T-79.298 Postgraduate Course in Digital Systems Science:

Completeness and Decision Procedures for Multimodal Logic and (Restricted) Temporal Logic

Petteri Kaski
petteri.kaski@hut.fi

November 26, 2001

1 Introduction

A *logic* can be viewed as a formal system that has two components: (a) a language in which to state properties (the *syntax*); and (b) a means for attaching a notion of truth and validity to the sentences of the language (the *semantics*). Also required is the concept of *entailment* for determining whether a sentence is a semantic consequence of a collection of sentences, called the *premises*. For example, if the premises are "today it rains" and "a rainy day is followed by a sunny day", then the semantics of the language allows us to decide whether "tomorrow is sunny" is entailed by the premises.

A *proof system* for a logic is a syntactic method for deriving sentences of the language out of a given collection of premises. For a proof system to be of use in logical reasoning, that is, in establishing or disproving semantic consequence, the set of sentences derivable from a given set of premises must parallel the semantic notion of entailment. Specifically, a proof system is *sound* if every sentence derivable from a collection of premises is also semantically entailed by the premises. In other words, if a proof system is sound, then the fact that we can derive "tomorrow is sunny" from the premises really implies that tomorrow is sunny. On the other hand, a proof system is *complete* if every sentence entailed by the premises is also derivable from the premises using the proof system.

In the model checking context our interest lies in establishing the existence of proof systems that are sound and complete for the modal and temporal logics commonly employed in system verification. Often the study of such proof systems enables one to derive algorithmic *decision procedures* that enable the automation of logical reasoning. Often such decision procedures in turn form a basis for efficient model checking algorithms.

This text is an expository treatment of proof systems and decision procedures for multimodal and temporal logics based on Chapters 6 and 7 of the survey article *Model Checking* by E. Clarke and B.-H. Schlingloff [1]. Additional influence was obtained from [2, 3, 7] and a set of old lecture notes from the course "Tik-79.146 Logic in Computer Science: Special Topics I" lectured by Professor Ilkka Niemelä at HUT.

The organization of this text is as follows. The first two sections consist of the necessary preliminaries. Section 2 presents the syntax and semantics of the two logics studied. The first logic considered is standard multimodal logic on arbitrary Kripke models. The second logic is a simplified temporal logic that contains an operator for reasoning about the "future" but lacks an "until"-operator. Section 3 defines concepts related to formal proof systems. The emphasis of this text is on Sections 4 and 5, where we present deductive proof systems for the two logics considered, and establish their soundness and completeness. The subsequent treatment is devoted to algorithmic decision procedures for the two logics. Section 6 derives generic decision procedures for the two logics based on the finite model property. Section 7 sketches a tableau-based decision method for the restricted temporal logic on

natural models. Finally, there is an appendix that contains proofs of some technical results that are required in the completeness proofs.

2 The two logics studied

2.1 Multimodal logic

Let $\mathcal{P}$ be a nonempty set of *atomic propositions* and let $\mathcal{R}$ be a nonempty set of *accessibility relation symbols*. The language of *multimodal logic* consists of all finite sentences that are defined recursively as follows

(i) Every atomic proposition $p \in \mathcal{P}$ is a sentence.

(ii) The symbol $\bot$ is a sentence.

(iii) If ϕ and ψ are sentences, then $(\phi \to \psi)$ is a sentence.

(iv) If $R \in \mathcal{R}$ is a relation symbol and ϕ is a sentence, then $\langle R \rangle \phi$ is a sentence.

The definition above can be expressed more compactly using the formal grammar below.

$$\mathbf{ML} \stackrel{\text{def}}{=} \mathcal{P} \mid \bot \mid (\mathbf{ML} \to \mathbf{ML}) \mid \langle \mathcal{R} \rangle \mathbf{ML}. \quad (1)$$

We assume that both $\mathcal{P}$ and $\mathcal{R}$ are at most countable sets to guarantee that the sentences formed using (1) constitute a set that is at most countable. (This property will be required later in Lemma 4.9.) In what follows we shall denote by **ML** the set of all finite sentences constructed according to (1).

For $\phi, \psi \in \mathbf{ML}$ we use the following standard syntactic abbreviations:

$$\neg\phi \stackrel{\text{def}}{=} (\phi \to \bot) \qquad (\phi \vee \psi) \stackrel{\text{def}}{=} (\neg\phi \to \psi)$$
$$(\phi \wedge \psi) \stackrel{\text{def}}{=} \neg(\neg\phi \vee \neg\psi) \qquad [R]\phi \stackrel{\text{def}}{=} \neg\langle R \rangle \neg\phi$$
$$\top \stackrel{\text{def}}{=} \neg\bot$$

We emphasize that these abbreviations are indeed for syntactic convenience only, and that the real **ML** sentences denoted by the abbreviations can always be substituted in place of the abbreviations without loss of generality in what follows.

The semantics of multimodal logic is defined through Kripke models, which attach a concrete interpretation to each **ML** sentence with respect to which semantic notions (e.g. truth, validity, entailment) can be evaluated.

Definition 2.1 A *Kripke model* for **ML** is a triple $\mathcal{M} = (U, \mathcal{I}, w_0)$, where

(i) U is a nonempty set of *states*;

(ii) $\mathcal{I}$ is a function that associates

- ▷ an *accessibility* relation $\mathcal{I}(R) \subseteq U \times U$ to each relation symbol $R \in \mathcal{R}$; and
- ▷ a subset $\mathcal{I}(p) \subseteq U$ to each proposition symbol $p \in \mathcal{P}$.

(iii) $w_0 \in U$ is the *current state*.

If we omit the current state w_0 from a model $\mathcal{M} = (U, \mathcal{I}, w_0)$, then the resulting structure $\mathcal{F} = (U, \mathcal{I})$ is called a *frame*.

We warn the reader that the above definitions for a Kripke model and a frame are somewhat nonstandard. We use them nevertheless for compatibility with [1].

Definition 2.2 (Truth) The truth of an **ML** sentence ϕ in a Kripke model $\mathcal{M} = (U, \mathcal{I}, w_0)$ is defined recursively by the structure of the sentence. We write $\mathcal{M} \models \phi$ if ϕ is *true* in $\mathcal{M}$; otherwise ϕ is *false* and we write $\mathcal{M} \not\models \phi$.

(i) For every $p \in \mathcal{P}$, we have $\mathcal{M} \models p$ if and only if $w_0 \in \mathcal{I}(p)$; and

(ii) Always $\mathcal{M} \not\models \bot$; and

(iii) For every $\psi_1, \psi_2 \in \mathbf{ML}$, we have $\mathcal{M} \models (\psi_1 \to \psi_2)$ if and only if either $\mathcal{M} \not\models \psi_1$ or $\mathcal{M} \models \psi_2$; and

(iv) For every $\psi \in \mathbf{ML}$, we have $\mathcal{M} \models \langle R \rangle \psi$ if and only if there exists a $w_1 \in U$ such that $(w_0, w_1) \in \mathcal{I}(R)$ and $(U, \mathcal{I}, w_1) \models \psi$.

If a frame $\mathcal{F} = (U, \mathcal{I})$ can be understood from the context, we shall write only $w \models \phi$ to indicate that $(U, \mathcal{I}, w) \models \phi$ for $w \in U$.

We make a slight digression here and remark that sometimes it is convenient to use an alternative formulation of **ML** in which the operator $\langle R \rangle$ is replaced with its *dual* operator $[R]$. In this case every sentence of the form $\langle R \rangle \phi$ is a syntactic abbreviation for $\neg[R]\neg\phi$, and (iv) in the above definition is replaced by (iv') below.

(iv') For every $\psi \in \mathbf{ML}$, we have $\mathcal{M} \models [R]\psi$ if and only if for every $w_1 \in U$ satisfying $(w_0, w_1) \in \mathcal{I}(R)$ it holds that $(U, \mathcal{I}, w_1) \models \psi$.

(This alternative formulation will be more convenient to use in Section 4.)

Informally, validity in logic extends the notion of a sentence being true locally to a global context. For example, recall that in propositional logic validity simply means that a sentence is true in all truth valuations. In modal logic the situation is more involved due to the additional structure present in the model. To keep things relatively simple, in this text we will only consider (a) validity in a fixed frame and (b) validity with respect to the class of all models $\mathscr{M}$ applicable to a logic. For **ML** the class $\mathscr{M}$ is the class of all Kripke models. These concepts are formalized in the following definition.

Definition 2.3 (Validity) An **ML** sentence ϕ is *valid in a frame* $\mathcal{F} = (U, \mathcal{I})$, written $\mathcal{F} \models \phi$, if $(U, \mathcal{I}, w) \models \phi$ for every $w \in U$. If $\mathcal{M} \models \phi$ holds for all models $\mathcal{M}$ in $\mathscr{M}$, then we say that ϕ is *(universally) valid*, written $\models \phi$.

The "dual" concepts for validity are satisfiability unsatisfiability.

Definition 2.4 (Satisfiability) An **ML** sentence is *satisfiable* if there exists a model in which the sentence is true. A sentence ϕ is *unsatisfiable* if it has no satisfying model (in other words, $\neg\phi$ is valid).

Akin to validity, the notion of logical consequence has several variations in modal logic. This text uses a global form of consequence (that is, validity of the premises in a frame implies validity of the conclusion in the frame) with respect to the class $\mathscr{M}$.

Definition 2.5 (Semantic consequence) Let $\phi \in \mathbf{ML}$ be a sentence and suppose $\Phi \subseteq \mathbf{ML}$ is a set of sentences. Then, ϕ is a *consequence* of Φ, written $\Phi \Vdash \phi$, if every frame that validates every sentence in Φ also validates ϕ. The sentences in Φ are in this context called *premises* and the sentence ϕ is the *conclusion.*

Observe that no restrictions were placed on Φ. In particular, it can be infinite as well as empty. In the case that Φ is empty we write simply $\Vdash \phi$; note that this coincides with the universal validity of a sentence, that is, $\Vdash \phi$ if and only if $\models \phi$.

2.2 Monomodal logic with transitive closure

The accessibility relations of multimodal logic can be viewed as giving the *immediate* successor state of a state in the Kripke model at hand, that is, w' is an immediate R-successor state of w if and only if $(w, w') \in \mathcal{I}(R)$. Being able to reason with immediate successor states is often not enough, however. What is required is the ability to state and verify properties that hold for *all* the successor states of a given state. Formally, this amounts to saying that a property must hold in all states which are accessible from w through the *transitive closure* of $\mathcal{I}(R)$.

Definition 2.6 Let $A \subseteq U \times U$ be a binary relation on U. The *transitive closure* of A is the intersection of all $S \subseteq U \times U$ that satisfy

(i) $A \subseteq S$; and

(ii) for every $w_0, w_1, w_2 \in U$, if $(w_0, w_1) \in S$ and $(w_1, w_2) \in S$, then $(w_0, w_2) \in S$.

We denote the transitive closure of A by A^+.

An equivalent definition for transitive closure is reached if we define A^+ as the set of all $(w, w') \in U \times U$ for which there exists a finite sequence $w_1, \ldots, w_n \in U$ that satisfies (a) $w_1 = w$, (b) $w_n = w'$, and (c) $(w_i, w_{i+1}) \in A$ holds for all $i = 1, \ldots, n-1$. This latter definition will be employed in the remainder of this text. (The equivalence proof for the two definitions is left as an illustrative exercise for the reader.)

We incorporate transitive closure into multimodal logic by performing the following modifications to the syntax and semantics of **ML**. First, we shall consider only *monomodal* logic, that is, a modal logic with a single accessibility relation. This simplifies the treatment without significant loss in generality.[1] Let us denote this accessiblity relation by the symbol $\prec$ and its transitive closure by

[1] The reader is invited to consider how the monomodal proof systems and decision procedures presented later in this text could be extended to cover the multimodal logic with transitive closure and universal accessibility presented in [1, Sec. 2.2].

$<$. Thus, the modification to the syntax of **ML** simply consists of fixing $\mathcal{R} = \{\prec, <\}$. The main modification is a semantical one. Namely, we restrict the class of Kripke models $\mathscr{M}$ with respect to which the truth, validity, and entailment of sentences are evaluated to the class of models that fix the interpretation of $<$ as

$$\mathcal{I}(<) \stackrel{\text{def}}{=} \mathcal{I}(\prec)^+. \tag{2}$$

We shall call the logic that results from these modifications $\mathbf{ML}_1^+$.

We remark that incorporating (2) into the logic with the above restrictions changes the expressivity of the logic in a fundamental way. We shall see some consequences of this (e.g. noncompactness) later.

To simplify the notation in what follows, we shall adopt the standard syntactic abbreviations listed below.

$$\mathbf{X}\phi \stackrel{\text{def}}{=} \langle\prec\rangle\phi, \qquad \mathbb{X}\phi \stackrel{\text{def}}{=} \neg\mathbf{X}\neg\phi,$$
$$\mathbf{F}^+\phi \stackrel{\text{def}}{=} \langle<\rangle\phi, \qquad \mathbf{F}^*\phi \stackrel{\text{def}}{=} (\phi \vee \mathbf{F}^+\phi),$$
$$\mathbf{G}^+\phi \stackrel{\text{def}}{=} \neg\mathbf{F}^+\neg\phi, \qquad \mathbf{G}^*\phi \stackrel{\text{def}}{=} \neg\mathbf{F}^*\neg\phi.$$

It is straightforward to verify from the semantics of these operators that $\mathbf{X}, \mathbf{F}^+$ is not the only combination which is sufficient to describe the six operators above. For example, either $\mathbb{X}, \mathbf{G}^*$ or $\mathbf{X}, \mathbf{F}^*$ can be used instead.

