Tableau Methods, Kluwer, 199?
5. Rajeev Goré, Wolfgang Heinle, and Alain Heuerding. Relations between propositional normal modal logics: an overview. Submitted.
6. Joseph Y. Halpern and Yoram Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54:319–379, 1992.
7. Alain Heuerding, Gerhard Jäger, Stefan Schwendimann, and Michael Seyfried. Propositional logics on the computer. In *Theorem Proving with Analytic Tableaux and Related Methods*, LNCS 918, 1995.
8. Richard E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.
9. Ilkka Niemelä and Heikki Tuominen. Helsinki logic machine: A system for logical expertise. Technical report, Digital Systems Laboratory, Department of Computer Science, Helsinki University of Technology, 1987.
10. F. Oppacher and E. Suen. Harp: A tableau-based theorem prover. *Journal of Automated Reasoning*, 4:69–100, 1988.
11. Dan Sahlin, Torkel Franzén, and Seif Haridi. An intuitionistic predicate logic theorem prover. *Journal of Logic and Computation*, 2(5):619–656, 1992.
12. Kurt Schütte. *Vollständige Systeme modaler und intuitionistischer Logik.* Springer, 1968.
13. Alasdair Urquhart. Complexity of proofs in classical propositional logic. In Yiannis N. Moschovakis, editor, *Logic from Computer Science*, pages 597–608. Springer, 1992.
14. Lincoln Wallen. *Automated Proof Search in Non-Classical Logics.* M.I.T. Press, Cambridge, Massachusetts, 1990.

This article was processed using the LaTeX macro package with LLNCS style