To further simplify the notation when a frame $\mathcal{F} = (U, \mathcal{I})$ has been fixed, we shall write simply $w \prec w'$ (respectively, $w < w'$) to indicate $(w, w') \in \mathcal{I}(\prec)$ (respectively, $(w, w') \in \mathcal{I}(<)$) for states $w, w' \in U$. The notation $w \leq w'$ is used to indicate verbatim "either $w = w'$ or $w < w'$".

3 Proof systems

In this section we define proof systems in an abstract setting to illustrate their syntactic nature. The following two sections will then present real-world proof systems for the logics **ML** and $\mathbf{ML}_1^+$.

3.1 Deductive proof systems

We start by defining deductive proof systems without fixing any particular logic on the sentences of which we operate. So, let **L** be any nonempty set (of sentences).

Definition 3.1 (Deductive proof system) A *deductive proof system* (alternatively, a *Hilbert-style proof system*) for **L** consists of a set of axioms and a set of deductive rules, where

(i) the set of *axioms* is a subset of **L**; and

(ii) a *deductive rule*, written $\phi_1, \ldots, \phi_M \vdash \psi$, consists of a finite nonempty set of *prerequisite* sentences $\phi_1, \ldots, \phi_M \in \mathbf{L}$ and a *conclusion* sentence $\psi \in \mathbf{L}$.[2]

The previous definition was presented to emphasize the syntactic nature of a deductive proof system: It is simply a construct built from the sentences in **L** without any reference to possible semantics of the sentences. *If* there is a connection between the proof system and the semantics of the sentences, then it has to be explicitly demonstrated.

A deductive proof system does not yet allow us to *prove* anything. What is required is the concept of a *proof*. Before presenting the following definitions we emphasize that everything is still performed entirely on a syntactic level. That is, we only manipulate elements of an arbitrary nonempty set **L** according to a proof system for **L** without attaching any semantic notions (e.g. truth or validity) to the sentences.

Definition 3.2 (Proof) Let **L** be a nonempty set of sentences and fix a deductive proof system $\mathscr{P}$ for **L**. A finite sequence of sentences $\psi_1, \ldots, \psi_N$ is a *proof* of $\psi \in \mathbf{L}$ if

(i) $\psi = \psi_N$; and

(ii) for every $i = 1, \ldots, N$, the sentence ψ_i is (a) an axiom or (b) the conclusion of a deductive rule whose prerequisite sentences $\phi_1, \ldots, \phi_M$ appear earlier in the sequence. (More formally, there exist $j_1, \ldots, j_M \in \mathbb{N}$ such that, for every $k = 1, \ldots, M$, both $1 \leq j_k < i$ and $\phi_k = \psi_{j_k}$.)

Definition 3.3 (Provability) Let **L** be a nonempty set of sentences and fix a deductive proof system $\mathscr{P}$ for **L**. A sentence $\psi \in \mathbf{L}$ is *provable*, written $\vdash \psi$, if there exists a proof for ψ.

The following two examples illustrate that provability can vary greatly depending on the proof system.

[2] Formally we may treat deductive rules as an ordered pairs $(\{\phi_1, \ldots, \phi_M\}, \psi)$, where $\{\phi_1, \ldots, \phi_M\} \subseteq \mathbf{L}$ is finite and nonempty, and $\psi \in \mathbf{L}$.

Example 3.4 Suppose a deductive proof system for $\mathbf{L}$ has an empty axiom set. Then, no sentence $\phi \in \mathbf{L}$ is provable.

Example 3.5 Suppose a deductive proof system for $\mathbf{L}$ has all sentences in $\mathbf{L}$ as axioms. Then, every $\phi \in \mathbf{L}$ is provable in this system since ϕ is an axiom and admits a proof $\phi = \phi_1$.

Definition 3.6 (Derivation) Let $\mathbf{L}$ be a nonempty set of sentences and fix a deductive proof system $\mathscr{P}$ for $\mathbf{L}$. A finite sequence of sentences $\psi_1, \ldots, \psi_N$ is a *derivation* of $\psi \in \mathbf{L}$ from a set of *premises* $\Phi \subseteq \mathbf{L}$ if

(i) $\psi = \psi_N$; and

(ii) for every $i = 1, \ldots, N$, the sentence ψ_i is (a) an axiom, (b) a premise, or (c) the conclusion of a deductive rule whose prerequisite sentences $\phi_1, \ldots, \phi_M$ appear earlier in the sequence. (More formally, there exist $j_1, \ldots, j_M \in \mathbb{N}$ such that, for every $k = 1, \ldots, M$, both $1 \leq j_k < i$ and $\phi = \psi_{j_k}$.)

Definition 3.7 (Provable consequence) Let $\mathbf{L}$ be a nonempty set of sentences and fix a deductive proof system for $\mathbf{L}$. A sentence $\phi \in \mathbf{L}$ is a *provable consequence* of $\Phi \subseteq \mathbf{L}$, written $\Phi \vdash \phi$, if there exists a derivation of ϕ from the premises in Φ.

3.2 Soundness and completeness

The last section considered deductive proof systems as syntactic objects only. In this section we attach the syntactic notions of provability and provable consequence to the semantic notions of validity and semantic consequence.

Fix a logic $\mathbf{L}$ and a (not necessarily deductive) proof system $\mathscr{P}$ for the logic. Recall that the semantics of a logic allows us to distinguish which sentences $\phi \in \mathbf{L}$ are valid (written $\Vdash \phi$) and which are semantic consequences of a set of premises $\Phi \subseteq \mathbf{L}$ (written $\Phi \Vdash \phi$). On the other hand, the proof system $\mathscr{P}$ provides us with analogous syntactic concepts of provability ($\vdash \phi$) and provable consequence ($\Phi \vdash \phi$).

For a proof system to be of significant use in logical reasoning, it is certainly desirable to require that provable consequence always implies semantic consequence. In other words, if we can prove a sentence is a consequence of the premises, then it really is a consequence of the premises in the semantic sense.

Definition 3.8 (Soundness) A proof system $\mathscr{P}$ for a logic $\mathbf{L}$ is *sound* if, for all $\Phi \subseteq \mathbf{L}$ and $\phi \in \mathbf{L}$, $\Phi \vdash \phi$ implies $\Phi \Vdash \phi$.

On the other hand, the usefulness of a proof system is significantly decreased if the nonexistence of a derivation is insufficient to demonstrate that semantic consequence does not hold. In other words, it is desirable that semantic consequence always implies provable consequence.

Definition 3.9 (Completeness) A proof system $\mathscr{P}$ for a logic $\mathbf{L}$ is *(strongly) complete* if, for all $\Phi \subseteq \mathbf{L}$ and $\phi \in \mathbf{L}$, $\Phi \Vdash \phi$ implies $\Phi \vdash \phi$.[3]

Both soundness and completeness are required for a proof system to be truly useful. To give two pathological examples of useless proof systems from a semantic viewpoint, consider Examples 3.4 and 3.5, where the former proof system is sound and the latter is complete.

4 Deductive proof system for ML

In this section we give a deductive proof system for multimodal logic **ML** and prove that it is both sound and complete.

As a preliminary we shall formalize the concept of substituting sentences in place of atomic propositions in a sentence. Let $\tau : \mathcal{P} \to \mathbf{ML}$ be a mapping that associates to each atomic proposition $p \in \mathcal{P}$ an **ML** sentence $\tau(p)$. Then, τ induces a mapping $\tilde{\tau} : \mathbf{ML} \to \mathbf{ML}$ defined recursively by the structure of a sentence:

(i) $\tilde{\tau}(p) \stackrel{\text{def}}{=} \tau(p)$ for all $p \in \mathcal{P}$.

(ii) $\tilde{\tau}(\bot) \stackrel{\text{def}}{=} \bot$.

(iii) $\tilde{\tau}((\psi_1 \to \psi_2)) \stackrel{\text{def}}{=} (\tilde{\tau}(\psi_1) \to \tilde{\tau}(\psi_2))$ for all $\psi_1, \psi_2 \in \mathbf{ML}$.

[3] We shall later encounter a weaker form of completeness in which the set Φ is restricted to be finite.

(iv) $\tilde{\tau}(\langle R\rangle\psi) = \langle R\rangle\tilde{\tau}(\psi)$ for all $\psi \in \mathbf{ML}$ and $R \in \mathcal{R}$.

Definition 4.1 Let $\phi, \psi \in \mathbf{ML}$. We say that ψ has been *constructed from ϕ by substitution* if there exists a $\tau : \mathcal{P} \to \mathbf{ML}$ such that $\psi = \tilde{\tau}(\phi)$.

Example 4.2 Let $\mathcal{P} = \{a, b\}$ and define $\tau : \mathcal{P} \to \mathbf{ML}$ by setting $\tau(a) = (a \to b)$ and $\tau(b) = (b \to \bot)$. Then,

$$\psi = ((a \to b) \to (b \to \bot))$$

has been constructed from $\phi = (a \to b)$ by substitution since $\tilde{\tau}(\phi) = \psi$.

We now proceed to discuss the deductive proof system for **ML**. Recall that a deductive proof system consists of a set of axioms and a set of deductive rules.

The **ML** proof system has two types of axioms. Axioms of the first type consist of all sentences constructible from propositional tautologies[4] by substitution. The following example illustrates axioms of the first type.

Example 4.3 Suppose that $p \in \mathcal{P}$. Then, $(p \to p)$ is clearly a propositional tautology. Take $R \in \mathcal{R}$. Then, $([R]p \to [R]p)$ is an axiom constructed from a propositional tautology by substitution $\tau(p) = [R]p$.

Axioms of the second type consist of sentences constructible by substitution from sentences of the form $([R](p \to q) \to ([R]p \to [R]q))$, where $p, q \in \mathcal{P}$ and $R \in \mathcal{R}$ are arbitrary.

The **ML** proof system has two types of deductive rules. First is the standard *modus ponens* rule that allows us to deduce the conclusion q from the prerequisites p and $p \to q$, where $p, q \in \mathcal{P}$. The second rule type, also known as the *necessitation* rule, allows us to conclude $[R]p$ from p for any $p \in \mathcal{P}$ and $R \in \mathcal{R}$. We again allow arbitrary substitutions $\tau : \mathcal{P} \to \mathbf{ML}$ to occur in the deductive rules, as long as the same substitution $\tilde{\tau}$ is applied to all prerequisite sentences and to the conclusion.

To summarize, we may express the deductive proof system for **ML** briefly as:

(T)	(Propositional tautologies)
(K)	$([R](p \to q) \to ([R]p \to [R]q))$
(MP)	$p,\ (p \to q) \vdash q$
(N)	$p \vdash [R]p,$

where it is understood that arbitrary **ML** sentences can be substituted in place of the atomic propositions $p, q \in \mathcal{P}$.

4.1 Examples

Let us now present some derivations that illustrate how the proof system is used.

Example 4.4 Let ϕ, ψ be arbitrary **ML** sentences and suppose $\Phi = \{(\phi \to \psi)\}$. We derive $[R]\phi \to [R]\psi$ as follows:

1.	$\phi \to \psi$	(GP)
2.	$[R](\phi \to \psi)$	(1,N)
3.	$([R](\phi \to \psi) \to ([R]\phi \to [R]\psi))$	(K)
4.	$([R]\phi \to [R]\psi)$	(2,3,MP)

Observe that the right hand side column in the derivation illustrates which rule has been applied to deduce the sentence at each row. For example, (GP) indicates that the rule is a global premise, (1,N) indicates that the sentence is deduced from sentence 1 of the derivation using the necessitation rule, (K) indicates that the sentence is an axiom, and (2,3,MP) indicates that the sentence is deduced from sentences 2 and 3 using the modus ponens rule.

Let us consider a slightly more complex derivation.

Example 4.5 Let ϕ, ψ be arbitrary **ML** sentences and suppose $\Phi = \{(\phi \to \psi)\}$. We derive $(\langle R\rangle\phi \to \langle R\rangle\psi)$ as follows:

1.	$\phi \to \psi$	(GP)
2.	$((\phi \to \psi) \to (\neg\psi \to \neg\phi))$	(T)
3.	$(\neg\psi \to \neg\phi)$	(1,2,MP)
4.	$[R](\neg\psi \to \neg\phi)$	(3,N)
5.	$([R](\neg\psi \to \neg\phi) \to ([R]\neg\psi \to [R]\neg\phi))$	(K)
6.	$([R]\neg\psi \to [R]\neg\phi)$	(4,5,MP)

[4] Recall that a *propositional tautology* is a sentence of propositional logic that is true in all truth valuations of propositional logic. For the purposes of this text it suffices to define a propositional tautology as an **ML** sentence that

(i) does not contain either of the modal operators $[R]$ and $\langle R\rangle$ for any $R \in \mathcal{R}$; and

(ii) is universally valid (see Definition 2.3).

7. $((\Box[R]\neg\psi \rightarrow \Box[R]\neg\phi) \rightarrow (\neg\Box[R]\neg\phi \rightarrow \neg\Box[R]\neg\psi))$ (T)
8. $(\neg\Box[R]\neg\phi \rightarrow \neg\Box[R]\neg\psi)$ (6,7,MP)
9. $(\Diamond\langle R\rangle\phi \rightarrow \langle R\rangle\psi)$ (8,Def)

Here (T) denotes an axiom obtained by substitution from a propositional tautology. The description (8,Def) indicates that the sentence is equivalent to sentence 8 by definition (in other words, sentence 9 is a syntactic abbreviation of sentence 8).

As the reader can probably observe, certain intuition is required in determining the correct axioms that produce a derivation for a sentence. Indeed, as far as the present author is aware, there exists no efficient algorithm that produces a Hilbert-style derivation for a fixed target sentence ϕ. Luckily enough, we shall later in this text encounter proof systems that can be automated more efficiently.

4.2 Soundness and completeness

In what follows we shall prove that the presented deductive proof system for **ML** is both sound and complete. Typically for such proofs, the soundness proof is straightforward, whereas the completeness proof is more involved.

Theorem 4.6 *The presented deductive proof system for* **ML** *is sound.*

Proof. Let $\Phi \subseteq \mathbf{ML}$ be a set of premises and let $\phi \in \mathbf{ML}$. Suppose that $\phi_1, \ldots, \phi_N$ is a derivation of ϕ from Φ. Recall that $\Phi \Vdash \phi$ holds if every frame $\mathcal{F} = (U, \mathcal{I})$ that validates every sentence in Φ also validates ϕ. Fix an arbitrary frame $\mathcal{F} = (U, \mathcal{I})$ in which every sentence in Φ is valid. Our task is to show that $\mathcal{F} \models \phi_N$. We proceed inductively by showing that if $\mathcal{F} \models \phi_j$ for all $j = 1, \ldots, i-1$, then it must be that $\mathcal{F} \models \phi_i$. Thus, $\mathcal{F} \models \phi_N$, and since $\mathcal{F}$ was arbitrary, we have $\Phi \Vdash \phi$.

Suppose that $\mathcal{F} \models \phi_j$ holds for all $j = 1, \ldots, i-1$. Since each sentence in a derivation is either (a) an axiom, (b) a premise or (c) the conclusion of a deductive rule, it suffices to establish $\mathcal{F} \models \phi_i$ case by case.

Clearly, $\mathcal{F} \models \phi_i$ holds by assumption if ϕ_i is a premise.

If ϕ_i is an axiom built from a propositional tautology by substitution, then it is clear by Definition 2.2 that ϕ_i is valid in *every* frame. So, $\mathcal{F} \models \phi_i$ in particular.

A similar result is easily verified for axioms of type (K): Let ψ_1, ψ_2 be arbitrary **ML** sentences and suppose that

$$\phi_i = (\Box[R](\psi_1 \rightarrow \psi_2) \rightarrow (\Box[R]\psi_1 \rightarrow \Box[R]\psi_2)).$$

Fix an arbitrary Kripke model $\mathcal{M}' = (U', \mathcal{I}', w_0')$. If either $\mathcal{M}' \not\models \Box[R](\psi_1 \rightarrow \psi_2)$ or $\mathcal{M}' \not\models \Box[R]\psi_1$, then trivially $\mathcal{M}' \models \phi_i$. If $\mathcal{M}' \models \Box[R](\psi_1 \rightarrow \psi_2)$ and $\mathcal{M}' \models \Box[R]\psi_1$, then Definition 2.2 allows us to conclude that both $(U', \mathcal{I}', w_1') \models \psi_1$ and $(U', \mathcal{I}', w_1') \models (\psi_1 \rightarrow \psi_2)$ hold for every $w_1' \in U'$ such that $(w_0', w_1') \in U'$. Consequently, we must have $(U', \mathcal{I}', w_1') \models \psi_2$ and $\mathcal{M}' \models \Box[R]\psi_2$. So, $\mathcal{M}' \models \phi_i$ holds, and since $\mathcal{M}'$ was arbitrary, $\mathcal{F} \models \phi_i$ must hold in particular.

It remains to show that the conclusion of a deductive rule is valid in $\mathcal{F}$ given that its prerequisites appear earlier in the derivation. For the modus ponens rule this is clear: Since $\mathcal{F} \models \phi_j$ and $\mathcal{F} \models (\phi_j \rightarrow \phi_i)$ by the induction hypothesis, we must have $\mathcal{F} \models \phi_i$ since we cannot have $(U, \mathcal{I}, w) \not\models \phi_j$ for any $w \in U$.

For the necessitation rule suppose that $\phi_i = \Box[R]\phi_j$. Again by the induction hypothesis $\mathcal{F} \models \phi_j$, or equivalently, $w \models \phi_j$ for all $w \in U$. This holds in particular for every R-successor state of every state, so $\mathcal{F} \models \Box[R]\phi_j$. ■

Theorem 4.7 *The presented deductive proof system for* **ML** *is strongly complete.*

Proof. Let $\Phi \subseteq \mathbf{ML}$ be a set of premises and let $\phi \in \mathbf{ML}$. We prove the contrapositive version of the claim, that is, if $\Phi \nvdash \phi$, then $\Phi \not\Vdash \phi$. In other words, from the assumption $\Phi \nvdash \phi$ we have to construct a frame $\mathcal{F}_\Phi$ in which every sentence in Φ is valid but which contains a state $w_0 \in U$ such that $w_0 \not\models \phi$. The frame $\mathcal{F}_\Phi$ will depend on Φ only, so we shall call it the *canonical frame* for Φ.

The frame is based on the syntactic notion of *consistency* with the premises Φ:

Definition 4.8 A set $\Psi \subseteq \mathbf{ML}$ is *consistent* (with Φ) if there exists no finite subset $\{\psi_1, \ldots, \psi_N\} \subseteq \Psi$ for which $\Phi \vdash \neg(\psi_1 \wedge \ldots \wedge \psi_N)$. A consistent set $\Psi \subseteq \mathbf{ML}$ is *maximal* if every proper extension $\Psi' \supset \Psi$ is inconsistent.

Note that if Φ is inconsistent with itself, then $\Phi \vdash \bot$. Since $(\bot \to \phi)$ is an axiom, $\Phi \vdash \phi$ holds trivially if Φ is inconsistent. In what follows we assume that Φ is consistent with itself. (We remark that this assumption is required by the subsequent lemmata, although this is not explicitly stated.)

The following two lemmata enable the construction of the canonical frame $\mathcal{F}_\Phi$ using maximal consistent sets. We postpone the proofs of these lemmata to the appendix so that their details do not clutter the top-level proof.

Lemma 4.9 (Lindenbaum's lemma) *Every consistent set $\Psi \subseteq \mathbf{ML}$ can be extended to a maximal consistent set.*

Lemma 4.10 *Let $\Psi \subseteq \mathbf{ML}$ be a maximal consistent set. Then $\Phi \subseteq \Psi$ and, for every $\psi \in \mathbf{ML}$, either $\psi \in \Psi$ or $\neg\psi \in \Psi$, but not both.*

We are now ready to define the canonical frame.

Definition 4.11 The *canonical frame* $\mathcal{F}_\Phi = (U, \mathcal{I})$ for Φ is defined as follows. The universe U consists of all maximally consistent extensions of Φ, that is, by Lemma 4.10

$$U \stackrel{\text{def}}{=} \{\Psi \subseteq \mathbf{ML} \ : \ \Psi \text{ is maximally consistent}\}.$$

For every $R \in \mathcal{R}$ the accessibility relation is defined by

$$\mathcal{I}(R) \stackrel{\text{def}}{=} \{(\Psi_0, \Psi_1) \in U \times U \ : \ \Psi_0^{[R]} \subseteq \Psi_1\},$$

where $\Psi^{[R]} \stackrel{\text{def}}{=} \{\psi \ : \ [R]\psi \in \Psi\}$. The truth valuation is defined for every $p \in \mathcal{P}$ by

$$\mathcal{I}(p) \stackrel{\text{def}}{=} \{\Psi \in U \ : \ p \in \Psi\}.$$

The following lemma is the hardest part of the proof since it provides the required connection between the (syntactic) maximal consistent sets and the (semantic) truth of a sentence. We again postpone the proof to the appendix.

Lemma 4.12 (Truth lemma) *For every $\psi \in \mathbf{ML}$ and every $\Psi \in U$, we have $\psi \in \Psi$ if and only if $\Psi \models \psi$.*

The top-level proof is now almost complete. Observe that we have now constructed a frame $\mathcal{F}_\Phi$ in which every sentence in Φ is valid. (To see this, note that $\Phi \subseteq \Psi$ holds for every $\Psi \in U$ by Lemma 4.10. So, every sentence in Φ is true in Ψ by Lemma 4.12.) To complete the proof we must locate a state $\Psi \in U$ such that $\Psi \not\models \phi$. Recall that we assume $\Phi \not\vdash \phi$. So, it must be that $\{\neg\phi\}$ is consistent. (Otherwise, $\Phi \vdash \neg(\neg\phi)$, which is a contradiction to the assumption $\Phi \not\vdash \phi$ since $\neg(\neg\phi) \to \phi$ is a tautology.) Let $\Psi \in U$ be an extension of $\{\neg\phi\}$ to a maximal consistent set, which exists by Lemma 4.9 and Definition 4.11. By Lemma 4.12 we have $\Psi \models \neg\phi$, so $\Psi \not\models \phi$, which completes the proof. ■

Note the ingenuity in the construction of the canonical frame. Based on the *syntax* of the logic and on the *syntactic* properties of the proof system, it is possible to construct the desired *semantic* object that allows us to refute semantic consequence between the premises in Φ and ϕ.

The following corollary demonstrates a difference between $\mathbf{ML}$ and $\mathbf{ML}_1^+$ that will become apparent in the next section. Recall that a logic is called *compact* if $\Phi \Vdash \phi$ implies that there exists a finite $\Phi' \subseteq \Phi$ such that $\Phi' \Vdash \phi$.

Corollary 4.13 (ML is compact) *Let $\Phi \subseteq \mathbf{ML}$ and suppose $\phi \in \mathbf{ML}$. If $\Phi \Vdash \phi$, then there exists a finite subset $\Phi' \subseteq \Phi$ such that $\Phi' \Vdash \phi$.*

Proof. Because the deductive proof system for $\mathbf{ML}$ is complete, $\Phi \Vdash \phi$ implies $\Phi \vdash \phi$. Since a derivation is a finite sequence, it can use only a finite number of premises from Φ. Let $\Phi' \subseteq \Phi$ be a finite set that contains these premises. Then clearly, $\Phi' \vdash \phi$. Now, $\Phi' \Vdash \phi$ follows by soundness. ■

5 Deductive proof system for $\mathbf{ML}_1^+$

In this section we modify the deductive proof system for $\mathbf{ML}$ to handle the transitive closure operator of $\mathbf{ML}_1^+$.

Using the conventions from the previous section, the deductive proof system for $\mathbf{ML}_1^+$ can be summarized as follows:

(T) (Propositional tautologies)
(K) $(\mathbb{X}(p \to q) \to (\mathbb{X}p \to \mathbb{X}q))$

(Rec)	$\mathbf{G}^*p \rightarrow (p \wedge \mathbb{X}\mathbf{G}^*p)$
(MP)	$p,\ (p \rightarrow q) \vdash q$
(N)	$p \vdash \mathbb{X}p$
(Ind)	$(p \rightarrow (q \wedge \mathbb{X}p)) \vdash (p \rightarrow \mathbf{G}^*q)$

We again allow arbitrary substitutions to the atomic propositions to occur, only this time the sentences that can be substituted are $\mathbf{ML}_1^+$ sentences instead of **ML** sentences.

Note that the proof system incorporates many parts of the **ML** proof system. In fact, only axioms of type (Rec) and the deductive rule (Ind) are new, since the operator $\mathbb{X}$ is simply an abbreviation for $[\prec]$. Axioms of type (Rec) capture the idea that a property p being true in the present state and all states "$<$"-reachable from the current state has certain local implications. In particular, p holds in the current state, and $\mathbf{G}^*p$ must hold in every "$\prec$"-successor state of the current state. The *inductive* rule (Ind) on the other hand allows us to conclude from the validity of $(p \rightarrow q \wedge \mathbb{X}p)$ that q must be true in all states "$<$"-reachable from a state in which p is true, that is, $(p \rightarrow \mathbf{G}^*q)$. We remark that this rule is somewhat nontrivial in the sense that for arbitrary relations $\mathcal{I}(\prec) \subseteq U \times U$ it is not immediately clear that such a deduction can be made. This will be demonstrated in the soundness proof.

5.1 Examples

Let us illustrate the $\mathbf{ML}_1^+$ proof system by some examples.

Example 5.1 Let ϕ be an arbitrary $\mathbf{ML}_1^+$ sentence and suppose that $\Phi = \{\phi\}$. We derive $\mathbf{G}^*\phi$ as follows:

1.	ϕ	(GP)
2.	$\mathbb{X}\phi$	(1,N)
3.	$(\phi \rightarrow (\mathbb{X}\phi \rightarrow (\phi \rightarrow (\phi \wedge \mathbb{X}\phi))))$	(T)
4.	$(\mathbb{X}\phi \rightarrow (\phi \rightarrow (\phi \wedge \mathbb{X}\phi)))$	(1,3,MP)
5.	$(\phi \rightarrow (\phi \wedge \mathbb{X}\phi))$	(2,4,MP)
6.	$\phi \rightarrow \mathbf{G}^*\phi$	(5,Ind)
7.	$\mathbf{G}^*\phi$	(1,6,MP)

Example 5.2 Let ϕ be an arbitrary $\mathbf{ML}_1^+$ sentence and suppose that $\Phi = \{\mathbf{G}^*\phi\}$. We derive $(\phi \wedge \mathbb{X}\phi \wedge \mathbb{X}\mathbb{X}\mathbf{G}^*\phi)$ as follows:

1.	$\mathbf{G}^*\phi$	(GP)
2.	$(\mathbf{G}^*\phi \rightarrow (\phi \wedge \mathbb{X}\mathbf{G}^*\phi))$	(Rec)
3.	$(\phi \wedge \mathbb{X}\mathbf{G}^*\phi)$	(1,2,MP)
4.	$((\phi \wedge \mathbb{X}\mathbf{G}^*\phi) \rightarrow \phi)$	(T)
5.	ϕ	(3,4,MP)
6.	$\mathbb{X}\phi$	(5,N)
7.	$\mathbb{X}\mathbf{G}^*\phi$	(1,N)
8.	$\mathbb{X}\mathbb{X}\mathbf{G}^*\phi$	(7,N)
9.	$(\phi \rightarrow (\mathbb{X}\phi \rightarrow (\phi \wedge \mathbb{X}\phi)))$	(T)
10.	$(\mathbb{X}\phi \rightarrow (\phi \wedge \mathbb{X}\phi))$	(5,9,MP)
11.	$(\phi \wedge \mathbb{X}\phi)$	(6,10,MP)
12.	$((\phi \wedge \mathbb{X}\phi) \rightarrow (\mathbb{X}\mathbb{X}\mathbf{G}^*\phi \rightarrow (\phi \wedge \mathbb{X}\phi \wedge \mathbb{X}\mathbb{X}\mathbf{G}^*\phi)))$	(T)
13.	$(\mathbb{X}\mathbb{X}\mathbf{G}^*\phi \rightarrow (\phi \wedge \mathbb{X}\phi \wedge \mathbb{X}\mathbb{X}\mathbf{G}^*\phi))$	(11,12,MP)
14.	$(\phi \wedge \mathbb{X}\phi \wedge \mathbb{X}\mathbb{X}\mathbf{G}^*\phi)$	(8,13,MP)

5.2 Soundness and completeness

Theorem 5.3 *The presented deductive proof system for* $\mathbf{ML}_1^+$ *is sound.*

Proof. Let $\Phi \subseteq \mathbf{ML}_1^+$ be a set of premises and let $\phi \in \mathbf{ML}_1^+$. We proceed as in Theorem 4.6 by induction on the length of the derivation. Fix a frame $\mathcal{F} = (U, \mathcal{I})$ in which all the sentences in Φ are valid. The axioms of type (Rec) and the (Ind)-rule are new, otherwise the proof is similar to Theorem 4.6.

We first prove that the (Rec) axioms $(\mathbf{G}^*\phi \rightarrow (\phi \wedge \mathbb{X}\mathbf{G}^*\phi))$ are valid in $\mathcal{F}$. Fix a Kripke model $\mathcal{M}' = (U', \mathcal{I}', w_0')$ and suppose $w_0' \models \mathbf{G}^*\phi$. (If $w_0' \not\models \mathbf{G}^*\phi$, then trivially $w_0' \models (\mathbf{G}^*\phi \rightarrow (\phi \wedge \mathbb{X}\mathbf{G}^*\phi))$.) By the semantics of $\mathbf{G}^*$ we have $w_1' \models \phi$ for every $w_1' \in U$ such that $w_0' \leq w_1'$. We must show that $w_0' \models \phi \wedge \mathbb{X}\mathbf{G}^*\phi$. Clearly $w_0' \models \phi$, so we only have to establish $w_0' \models \mathbb{X}\mathbf{G}^*\phi$. If w_0' has no successors, then we are done; otherwise select any $w_1' \in U$ such that $w_0' \prec w_1'$. Select a w_2' such that $w_1' \leq w_2'$. Since $<$ is the transitive closure of $\prec$, we have $w_0' < w_2'$. Consequently, $w_2' \models \phi$ because $w_0' \models \mathbf{G}^*\phi$. Since w_1' and w_2' were arbitrary, we must have $w_0' \models \mathbb{X}\mathbf{G}^*\phi$.

We now turn to the deductive rule (Ind). Let $\psi_1, \psi_2 \in \mathbf{ML}_1^+$. Suppose that $(\psi_1 \rightarrow (\psi_2 \wedge \mathbb{X}\psi_1))$ is valid on $\mathcal{F}$. We have to prove that $w \models (\psi_1 \rightarrow \mathbf{G}^*\psi_2)$ for all $w \in U$. Select a $w \in U$ and suppose that $w \models \psi_1$. (The case $w \not\models \psi_1$ being again trivial.) Now, select an arbitrary $w' \in U$ such that $w \leq w'$. If we can establish $w' \models \psi_2$, then clearly $w \models \mathbf{G}^*\psi_2$. The case $w = w'$ is evident

since $w \models \psi_1$ and $w \models (\psi_1 \rightarrow (\psi_2 \wedge \mathbb{X}\psi_1))$ by validity. So, suppose $w < w'$. Since $<$ is the transitive closure of $\prec$, there exists a finite sequence $w_1, \ldots, w_n \in U$ such that $w_1 = w$, $w_n = w'$, and $w_i \prec w_{i+1}$ for all $i = 1, \ldots, n-1$. Now since $(\psi_1 \rightarrow (\psi_2 \wedge \mathbb{X}\psi_1))$ is valid in $\mathcal{F}$, we must have $w_i \models (\psi_1 \rightarrow (\psi_2 \wedge \mathbb{X}\psi_1))$ for all $i = 1, \ldots, n$. Starting from the assumption $w_1 \models \psi_1$, we may now progressively conclude that $w_{i+1} \models \psi_1$ from $w_i \models \psi_1$ by using the validity of $(\psi_1 \rightarrow (\psi_2 \wedge \mathbb{X}\psi_1))$ and the fact that $w_i \prec w_{i+1}$. Thus, we must have $w_n \models \psi_1$ and hence $w_n = w' \models \psi_2$. ■

We will next address the completeness of the presented deductive proof system, and start with a seemingly unrelated observation. Namely, after introduction of transitive closure the logic is no longer compact as shown below:

Proposition 5.4 (Noncompactness of $\mathbf{ML}_1^+$) *There exists a set of premises $\Phi \subseteq \mathbf{ML}_1^+$ and a sentece $\phi \in \mathbf{ML}_1^+$ such that $\Phi \Vdash \phi$, but $\Phi' \not\Vdash \phi$ for every finite subset $\Phi' \subseteq \Phi$.*

Proof. Select any $p \neq q \in \mathcal{P}$. Put

$$\Phi = \{(p \rightarrow \mathbb{X}^n q) \ : \ n \in \mathbb{N}\}$$

and $\phi = (p \rightarrow G^* q)$. Select any frame $\mathcal{F} = (U, \mathcal{I})$ that validates all sentences in Φ. Let $w \in U$, suppose that $w \models p$ and select any $w' \in U$ such that $w \leq w'$. If $w = w'$, then trivially $w \models q$ since $(p \rightarrow q)$ is a premise. So, suppose $w < w'$. Then, there exist $w_1, \ldots, w_n \in U$ such that $w_1 = w$, $w_n = w'$ and $w_i \prec w_{i+1}$ for all $i = 1, \ldots, n-1$. Now, since $w \models (p \rightarrow \mathbb{X}^{n-1} q)$, we must have $w' \models q$ and thus $w \models \mathbf{G}^* q$. The task of constructing for every finite $\Phi' \subset \Phi$ a model that invalidates $\Phi' \Vdash \phi$ is left as an illustrative exercise for the reader. (Hint: suppose p is true only in the initial state.) ■

This noncompactness result has an important corollary in the form of nonexistence of a strongly complete and sound deductive proof system. In particular, it is no longer possible to present a *finite* derivation (which naturally uses a finite number of premises) for every sentence ϕ semantically entailed by an infinite set of premises Φ. (Suppose that this were possible. Then the noncompactness would be contradicted by the soundness theorem and the fact that a derivation uses only a finite number of premises.)

Corollary 5.5 *No sound deductive proof system for $\mathbf{ML}_1^+$ is strongly complete.*

So, the strongest form of completeness that can be achieved with a sound deductive proof system for a noncompact logic is that every sentence semantically entailed by a *finite* set of premises is derivable from these premises. This observation results in the following definition.

Definition 5.6 A proof system is *weakly complete* if $\Phi \Vdash \phi$ implies $\Phi \vdash \phi$ for every *finite* set of premises Φ.

Settling for weak completeness eases our task somewhat as the corollary of the following theorem demonstrates.

Theorem 5.7 (Deduction theorem for $\mathbf{ML}_1^+$) *Let $\phi, \psi \in \mathbf{ML}_1^+$. Then, $\psi \Vdash \phi$ if and only if $\Vdash (\mathbf{G}^* \psi \rightarrow \phi)$.*

Proof. We consider the "if"-direction first. Suppose $\Vdash (\mathbf{G}^* \psi \rightarrow \phi)$ and fix any frame $\mathcal{F} = (U, \mathcal{I})$ such that $\mathcal{F} \models \psi$. Select any $w \in U$. Obviously $w \models \mathbf{G}^* \psi$, so we must have $w \models \phi$. Since $\mathcal{F}$ and w were arbitrary, $\psi \Vdash \phi$.

The "only if"-direction is next. Suppose $\psi \Vdash \phi$. Fix any frame $\mathcal{F} = (U, \mathcal{I})$, and consider any state $w \in U$. If $w \not\models \mathbf{G}^* \psi$, then we are done. Otherwise, suppose $w \models \mathbf{G}^* \psi$. Let $U_w \stackrel{\text{def}}{=} \{w' \in U \ : \ w \leq w'\}$. Define $\mathcal{F}_w$ as the frame obtained by restricting $\mathcal{F}$ to U_w, in other words, $\mathcal{F}_w = (U_w, \mathcal{I}_w)$, where $\mathcal{I}_w(p) \stackrel{\text{def}}{=} \mathcal{I}(p) \cap U_w$ for all $p \in \mathcal{P}$ and

$$\mathcal{I}_w(\prec) \stackrel{\text{def}}{=} \mathcal{I}(\prec) \cap (U_w \times U_w),$$
$$\mathcal{I}_w(<) \stackrel{\text{def}}{=} \mathcal{I}(<) \cap (U_w \times U_w).$$

We now claim without proof (the interested reader is invited to verify this) that, for all $\psi' \in \mathbf{ML}_1^+$, $(U, \mathcal{I}, w) \models \psi'$ if and only if $(U_w, \mathcal{I}_w, w) \models \psi'$. So, in particular $(U_w, \mathcal{I}_w, w) \models G^* \psi$. By definition of U_w this implies $(U_w, \mathcal{I}_w, w') \models \psi$ for all $w' \in U_w$. Since $\psi \Vdash \phi$, we must thus have $(U_w, \mathcal{I}_w, w) \models \phi$. Consequently, $(U, \mathcal{I}, w) \models \phi$, which completes the proof since $\mathcal{F}$ and w were arbitrary. ■

Corollary 5.8 *The presented deductive proof system for $\mathbf{ML}_1^+$ is weakly complete if and only if $\Vdash \phi$ implies $\vdash \phi$.*

Proof. The "only if" direction is trivial. For the "if" direction, note that a frame validates all sentences in $\Phi = \{\psi_1, \ldots, \psi_m\} \subseteq \mathbf{ML}_1^+$ if and only if it validates their conjunction $\psi_1 \wedge \cdots \wedge \psi_m$. So, by the deduction theorem we have $\{\psi_1, \ldots, \psi_m\} \Vdash \phi$ if and only if $\Vdash (\mathbf{G}^*(\psi_1 \wedge \cdots \wedge \psi_n) \rightarrow \phi)$. The latter holds by assumption only if

$$\vdash (\mathbf{G}^*(\psi_1 \wedge \cdots \wedge \psi_n) \rightarrow \phi). \qquad (3)$$

Clearly, $\{\psi_1, \ldots, \psi_n\} \vdash \psi_1 \wedge \cdots \wedge \psi_n$, which combined with the derivation in Example 5.1 yields $\{\psi_1, \ldots, \psi_n\} \vdash \mathbf{G}^*(\psi_1 \wedge \cdots \wedge \psi_n)$. Now (3) and the (MP) rule establish the desired conclusion $\{\psi_1, \ldots, \psi_m\} \vdash \phi$. ■

Theorem 5.9 *The presented deductive proof system for* $\mathbf{ML}_1^+$ *is weakly complete.*

Proof. By Corollary 5.8 it suffices to show that $\Vdash \phi$ implies $\vdash \phi$. We shall prove the contrapositive claim $\nvdash \phi$ implies $\nVdash \phi$.

The proof is similar to that of Theorem 4.7. We first construct a canonical frame for ϕ based on syntactic notion of consistency, and then show that it contains a state in which ϕ is false.

Definition 5.10 A set $\Psi \subseteq \mathbf{ML}_1^+$ is *consistent* if there exists no finite subset $\{\psi_1, \ldots, \psi_n\} \subseteq \Psi$ such that $\vdash \neg(\psi_1 \wedge \cdots \wedge \psi_n)$.

Definition 5.11 Let $\phi \in \mathbf{ML}_1^+$. The set of *extended subformulas* of ϕ, denoted $\mathrm{ESF}(\phi)$, is the minimal set of formulas that satisfies

1. $\phi \in \mathrm{ESF}(\phi)$.
2. If $(\psi_1 \rightarrow \psi_2) \in \mathrm{ESF}(\phi)$, then $\psi_1, \psi_2 \in \mathrm{ESF}(\phi)$.
3. If $\mathbf{X}\psi \in \mathrm{ESF}(\phi)$, then $\psi \in \mathrm{ESF}(\phi)$.
4. If $\mathbf{F}^*\psi \in \mathrm{ESF}(\phi)$, then $\psi, \mathbf{XF}^*\psi \in \mathrm{ESF}(\phi)$.

It is easy to see that $\mathrm{ESF}(\phi)$ is finite for every $\phi \in \mathbf{ML}_1^+$. (A fixpoint iteration for $\mathrm{ESF}(\phi)$ is as follows. Starting from $X_0 = \{\phi\}$, iteratively expand X_n to X_{n+1} by using (1-4) for every $\psi \in X_n$. Terminate when $X_{n+1} = X_n$.)

Definition 5.12 Let $\Phi \subseteq \mathbf{ML}_1^+$. A consistent set $\Psi \subseteq \Phi$ is Φ-*maximal* if either $\psi \in \Psi$ or $\neg\psi \in \Psi$ for every $\psi \in \Phi$.

Let $\neg\mathrm{ESF}(\phi) \stackrel{\mathrm{def}}{=} \{\neg\psi \ : \ \psi \in \mathrm{ESF}(\phi)\}$.

Lemma 5.13 *Every consistent set* $\Phi \subseteq \mathrm{ESF}(\phi) \cup \neg\mathrm{ESF}(\phi)$ *can be extended to an* $\mathrm{ESF}(\phi)$*-maximal consistent set.*

The proof of this lemma is analogous to that of Lindenbaum's Lemma (Lemma 4.9); the set of premises Φ is now empty, and instead of enumerating **ML** we enumerate only the finite set $\mathrm{ESF}(\phi)$.

Definition 5.14 The *canonical frame* $\mathcal{F}_\phi = (U, \mathcal{I})$ for ϕ is defined as follows. The universe U consists of all $\mathrm{ESF}(\phi)$-maximal consistent sets. The successor relation is defined by

$$\mathcal{I}(\prec) \stackrel{\mathrm{def}}{=} \{(\Psi_0, \Psi_1) \in U \times U \ : \ \Psi_0^{\neg\mathbf{X}} \subseteq \Psi_1\},$$

where $\Psi^{\neg\mathbf{X}} \stackrel{\mathrm{def}}{=} \{\neg\psi \ : \ \neg\mathbf{X}\psi \in \Psi\}$. The interpretation of every $p \in \mathcal{P}$ is defined by

$$\mathcal{I}(p) \stackrel{\mathrm{def}}{=} \{\Psi \in U \ : : p \in \Psi\}.$$

Note that U is finite with at most $2^{|\mathrm{ESF}(\phi)|}$ elements. The following lemma is the heart of the proof, however, due to its technicality and length we postpone it to the appendix.

Lemma 5.15 (Truth lemma) *Let* $\psi \in \mathrm{ESF}(\phi)$ *and suppose* $\Psi \in U$*. Then,* $\psi \in \Psi$ *if and only if* $\mathcal{M}_\phi, \Psi \models \psi$*.*

Recall that we assume $\nvdash \phi$. So, it must be that $\{\neg\phi\}$ is consistent. (Otherwise $\vdash \neg(\neg\phi)$, that is, $\vdash \phi$.) By Lemma 5.13 we can extend $\{\neg\phi\}$ to an $\mathrm{ESF}(\phi)$-maximal consistent set $\Psi \in U$. Since Ψ is consistent, we have $\phi \notin \Psi$, which implies $\mathcal{M}_\phi, \Psi \not\models \phi$ by the truth lemma. Consequently, $\mathcal{M}_\phi \not\models \phi$. ■

The following corollary is easily extractible from the completeness proof.

Corollary 5.16 (Finite model property) *A sentence* $\phi \in \mathbf{ML}_1^+$ *is not universally valid if and only if there exists a finite model* $\mathcal{M} = (U, \mathcal{I}, w)$ *for which* $\mathcal{M} \nVdash \phi$*. Moreover,* $|U| \leq 2^{|\mathrm{ESF}(\phi)|}$*.*

Proof. The "if"-direction is trivial. The model required by the "only if"-direction is the canonical frame augmented with a state w for which $w \not\models \phi$. Such a state exists since the assumption $\nVdash \phi$ implies $\nvdash \phi$ by the soundness theorem. ■

6 Decision procedures

Now that we have shown that it is possible to characterize semantic consequence using purely syntactic tools, the next natural task is to automate the decision process for semantic consequence.

Given the discussion around deductive proof systems in the previous sections, it is natural to ask whether an algorithm could be constructed that outputs a derivation of ϕ from the premises Φ when one exists. On the other hand, if a sentence is not derivable, then the algorithm should output `false`. If the underlying proof system is sound and complete, then such an algorithm would correctly decide semantic consequence. Unfortunately, there are two major problems that make this approach inapplicable.

First, assuming that a derivation exists, how can we find one? For the **ML** and $\mathbf{ML}_1^+$ proof systems it is possible to enumerate all derivations one by one because the axioms and the deductive rules are recursively enumerable[5] (naturally, we have to assume that the premises as well are recursively enumerable). However, the enumerative approach is utterly ineffective in practice because no effective search heuristics are known (as far as the present author is aware).

Second, how is the algorithm to decide that a derivation does not exist? This is a nontrivial problem. In fact, for some logics *no such algorithm can exist*, even though they have a sound and complete proof system. These logics are called *undecidable*. First-order predicate logic is the standard example of such a logic (see e.g. [8]).

Undecidability arises easily in logic. If we allow arbitrary recursively enumerable (or recursive[6]) premise sets over a countable $\mathcal{P}$, then even propositional logic is undecidable. So, to keep matters simple and decidable, we shall restrict to finite premise sets only.

The above discussion hopefully convinced the reader that although deductive proof systems are useful as theoretical constructs, they are not particularly well-suited for automation. Practical decision algorithms are usually somewhere "in between" the semantic and syntactic interpretations of consequence. Typically the place to look for ideas for such an algorithm is the completeness proof.

Recall Corollary 5.16 of the $\mathbf{ML}_1^+$ completeness proof from the previous section. Informally, it states that a sentence is not universally valid precisely when there exists a finite model (whose size can be upper-bounded by the structure of the sentence) that demonstrates this. But this is just what is required to produce a decision algorithm. Namely, we can easily design an algorithm that exhaustively searches through all Kripke models[7] up to the size bound, and decides according to whether the falsifying model was found. By Corollary 5.8 this algorithm is sufficient to decide $\mathbf{ML}_1^+$ with finite sets of premises. Because of noncompactness, this is in a sense the best we can hope for $\mathbf{ML}_1^+$.

Not surprisingly, a similar decision algorithm works for **ML** and finite sets of premises. Such an algorithm is the topic of the next subsection.

6.1 Decision procedure for ML

In this section we present a procedure that allows us to decide whether $\Phi \Vdash \phi$ for finite premise sets $\Phi \subseteq \mathbf{ML}$. The procedure decides satisfiability of ϕ subject to the premises Φ by attempting to construct a model for ϕ in which the premises are true in every state. This can then be applied to settle semantic consequence since $\Phi \Vdash \neg\phi$ holds if and only if ϕ is unsatisfiable subject to the premises Φ.

The algorithm proceeds top-down. Starting from a large frame that is guaranteed to contain a satisfying model (if one exists), the algorithm deletes from the frame states and arcs that cannot contribute to a satisfying model. When no further deletions can be performed, the algorithm checks whether the frame contains a state in which ϕ is true, and returns accordingly either "satisfiable" or "unsatisfiable."

The states in the initial frame consist of all propositionally consistent sets.

Definition 6.1 Denote by SF the set of all subformulas of the sentences in $\Phi \cup \{\phi\}$. A subset $w \subseteq$ SF is *propositionally consistent* if

[5] A set is *recursively enumerable* if there exists an algorithm that outputs every element of the set at least once.

[6] A set is *recursive* if there exists an algorithm that outputs `yes` if its input is a member of the set and `no` if it is not.

[7] We naturally have to restrict the set of atomic propositions to those that occur in ϕ.

1. $\bot \notin w$; and
2. if $(\psi_1 \to \psi_2) \in \mathrm{SF}$, then $(\psi_1 \to \psi_2) \in w$ if and only if $\psi_1 \notin w$ or $\psi_2 \in w$.

A sentence $\psi \in \mathrm{SF}$ is a *modal formula* if it is of the form $\psi = \langle R\rangle\psi_1$ or $\psi = [R]\psi_1$ for some $R \in \mathcal{R}$ and $\psi_1 \in \mathrm{SF}$.

Example 6.2 Let $\Phi \cup \{\phi\} = \{\langle R\rangle(\langle R\rangle p \to q)\}$. Then

$$\mathrm{SF} = \{\langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q),\ \langle R\rangle p,\ p,\ q\}.$$

The modal formulas in SF are $\langle R\rangle(\langle R\rangle p \to q)$ and $\langle R\rangle p$. The propositionally consistent subsets of SF are

1. $\{p,\ q,\ \langle R\rangle p,\ \langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
2. $\{p,\ q,\ \langle R\rangle p,\ (\langle R\rangle p \to q)\}$
3. $\{p,\ q,\ \langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
4. $\{p,\ q,\ (\langle R\rangle p \to q)\}$
5. $\{p,\ \langle R\rangle p,\ \langle R\rangle(\langle R\rangle p \to q)\}$
6. $\{p,\ \langle R\rangle p\}$
7. $\{p,\ \langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
8. $\{p,\ (\langle R\rangle p \to q)\}$
9. $\{q,\ \langle R\rangle p,\ \langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
10. $\{q,\ \langle R\rangle p,\ (\langle R\rangle p \to q)\}$
11. $\{q,\ \langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
12. $\{q,\ ,(\langle R\rangle p \to q)\}$
13. $\{\langle R\rangle p,\ \langle R\rangle(\langle R\rangle p \to q)\}$
14. $\{\langle R\rangle p\}$
15. $\{\langle R\rangle(\langle R\rangle p \to q),\ (\langle R\rangle p \to q)\}$
16. $\{(\langle R\rangle p \to q)\}$

Observe that all $2^4 = 16$ combinations of the modal formulas $\{\langle R\rangle(\langle R\rangle p \to q),\ \langle R\rangle p\}$ and the atomic propositions $\{p,\ q\}$ occur in the propositionally consistent sets.

Propositionally consistent sets are "consistent for propositional logic" in the sense that once the modal formulas and the atomic propositions that appear in a propositionally consistent set are fixed, then the other formulas in the set are uniquely determined. Namely, a propositionally consistent set $w \subseteq \mathrm{SF}$ consists of precisely the sentences in SF that are true in a Kripke model that satisfies

1. for every atomic proposition $p \in \mathrm{SF}$, $w \in \mathcal{I}(p)$ if and only if $p \in w$; and
2. for every modal formula $\psi \in \mathrm{SF}$, $w \models \psi$ if and only if $\psi \in w$.

(In some cases such a Kripke model may not exist because the modal formulas specify constraints that are impossible to meet in a model, e.g. $\{\langle R\rangle p, \neg\langle R\rangle p\}$.)

The following is a step by step description of the algorithm:

1. Construct the set SF of subformulas of $\Phi \cup \{\phi\}$.
2. Let
$$U = \{w \subseteq \mathrm{SF} \ :\ w \text{ is p. consist. and } \Phi \subseteq w\}.$$
3. Put $\mathcal{I}(R) = U \times U$ for every $R \in \mathcal{R}$ that appears in SF.
4. (Put $\mathcal{I}(p) = \{w \in U \ :\ p \in w\}$ for every $p \in \mathcal{P}$ that appears in SF.)
5. Delete bad states and arcs from $(U, \mathcal{I})$ until none exist.
   - A *state* $w \in U$ *is bad* if there exists a $\langle R\rangle\psi \in \mathrm{SF}$ such that $\langle R\rangle\psi \in w$, but for every $(w, w') \in \mathcal{I}(R)$ it holds that $\psi \notin w'$.
   - An *arc* $(w, w') \in \mathcal{I}(R)$ *is bad* if there exists a $\langle R\rangle\psi \in \mathrm{SF}$ such that $\langle R\rangle\psi \notin w$ but $\psi \in w'$.
6. If the resulting frame $(U, \mathcal{I})$ contains a state w with $\phi \in w$, then output "satisfiable"; otherwise output "unsatisfiable."

Step 4 is not necessary for correct operation of the algorithm. We include it since it completes the partial structure $(U, \mathcal{I})$ to a satisfying frame. The following theorem demonstrates the correctness of the algorithm.

Theorem 6.3 *Let $\Phi \subseteq$ **ML** be a finite set and suppose $\phi \in$ **ML**. Then, the presented* **ML** *decision procedure outputs "satisfiable" on input Φ, ϕ if and only if there exists a frame $\mathcal{F} = (U, \mathcal{I})$ with (a) $\mathcal{F} \models \Phi$; and (b) there exists a $w_0 \in U$ such that $(U, \mathcal{I}, w_0) \models \phi$.*

Proof. We start with the "only if" direction. Suppose that $\mathcal{F} = (U, \mathcal{I})$ is the frame that remains after all the deletions have been performed, and let $w_0 \in U$ be a state that satisfies $\phi \in w_0$. (Such

a state exists since the algorithm outputs "satisfiable.") It can now be shown by induction that $\mathcal{F}$ satisfies

$$w \models \psi \text{ if and only if } \psi \in w, \tag{4}$$

for every $\psi \in$ SF. The atomic propositions in SF form the base case, which holds by assumption (that is, Step 4 in the algorithm description). Since every $w \in U$ is propostitionally consistent, the claim must also hold for sentences of the form $(\psi_1 \rightarrow \psi_2) \in$ SF. We analyze the modal formulas in more detail. Fix $\langle R\rangle\psi \in$ SF and suppose $w \models \langle R\rangle\psi$. Then there exists a $w' \in U$ such that $w' \models \psi$. By the induction hypothesis we thus have $\psi \in w'$. So, $\langle R\rangle\psi \in w$, because otherwise the arc $(w, w') \in \mathcal{I}(R)$ would be bad, which is impossible since all bad arcs are deleted from $\mathcal{F}$. For the other direction, suppose $\langle R\rangle\psi \in w$. Then there must exist a $w' \in U$ such that $(w, w') \in \mathcal{I}(R)$ and $\psi \in w'$, because otherwise the state w would be bad, which is impossible. We conclude $w' \models \psi$ by the induction hypothesis, so $w \models \langle R\rangle\psi$. The frame $\mathcal{F}$ now satisfies $\mathcal{F} \models \Phi$ since $\Phi \subseteq w$ for every $w \in U$ by construction. Furthermore, (4) implies $w_0 \models \phi$.

Next is the "if" direction. Let $\mathcal{F} = (U, \mathcal{I})$ be the frame that satisfies $\mathcal{F} \models \Phi$ and $(U, \mathcal{I}, w_0) \models \phi$. Select any $w \in U$, and define

$$w^{\equiv} \stackrel{\text{def}}{=} \{\psi \in \text{SF} \ : \ w \models \psi\},$$

that is, $w^{\equiv}$ consists of the sentences in SF that are true in w. The set $w^{\equiv}$ is propositionally consistent by construction. Now define $\mathcal{I}^{\equiv}$ by setting

$$\mathcal{I}^{\equiv}(p) \stackrel{\text{def}}{=} \{w^{\equiv} \ : \ p \in w^{\equiv}\},$$
$$\mathcal{I}^{\equiv}(R) \stackrel{\text{def}}{=} \{(w^{\equiv}, w'^{\equiv}) \ : \ (w, w') \in \mathcal{I}(R)\}$$

for all atomic propositions $p \in$ SF. The interpretations of the atomic propositions $p \in$ SF agree with the initial frame in the decision procedure. Moreover, $\Phi \subseteq w^{\equiv}$ for all $w \in U$. Thus, the frame $\mathcal{F}^{\equiv} \stackrel{\text{def}}{=} (U^{\equiv}, \mathcal{I}^{\equiv})$ is a subframe of the initial frame in the decision procedure. Furthermore, it is easy to verify that $\mathcal{F}^{\equiv}$ contains no bad states nor arcs. Therefore, $\mathcal{F}^{\equiv}$ is a subframe of the frame that results when all bad states and arcs are deleted from the initial frame built from input Φ, ϕ. Because $\phi \in w_0^{\equiv}$, the decision procedure will output "satisfiable." ■

6.2 Decision procedure for $\mathbf{ML}_1^+$

The decision procedure for **ML** from the previous section admits straightforward extension to the transitive closure operator of $\mathbf{ML}_1^+$. There are two modifications. First, instead of the subformulas SF of $\Phi \cup \{\phi\}$ we consider the extended subformulas ESF of $\Phi \cup \{\phi\}$. (Recall from Definition 5.11 that $\mathbf{XF}^*\psi$ is an extended subformula of $\mathbf{F}^*\psi$.)

Example 6.4 Let

$$\Phi \cup \{\phi\} = \{((p \vee \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p)\}.$$

Expanding the syntactic abbreviations, we obtain

$$\Phi \cup \{\phi\} = \{(((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p)\}.$$

The extended subformulas of $\Phi \cup \{\phi\}$ are:

$$\begin{aligned}\text{ESF} = \{&p,\ \mathbf{XF}^*p,\ \mathbf{F}^*p,\ \bot,\\ &(p \rightarrow \bot),\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\\ &(((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p)\}\end{aligned}$$

The propositionally consistent subsets of ESF are:

1. $\{\ (((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p),\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ (p \rightarrow \bot),\ \mathbf{XF}^*p,\ \mathbf{F}^*p\ \},$
2. $\{\ (((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p),\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ p,\ \mathbf{XF}^*p,\ \mathbf{F}^*p\ \},$
3. $\{\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ (p \rightarrow \bot),\ \mathbf{XF}^*p\ \},$
4. $\{\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ p,\ \mathbf{XF}^*p\ \},$
5. $\{\ (((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p),\ (p \rightarrow \bot),\ \mathbf{F}^*p\ \},$
6. $\{\ (((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p),\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ p,\ \mathbf{F}^*p\ \},$
7. $\{\ (((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p) \rightarrow \mathbf{F}^*p),\ (p \rightarrow \bot)\ \},$
8. $\{\ ((p \rightarrow \bot) \rightarrow \mathbf{XF}^*p),\ p\ \}.$

The second change is that the rules that determine which states and arcs are bad have to be modified to take into account the transitive closure operator $\mathbf{F}^*$. More specifically:

- An *arc* $(w, w') \in \mathcal{I}(\prec)$ *is bad* if
  1. $\mathbf{X}\psi \notin w$ but $\psi \in w'$; or

2. $\mathbf{F}^*\psi \notin w$ but $\mathbf{F}^*\psi \in w'$.

- A *state* $w \in U$ *is bad* if

1. $\mathbf{X}\psi \in w$ but $\psi \notin w'$ for all $w' \in U$ such that $(w, w') \in \mathcal{I}(\prec)$; or
2. $\mathbf{F}^*\psi \notin w$ but $\psi \in w$; or
3. $\mathbf{F}^*\psi \in w$ but $\psi \notin w$ and $\psi \notin w'$ for every $w' \in U$ such that $(w, w') \in \mathcal{I}(\prec)^+$.

For the correctness proof of the algorithm (and an extension to **CTL**) we follow [1] and point the reader to [4, 5].

6.3 Decision procedures for natural models

The decision procedures for **ML** and $\mathbf{ML}_1^+$ presented in the two previous subsections decide satisfiability with respect to the class of all Kripke models. There is a drawback in such generality, namely the algorithms require exponential time *and space* with respect to the number of distinct atomic propositions and modal formulas in (E)SF (cf. Examples 6.2 and 6.4). What is even worse, the space requirement is *always* exponential, even though the frame that results after all deletions have been performed might be small in comparison.

There are at least two ways to alleviate the space and time requirements of the decision algorithms.

The first approach is to perform the search bottom-up instead of top-down. That is, instead of starting from the large frame and deleting unnecessary states and arcs, we start from an empty frame and attempt to complete it to a satisfying model by addition of states and arcs. Although the worst-case behaviour may still be exponential, this need not always be the case. The problem with the bottom-up approach for arbitrary models is that it is hard to determine which states should be added to the frame, and in particular how the accessibility relation(s) should be updated to produce a satisfying model in the end.

The second approach is to restrict the class of models considered. For example, linear time logics operate on the class of natural models, which are sequences of states.

Definition 6.5 A Kripke model $\mathcal{M} = (U, \mathcal{I}, w_0)$ for $\mathbf{ML}_1^+$ is a *natural model* if

(i) for each state $w \in U$ there exists at most one $w' \in U$ such that $w \prec w'$; and

(ii) for each state $w \in U$ there exists at most one $w' \in U$ such that $w' \prec w$; and

(iii) there exists no $w' \in U$ such that $w' \prec w_0$.

(iv) for every distinct $w, w' \in U$, either $w < w'$ or $w' < w$.

(Observe that restricting to natural models also forces us to restrict to monomodal logic.) Restricting to natural models immediately reduces the number of arcs that need to be stored and manipulated from quadratic to linear in the number of states (which is in general exponential in the size of the input formula). In fact, no arcs need to be explicitly stored since a sequence of states implicitly encodes the successor relation for natural models: the next state in the sequence is the successor state of the present state. This property makes deciding satisfiability with respect to natural models well-suited for a bottom-up backtrack search implementation.

To illustrate such an algorithm, we consider for simplicity the fragment of $\mathbf{ML}_1^+$ that does not contain the transitive closure operator $\mathbf{F}^*$, that is, $\mathbf{X}$ and its dual $\mathbb{X}$ are the only modal operators allowed.

Let Φ be a set of premises and let ϕ be the sentence whose satisfiability is to be decided with respect to Φ and natural models.

The decision algorithm is a two-stage backtrack search. The first stage considers all possibilities for the initial state w_0, that is, all propositionally consistent sets $w_0 \subseteq \mathrm{SF}$ that satisfy (a) $\Phi \subseteq w_0$ and (b) $\phi \in w_0$. The second stage attempts to complete the initial state w_0 to a natural model by recursively extending the input state w_i to a successor state w_{i+1} so that all *future obligations* in the input state are met. These are:

1. *Positive future obligations*: $\psi \in w_{i+1}$ for all sentences $\mathbf{X}\psi \in w_i$.
2. *Negative future obligations*: $\psi \notin w_{i+1}$ for all sentences $\neg\mathbf{X}\psi \in w_i$.
3. *Premises*: $\Phi \subseteq w_{i+1}$.
4. *Consistency*: w_{i+1} must be propositionally consistent.

If for input w_i the obligations cannot be met, then the algorithm backtracks from level $i+1$ to level i and considers the next possible w_i. There are two successful termination conditions. The first is that the input w_i contains no future obligations. Then the sequence $(w_0, \ldots, w_i)$ is a satisfying model if we put $\mathcal{I}(p) = \{w_i \ : \ p \in w_i\}$ for all atomic propositions $p \in \mathrm{SF}$. The second condition occurs when the constructed w_{i+1} satisfies $w_j = w_{i+1}$ for some $j \leq i$. Then the infinite sequence

$$(w_0, \ldots, w_{j-1}) \circ (w_j, \ldots, w_i)^\omega$$

is a satisfying model.

The algorithm terminates always because the number of propostionally consistent subsets of SF is finite. Thus, either a successful termination condition is reached at some point of the search, or the algorithm terminates unsuccessfully because all propositionally consistent initial states were considered, and no satisfying extension to a natural model was found.

7 Tableau methods for natural models

Tableau methods provide an alternative decision method for modal logics [6] and temporal logics [9].

In this section we sketch a tableau-based decision procedure for $\mathbf{ML}_1^+$ and natural models. The treatment is rather succinct; we refer the reader unfamiliar with tableau methods in logic to standard textbooks on computational logic (e.g. [2, 7]).

Definition 7.1 An $\mathbf{ML}_1^+$-*tableau* is a rooted tree whose nodes are subsets of $\mathbf{ML}_1^+$ sentences; each of the sentences is prefixed either with the symbol T or the symbol F.[8] The root node of a tableau may be arbitrary, but it is required that the children of each node (if any) are constructed according to the tableau rules given below.

The tableau rules are as follows. A sentence of the form $(\psi_1 \to \psi_2)$ is expanded using the rules

$$\frac{\Gamma,\ \mathsf{T}(\psi_1 \to \psi_2)}{\Gamma,\ \mathsf{F}\psi_1 \quad | \quad \Gamma,\ \mathsf{T}\psi_2}, \qquad \frac{\Gamma,\ \mathsf{F}(\psi_1 \to \psi_2)}{\Gamma,\ \mathsf{T}\psi_1,\ \mathsf{F}\psi_2}. \tag{5}$$

The sentences above the horizontal line indicate the content of the parent node, and the sentences below the horizontal line indicate the sentences in the child node(s). A vertical bar "|" separates multiple child nodes. The symbol Γ denotes all the other prefixed sentences in the particular tableau node.

Contradictory nodes are closed by the following rules. The symbol "$*$" indicates that the tableau node is *closed* and cannot be expanded further.

$$\frac{\Gamma,\ \mathsf{F}\psi,\ \mathsf{T}\psi}{*}, \qquad \frac{\Gamma,\ \mathsf{T}\bot}{*}, \qquad \frac{\Gamma,\ \mathsf{F}\bot}{\Gamma} \tag{6}$$

A sentence of the form $\mathbf{F}^*\psi$ is expanded using the rules:

$$\frac{\Gamma,\ \mathsf{T}\mathbf{F}^*\psi}{\Gamma,\ \mathsf{T}\psi \quad | \quad \Gamma,\ \mathsf{T}\mathbf{X}\mathbf{F}^*\psi}, \qquad \frac{\Gamma,\ \mathsf{F}\mathbf{F}^*\psi}{\Gamma,\ \mathsf{F}\psi\ \mathsf{F}\mathbf{X}\mathbf{F}^*\psi} \tag{7}$$

All sentences of the form $\mathbf{X}\psi$ are expanded at once using the rules

$$\frac{\Gamma,\ \mathsf{T}\mathbf{X}\varphi_1, \ldots, \mathsf{T}\mathbf{X}\varphi_n,\ \mathsf{F}\mathbf{X}\psi_1, \ldots, \mathsf{F}\mathbf{X}\psi_m}{\mathsf{T}\Phi,\ \mathsf{T}\varphi_1, \ldots, \mathsf{T}\varphi_n,\ \mathsf{F}\psi_1, \ldots, \mathsf{F}\psi_m} \tag{8}$$

and

$$\frac{\Gamma}{\quad}, \tag{9}$$

where Φ is the set of global premises (each of which prefixed with the symbol T). If rule (9) is applied, then the node is *open* and cannot be expanded further.

The applicability of rules (8) and (9) is restricted as follows:

- Rules (8) and (9) are applicable only if none of the rules (5)–(7) can be applied. For example, if a node contains the sentence $\mathsf{F}(\psi_1 \to \psi_2)$, then neither (8) nor (9) is applicable since rule (5) is applicable.
- If the above condition holds, then rule (8) is applicable only if the parent node contains a sentence of the form $\mathsf{T}\mathbf{X}\varphi$; otherwise rule (9) **must** be applied.
- When rule (8) is applied, it is required that Γ contains no sentences of the form $\mathsf{T}\mathbf{X}\varphi$ or $\mathsf{F}\mathbf{X}\psi$.

[8] Intuitively, the prefixes T and F indicate that the sentence is forced to be true or false, respectively, in the present node. The tableau rules take care of propositional consistency and consistency of modal formulas between states. (E.g. rule (8) enforces the future obligations; recall the previous section.)

Definition 7.2 A tableau node is *looping* if it (a) has no children and (b) is a subset of a node that occurs on the path to the root node (that includes the root node). A tableau is *completed* if every leaf node is either closed, open, or looping.

A *loop graph* of a completed tableau is a directed graph that results if the looping nodes are identified with a node that induces the looping condition. A strongly connected component (SCC) in the loop graph is *self-fulfilling* if for every sentence $\mathsf{T}\mathbf{F}^*\psi$ that occurs in a node of the SCC there exists a node in the SCC that contains the sentence $\mathsf{T}\psi$.

Definition 7.3 A completed tableau is *successful* if (a) it contains an open leaf node or (b) there exists a looping node whose SCC is self-fulfilling in a loop graph of the tableau.

We state the following correctness theorem without proof.

Theorem 7.4 *Let $\Phi \subseteq \mathbf{ML}_1^+$ be a finite set of premises and suppose $\phi \in \mathbf{ML}_1^+$. Then, ϕ is satisfiable subject to the premises Φ in the class of natural models if and only if there exists a successful tableau whose root node is $\mathsf{T}\Phi \cup \{\mathsf{T}\phi\}$. (Moreover, if there exists a successful tableau, then every completed tableau is successful.)*

References

[1] E. Clarke and B.-H. Schlingloff. Model Checking. Chapter 24 in Volume 2 of *Handbook of Automated Reasoning* (A. Robinson and A. Voronkov, eds.), pages 1689–1711, Elsevier Science Publishers, 2001.

[2] M. Ben-Ari. *Mathematical Logic for Computer Science*, 2nd Edition. Springer-Verlag, London, 2000.

[3] P. Blackburn, M. de Rijke and Y. Venema. *Modal Logic*. Cambridge University Press, Cambridge, England, 2001.

[4] E. A. Emerson and A. P. Sistla. Deciding full branching time logic. *Inform. and Control* **61** (1984) no. 3, 175–201.

[5] E. A. Emerson. Temporal and modal logic. Chapter 16 in Volume B of *Handbook of Theoretical Computer Science* (J. van Leeuwen, ed.), pages 997–1072, Elsevier Science Publishers, 1990.

[6] M. Fitting. *Proof Methods for Modal and Intuitionistic Logics*. D. Reidel Publishing Co., Boston, Massachusetts, 1983.

[7] A. Nerode and R. A. Shore. *Logic for Applications*, 2nd Edition. Springer-Verlag, New York, 1997.

[8] C. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, Massachusetts, 1994.

[9] P. Wolper, The tableau method for temporal logic: An overview. *Logique et Anal. (N.S.)* **28** (1985) no. 110-111, 119–136.

A Appendix

This appendix contains proofs of the lemmata stated but not proven in the main text.

A.1 Proof of Lemma 4.9

Recall that we assumed that the sets $\mathcal{P}$ and $\mathcal{R}$ are at most countable. Consequently, the set $\mathbf{ML}$ is countable. Fix an enumeration $\phi_1, \phi_2, \phi_3, \ldots$ of $\mathbf{ML}$ and define, for all $i = 1, 2, \ldots$,

$$\Delta_1 \stackrel{\text{def}}{=} \Psi,$$

$$\Delta_{i+1} \stackrel{\text{def}}{=} \begin{cases} \Delta_i \cup \{\phi_i\} & \text{if } \Delta_i \cup \{\phi_i\} \text{ is consitent;} \\ \Delta_i \cup \{\neg\phi_i\} & \text{otherwise,} \end{cases}$$

$$\Delta \stackrel{\text{def}}{=} \bigcup_{i=1}^{\infty} \Delta_i.$$

We will show that Δ is a maximally consistent set if Ψ is consistent. First, we establish by induction that every Δ_i is consistent. The base case $i = 1$ is true by assumption. For the inductive step, suppose that Δ_i is consistent. If Δ_{i+1} is inconsistent, then $\Delta_i \cup \{\phi_i\}$ is inconsistent and $\Delta_{i+1} = \Delta_i \cup \{\neg\phi_i\}$. Since Δ_i is consistent, we have both $\Phi \vdash \neg(\phi_1^+ \wedge \cdots \wedge \phi_{n^+}^+ \wedge \phi_i)$ and $\Phi \vdash \neg(\phi_1^- \wedge \cdots \wedge \phi_{n^-}^- \wedge \neg\phi_i)$,

where $\{\phi_1^+, \ldots, \phi_{n^+}^+, \phi_1^-, \ldots, \phi_{n^-}^-\} \subseteq \Delta_i$. By combining the two derivations we obtain

$$\Phi \vdash \neg(\phi_1^+ \wedge \cdots \wedge \phi_{n^+}^+ \wedge \phi_1^- \wedge \cdots \wedge \phi_{n^-}^-)$$

and hence Δ_i is inconsistent contrary to our assumption. Thus, Δ_{i+1} must be consistent.

The union Δ is consistent since every finite subset of Δ is a finite subset of some Δ_i, which is consistent. To see that Δ is maximal, suppose that $\Delta \cup \{\phi_k\}$ is consistent. Then, since every subset of a consistent set is consistent, we have that $\Delta_k \cup \{\phi_k\} \subseteq \Delta \cup \{\phi_k\}$ is consistent. Thus, $\Delta_{k+1} = \Delta_k \cup \{\phi_k\}$ by definition. Consequently, $\phi_k \in \Delta_{k+1} \subseteq \Delta$.

A.2 Proof of Lemma 4.10

Fix a maximal consistent set $\Psi \subseteq \mathbf{ML}$. Suppose that $\psi \in \Phi$ but $\psi \notin \Psi$. Then $\Psi \cup \{\psi\}$ is inconsistent and $\Phi \vdash \neg(\psi_1 \wedge \cdots \wedge \psi_n \wedge \psi)$ for some $\{\psi_1, \ldots, \psi_n\} \subseteq \Psi$. But since $\psi \in \Phi$, we have $\Phi \vdash \neg(\psi_1 \wedge \cdots \wedge \psi_n)$, which is a contradiction since Ψ is consistent.

Suppose that both $\psi, \neg\psi \notin \Psi$. Then, by maximality of Ψ, both $\Psi \cup \{\psi\}$ and $\Psi \cup \{\neg\psi\}$ are inconsistent. Consequently, we have both $\Phi \vdash \neg(\psi_1^+ \wedge \cdots \wedge \psi_{n^+}^+ \wedge \psi)$ and $\Phi \vdash \neg(\psi_1^- \wedge \cdots \wedge \psi_{n^-}^- \wedge \neg\psi)$, where $\{\psi_1^+, \ldots, \psi_{n^+}^+\}, \{, \psi_1^-, \ldots, \psi_{n^-}^-\} \subseteq \Psi$ By combining the two derivations we obtain

$$\Phi \vdash \neg(\psi_1^+ \wedge \cdots \wedge \psi_{n^+}^+ \wedge \psi_1^- \wedge \cdots \wedge \psi_{n^-}^-),$$

which is a contradiction to the assumption that Ψ was consistent. On the other hand, $\psi, \neg\psi \in \Psi$ is also impossible since $\neg(\psi \wedge \neg\psi)$ is a propositional tautology.

A.3 A technical lemma

The following lemma facilitating the consistent extension of a set is required in the proof of Lemma 4.12.

Lemma A.1 *Let $\Psi \subseteq \mathbf{ML}$ be a consistent set, and suppose that $R \in \mathcal{R}$ and $\neg[R]\phi \in \Psi$. Then, the set $\Psi^{[R]} \cup \{\neg\phi\}$ is consistent.*

Proof. Let $\Psi \subseteq \mathbf{ML}$ be a consistent set, and let $R \in \mathcal{R}$ and $\neg[R]\phi \in \Psi$. Suppose that $\Psi^{[R]} \cup \{\neg\phi\}$ is inconsistent. Then $\Phi \vdash \neg(\psi_1 \wedge \cdots \wedge \psi_n)$ for some $\{\psi_1, \ldots, \psi_n\} \subseteq \Psi^{[R]} \cup \{\neg\phi\}$. Without loss of generality we may assume $\Phi \vdash \neg(\psi_1 \wedge \cdots \wedge \psi_n \wedge \neg\phi)$ since $\neg A \to \neg(A \wedge B)$ is a propositional tautology. Continuing the derivation, we obtain

1. $\neg(\psi_1 \wedge \cdots \wedge \psi_n \wedge \neg\phi)$
2. $\psi_1 \wedge \cdots \wedge \psi_n \to \phi$ (1,T,MP)
3. $[R]\psi_1 \wedge \cdots \wedge [R]\psi_n \to [R]\phi$ (2,GR)
4. $\neg([R]\psi_1 \wedge \cdots \wedge [R]\psi_n \wedge \neg[R]\phi)$ (4,T,MP),

which is a contradiction since Ψ is consistent. ■

A.4 Proof of Lemma 4.12

Fix $\psi \in \mathbf{ML}$ and a maximal consistent set $\Psi \in U$. We proceed by induction in the structure of ψ.

First, $\bot \notin \Psi$ because otherwise Ψ would be inconsistent as $\dashv\bot$ is a propositional tautology. For the other base case, let $\psi = p \in \mathcal{P}$. Then by Definition 4.11, $\mathcal{M}_\Phi, \Psi \models p$ if and only if $p \in \Psi$.

Let $\psi = (\psi_1 \to \psi_2)$. By the induction hypothesis we have to establish that $(\psi_1 \to \psi_2) \notin \Psi$ if and only if $\psi_1 \in \Psi$ and $\psi_2 \notin \Psi$. We prove first the "only if" direction. Suppose $(\psi_1 \to \psi_2) \notin \Psi$. By Lemma 4.10 we then have $\psi_1 \wedge \neg\psi_2 \in \Psi$. But then both $\neg\psi_1 \in \Psi$ and $\psi_2 \in \Psi$ are impossible since $\neg(\psi_1 \wedge \neg\psi_2 \wedge \neg\psi_1)$ and $\neg(\psi_1 \wedge \neg\psi_2 \wedge \psi_2)$ are prositional tautologies (and hence, Ψ would be inconsistent if either of the sentences $\neg\psi_1$, ψ_2 were in Ψ). So, we must have $\psi_1 \in \Psi$ and $\psi_2 \notin \Psi$ by Lemma 4.10. The "if" direction follows similarly using Lemma 4.10 and the observation that $\neg(\psi_1 \wedge \neg\psi_2 \wedge (\psi_1 \to \psi_2))$ is a propositional tautology.

We prove the $\psi = \langle R\rangle\psi_1$ case using the dual operator $[R]$ and $\psi = [R]\psi_1$. (Then the $\psi = \langle R\rangle\psi_1$ case follows from $\langle R\rangle\psi_1 = (([R]\psi_1) \to \bot) \to \bot$ and the induction hypothesis.) We first prove the "only if" direction. Suppose $[R]\psi_1 \in \Psi$. For every $\Psi_1 \in U$ such that $(\Psi, \Psi_1) \in \mathcal{I}(R)$ we have $\Psi^{[R]} \subseteq \Psi_1$ by Definition 4.11. Thus, $\psi_1 \in \Psi_1$, and $\mathcal{M}_\phi, \Psi_1 \models \psi_1$ by the induction hypothesis. Since Ψ_1 was arbitrary, $\mathcal{M}_\phi, \Psi \models [R]\psi_1$. We prove the "if" direction using the contrapositive form $[R]\psi_1 \notin \Psi$ implies $\mathcal{M}_\Phi, \Psi \not\models [R]\psi_1$. Suppose $[R]\psi_1 \notin \Psi$. Then, by Lemma 4.10 $\neg[R]\psi_1 \in \Psi$. Consequently, Lemma A.1 applies, and the set $\Psi^{[R]} \cup \{\neg\psi_1\}$ is consistent. Let Ψ_1 be a maximal consistent extension of $\Psi^{[R]} \cup \{\neg\psi_1\}$. By Definition 4.11 we have $\Psi_1 \in U$ and $(\Psi, \Psi_1) \in \mathcal{I}(R)$. Furthermore, since $\neg\psi_1 \in \Psi_1$, we have by Lemma 4.10 and the induction hypothesis $\mathcal{M}_\Phi, \Psi_1 \not\models \psi_1$. Consequently, $\mathcal{M}_\Phi, \Psi \not\models [R]\psi_1$.

A.5 Proof of Lemma 5.15

Fix an ESF(ϕ)-maximal consistent set $\Psi \in U$ and let $\psi \in \mathrm{ESF}(\phi)$. We proceed by induction on the structure of ψ.

The proofs of the base cases and the case $\psi = (\psi_1 \to \psi_2)$ are similar to the proof of Lemma 4.12. (Note that the "either-or" conclusion of Lemma 4.10 is built into Definition 5.12.)

Suppose that $\psi = \mathbf{X}\psi_1 \in \mathrm{ESF}(\phi)$. We have to show that $\mathbf{X}\phi_1 \in \Psi$ if and only if $\mathcal{M}_\phi, \Psi \models \mathbf{X}\psi_1$. We prove the "if" direction first. Suppose that $\mathcal{M}_\phi, \Psi \models \mathbf{X}\psi_1$. Then there exists a $\Psi_1 \in U$ such that $\Psi \prec \Psi_1$ and $\mathcal{M}_\phi, \Psi_1 \models \psi_1$. Clearly, $\psi_1 \in \mathrm{ESF}(\phi)$, so we thus have $\psi_1 \in \Psi_1$ by the induction hypothesis. To reach a contradiction, suppose that $\mathbf{X}\psi_1 \notin \Psi$. Then $\neg\mathbf{X}\psi_1 \in \Psi$ by maximality of Ψ. By definition of $\mathcal{I}(\prec)$ we thus have $\neg\psi_1 \in \Psi_1$, which is a contradiction. In the "only if" direction, suppose that $\mathbf{X}\psi_1 \in \Psi$. We have to locate a $\Psi_1 \in U$ such that $\Psi \prec \Psi_1$ and $\mathcal{M}_\phi, \Psi_1 \models \psi_1$. Let $Z \stackrel{\text{def}}{=} \{\psi_1\} \cup \{\neg\xi \ : \ \neg X\xi \in \Psi\}$, removing double negations if necessary so that each $\neg\xi \in \mathrm{ESF}(\phi) \cup \neg\mathrm{ESF}(\phi)$. With the aim of applying Lemma 5.13 to extend Z to a suitable Ψ_1, we first establish that Z is consistent. Suppose that Z is inconsistent. Then, there exist $\{\neg\xi_1, \ldots, \neg\xi_n, \psi_1\} \subseteq Z$ such that $\vdash \neg(\neg\xi_1 \wedge \cdots \wedge \neg\xi_n \wedge \psi)$, or equivalently, $\vdash \xi_1 \vee \cdots \vee \xi_n \vee \neg\psi_1$. (This latter form shows that we may without loss of generality include ψ_1 in the set inducing the inconsistency.) An application of the (N) rule gives $\vdash \mathbf{X}(\xi_1 \vee \cdots \vee \xi_n \vee \neg\psi_1)$, or equivalently, $\vdash \neg\mathbf{X}(\neg\xi_1 \wedge \cdots \wedge \neg\xi_n \wedge \psi_1)$. We have

$$\vdash ((\neg\mathbf{X}\xi_1 \wedge \cdots \wedge \neg\mathbf{X}\xi_n \wedge \mathbf{X}\psi_1) \to \mathbf{X}(\neg\xi_1 \wedge \cdots \wedge \neg\xi_n \wedge \psi_1)) \tag{10}$$

(the derivation is left as an exercise to the reader). Taking the contrapositive of (10) and applying the (MP) rule, we obtain $\vdash \neg(\neg\mathbf{X}\xi_1 \wedge \cdots \wedge \neg\mathbf{X}\xi_n \wedge \mathbf{X}\psi_1)$, which is a contradiction since Ψ is consistent. So, Z must be consistent. Since Ψ is ESF(ϕ)-maximal and $\psi_1 \in \mathrm{ESF}(\phi)$, we have $Z \subseteq \mathrm{ESF}(\phi) \cup \neg\mathrm{ESF}(\phi)$. Consequently, Z satisfies the conditions of Lemma 5.13. Let $\Psi_1 \in U$ be a ESF(ϕ)-maximal consistent extension of Z. We have $\Psi \prec \Psi_1$ by definition of $\mathcal{I}(\prec)$. Furthermore, since $\psi_1 \in Z \subseteq \Psi_1 \in U$ and $\psi_1 \in \mathrm{ESF}(\phi)$, we have by the induction hypothesis $\mathcal{M}_\phi, \Psi_1 \models \psi_1$.

Suppose that $\psi = \mathbf{F}^*\psi_1 \in \mathrm{ESF}(\phi)$. We prove first the "if" direction using the contrapositive form $\mathbf{F}^*\psi_1 \notin \Psi$ implies $\mathcal{M}_\phi, \Psi \not\models \mathbf{F}^*\psi_1$. Suppose that $\mathbf{F}^*\psi_1 \notin \Psi$. We have to show that $\mathcal{M}_\phi, \Psi' \not\models \psi_1$ for all $\Psi \leq \Psi' \in U$. Select any $\Psi' \in U$ such that $\Psi \leq \Psi'$. By definition of transitive closure there exists a sequence of states $\Psi_1, \ldots, \Psi_n$ such that

$$\Psi = \Psi_1 \prec \cdots \prec \Psi_n = \Psi'.$$

We prove by induction on n that $\mathbf{F}^*\psi_1 \notin \Psi_n$ for all $n \geq 1$. The base case $n = 1$ is trivial since we assume $\mathbf{F}^*\psi_1 \notin \Psi$. For the inductive step, suppose that $\mathbf{F}^*\psi_1 \notin \Psi_{n-1}$. By maximality of Ψ_{n-1} we have $\neg\mathbf{F}^*\psi_1 \in \Psi_{n-1}$. By definition of ESF($\phi$) we have $\mathbf{X}\mathbf{F}^*\psi_1 \in \mathrm{ESF}(\phi)$, so either $\mathbf{X}\mathbf{F}^*\psi_1 \in \Psi_{n-1}$ or $\neg\mathbf{X}\mathbf{F}^*\psi_1 \in \Psi_{n-1}$ by maximality of Ψ_{n-1}. The former case is impossible since Ψ_{n-1} is consistent and $\vdash \neg(\neg\mathbf{F}^*\psi_1 \wedge \mathbf{X}\mathbf{F}^*\psi_1)$. (The derivation is left as an exercise to the reader.) Thus, $\neg\mathbf{X}\mathbf{F}^*\psi_1 \in \Psi_{n-1}$. Let Ψ_n be any state such that $\Psi_{n-1} \prec \Psi_n$. By definition of $\mathcal{I}(\prec)$ we have $\neg\mathbf{F}^*\psi_1 \in \Psi_n$ because $\neg\mathbf{X}\mathbf{F}^*\psi_1 \in \Psi_{n-1}$. So, $\mathbf{F}^*\psi_1 \notin \Psi_n$ by consistency of Ψ_n. This completes the inductive step. We now have $\mathbf{F}^*\psi_1 \notin \Psi'$ for all $\Psi \leq \Psi'$. Since $\psi_1 \in \mathrm{ESF}(\phi)$ and $\vdash \neg(\neg\mathbf{F}^*\psi_1 \wedge \psi_1)$, we must have $\neg\psi_1 \in \Psi'$ by consistency and maximality of Ψ'. Therefore $\mathcal{M}_\phi, \Psi' \not\models \psi_1$ by the induction hypothesis, and since Ψ' was arbitrary, $\mathcal{M}_\phi, \Psi \not\models \mathbf{F}^*\psi_1$. The "only if" direction (in contrapositive form $\mathcal{M}_\phi, \Psi \not\models \mathbf{F}^*\psi_1$ implies $F^*\psi_1 \notin \Psi$) is the most involved part of the proof and requires additional notation for convenient exposition. Recall that any ESF(ϕ)-maximal consistent set $\Psi \in U$ is finite and consists of exactly $|\mathrm{ESF}(\phi)|$ sentences. We denote by $\hat{\Psi}$ the conjuction of all sentences in Ψ, that is, $\hat{\Psi} \stackrel{\text{def}}{=} \xi_1 \wedge \cdots \wedge \xi_{|\mathrm{ESF}(\phi)|}$, where $\Psi = \{\xi_1, \ldots, \xi_{|\mathrm{ESF}(\phi)|}\}$. Similarly, the set U is finite with at most $2^{|\mathrm{ESF}(\phi)|}$ elements. So, any subset $W = \{\Psi_1, \ldots, \Psi_m\} \subseteq U$ is finite. We denote by $\check{W}$ the disjunction of the sentences $\hat{\Psi}_1, \cdots, \hat{\Psi}_m$, that is, $\check{W} \stackrel{\text{def}}{=} \hat{\Psi}_1 \vee \cdots \vee \hat{\Psi}_m$. Armed with this additional notation we now continue the proof. Suppose that $\mathcal{M}_\phi, \Psi \not\models \mathbf{F}^*\psi_1$ and define

$$T_\Psi \stackrel{\text{def}}{=} \{\Psi' \in U \ : \ \Psi \leq \Psi'\},$$

that is, T_Ψ is the set of all $\Psi' \in U$ reachable from Ψ. By $\mathcal{M}_\phi, \Psi \not\models \mathbf{F}^*\psi_1$ we thus have $\mathcal{M}_\phi, \Psi' \not\models \psi_1$ for all $\Psi' \in T_\Psi$. Since $\psi_1 \in \mathrm{ESF}(\phi)$, the induction hypothesis now implies $\psi_1 \notin \Psi'$ for all $\Psi' \in T_\Psi$. By maximality of Ψ' we must have $\neg\psi_1 \in \Psi'$. So,

$\vdash \neg(\psi_1 \wedge \hat{\Psi}')$, or equivalently, $\vdash (\hat{\Psi}' \rightarrow \neg\psi_1)$ for all $\Psi' \in T_\Psi$. Consequently,

$$\vdash (\check{T}_\Psi \rightarrow \neg\psi_1). \tag{11}$$

Suppose for the moment that

$$\vdash (\check{T}_\Psi \rightarrow \mathbb{X}\check{T}_\Psi). \tag{12}$$

(We will justify this claim at the end of the proof.) Derivations (11) and (12) can clearly be combined to yield

$$\vdash (\check{T}_\Psi \rightarrow \neg\psi_1 \wedge \mathbb{X}\check{T}_\Psi).$$

So, an application of the (Ind) rule gives $\vdash (\check{T}_\Psi \rightarrow \mathbf{G}^*\neg\psi_1)$. Since $\Psi \in T_\Psi$, we obviously have $\vdash (\hat{\Psi} \rightarrow \check{T}_\Psi)$. Combining the two derivations, we get $\vdash (\hat{\Psi} \rightarrow \mathbf{G}^*\neg\psi_1)$, or equivalently, $\vdash \neg(\hat{\Psi} \wedge \mathbf{F}^*\psi_1)$. Since Ψ is consistent, we must have $\mathbf{F}^*\psi_1 \notin \Psi$.

The proof is now otherwise complete, but we still have to justify (12). Define

$$S_\Psi \stackrel{\text{def}}{=} \{\Psi' \in U \ : \ \Psi \prec \Psi'\},$$

that is, S_Ψ is the set of all immediate successors of Ψ. We will first establish

$$\vdash (\hat{\Psi} \rightarrow \mathbb{X}\check{S}_\Psi), \tag{13}$$

which we will then extend to (12). Clearly,

$$\vdash ((\mathbb{X}\xi_1 \wedge \cdots \wedge \mathbb{X}\xi_m) \rightarrow \mathbb{X}(\xi_1 \wedge \cdots \wedge \xi_m)),$$

so we have

$$\vdash (\hat{\Psi} \rightarrow \mathbb{X}(\bigwedge\{\neg\xi \ : \ \neg\mathbf{X}\xi \in \Psi\})). \tag{14}$$

Furthermore, $\vdash (\hat{\Psi} \rightarrow \mathbb{X}\check{U})$ holds since $\vdash \check{U}$ holds. (To see that $\vdash \check{U}$, observe that

$$Z \stackrel{\text{def}}{=} \bigvee\{\hat{M} \ : \ M \text{ is ESF}(\phi)\text{-maximal}\}$$

is obtained by substitution from a propositional tautology. The inconsistent ESF(ϕ)-maximal sets can now be removed from Z using their inconsistency derivations in conjunction with suitable sentences derived from propositional tautologies and the (MP) rule. This results in a derivation for $\check{U}$; details are left as an exercise to the reader.) Combining (14) and $\vdash (\hat{\Psi} \rightarrow \mathbb{X}\check{U})$, we obtain

$$\vdash (\hat{\Psi} \rightarrow \mathbb{X}(\check{U} \wedge \bigwedge\{\neg\xi \ : \ \neg\mathbf{X}\xi \in \Psi\}),$$

from which (13) can be derived by dropping the conjunctions in $\check{U}$ that conflict with $\bigwedge\{\neg\xi \ : \ \neg\mathbf{X}\xi \in \Psi\}$; details are left to the reader. From (13) we obtain

$$\vdash ((\vee_{\Psi' \in T_\Psi}\hat{\Psi}') \rightarrow (\vee_{\Psi' \in T_\Psi}\mathbb{X}\check{S}_{\Psi'})),$$

which implies

$$\vdash ((\vee_{\Psi' \in T_\Psi}\hat{\Psi}') \rightarrow \mathbb{X}(\vee_{\Psi' \in T_\Psi}\check{S}_{\Psi'})). \tag{15}$$

Since $\cup_{\Psi' \in T_\Psi} S_{\Psi'} \subseteq T_\Psi$, we have

$$\vdash (\vee_{\Psi' \in T_\Psi}\check{S}_{\Psi'}) \rightarrow \check{T}_\Psi. \tag{16}$$

Combining (15) and (16), we finally obtain (12).