On the Completeness of Propositional Raw TLA

Stephan Merz

Abstract

This note defines a propositional variant of the "raw" (stuttering-sensitive) Temporal Logic of Actions and gives a complete axiomatization of that logic. It is intended as a companion to and justification of my Isabelle encoding of (raw) TLA.

1 Propositional RTLA

1.1 Syntax

The language of RTLA is based on a countably infinite set $\mathcal{V}$ of *proposition symbols*. Formulas of RTLA are inductively defined as follows:

- For every proposition symbol $v \in \mathcal{V}$, both v and v' are formulas.
- If F and G are formulas, then $\neg F$, $F \rightarrow G$, and $\Box F$ are formulas.

The logic RTLA defined here differs from Lamport's TLA [6] and the propositional logic PTLA of [1] in that a primed proposition symbol like v' is a formula, and not only occurrences such as $[v']$ or $\Box[v']_w$. Consequently, there is no need to consider a separate syntactic category of action formulas. RTLA differs from standard propositional linear-time temporal logic PTL [5, 7] in that the prime may be applied only to proposition symbols, unlike PTL's next-time operator, which may be applied to arbitrary formulas.

A *state formula* is an RTLA formula that contains neither primed symbols nor the $\Box$ operator. In the following, we will use letters like $P, Q, \ldots$ to denote state formulas and letters like $F, G, \ldots$ to denote arbitrary RTLA formulas.

We will use standard boolean connectives such as TRUE, FALSE, $\wedge$, $\vee$, and $\leftrightarrow$, which can be defined by standard abbreviations. We write $\Diamond F$ as an abbreviation for the formula $\neg\Box\neg F$. Finally, if P is a state formula, we write P' for the formula that results from P by replacing every proposition symbol v that occurs in P by v'.

1.2 Semantics

The semantics of RTLA is a straightforward adaptation of the standard PTL semantics. An interpretation is a mapping $\mathcal{K}$ that assigns to each proposition symbol $v \in \mathcal{V}$ a set $\mathcal{K}(v) \subseteq I\!N$ of natural numbers. Intuitively, we think of an interpretation as an infinite sequence $\langle\!\langle s_0, s_1, \ldots\rangle\!\rangle$ of states, and $i \in \mathcal{K}(v)$ holds iff v is true at state s_i.

We now define the satisfaction relation between interpretations, natural numbers, and formulas, by induction on the structure of formulas; informally, $\mathcal{K}_i \models F$ means that formula F is true in interpretation $\mathcal{K}$ at state i.

$$
\begin{array}{rcll}
\mathcal{K}_i \models v & \text{iff} & i \in \mathcal{K}(v) & (\text{for } v \in \mathcal{V}) \\
\mathcal{K}_i \models v' & \text{iff} & i+1 \in \mathcal{K}(v) & (\text{for } v \in \mathcal{V}) \\
\mathcal{K}_i \models \neg F & \text{iff} & \mathcal{K}_i \not\models F & \\
\mathcal{K}_i \models F \rightarrow G & \text{iff} & \mathcal{K}_i \not\models F \text{ or } \mathcal{K}_i \models G & \\
\mathcal{K}_i \models \Box F & \text{iff} & \mathcal{K}_j \models F \text{ for every } j \geq i &
\end{array}
$$

The formula F is *satisfiable* iff there exists an interpretation $\mathcal{K}$ such that $\mathcal{K}_i \models F$ holds for some $i \in I\!N$. The formula F is *valid* iff $\mathcal{K}_i \models F$ holds for every interpretation $\mathcal{K}$ and every $i \in I\!N$. We say that formula F is *valid in interpretation* $\mathcal{K}$ and write $\mathcal{K} \models F$ iff $\mathcal{K}_i \models F$ holds for every $i \in I\!N$. The formula F *follows from* a set $\mathcal{F}$ of formulas ($\mathcal{F} \models F$) iff F is valid in every interpretation $\mathcal{K}$ where every formula $G \in \mathcal{F}$ is valid.

Note that we have chosen the "floating" definition of validity in contrast to the "anchored" definition preferred by Abadi and Lamport [1, 6] that defines F to be valid iff $\mathcal{K}_0 \models F$ holds for every interpretation $\mathcal{K}$. It is well-known that the two definitions are equivalent as far as validity is concerned; however, the floating definition generalizes more smoothly to the notion of consequence, which is not introduced by Abadi and Lamport. In particular, our definitions imply that $\mathcal{F} \models \Box F$ whenever $\mathcal{F} \models F$.

2 A proof system for RTLA

The logic RTLA introduced in section 1 is obviously a sublogic of PTL with a syntactic restriction on the occurrence of the next-time operator. In principle, there is no need for a new proof system: to decide whether $\mathcal{F} \models F$ holds, we could simply find a derivation in some sound and complete proof system for PTL [2, 5]. However, such a derivation would possibly contain intermediate PTL formulas that are not RTLA formulas. A direct axiomatization of RTLA is therefore a more convincing argument in favor of RTLA's status as a credible logic. Besides, it may reveal new insights into the essential ingredients of RTLA. In this section, we will present a proof system for RTLA, whose completeness will be shown in section 3. One should keep in mind that a sublogic $\mathcal{L}_1$ of some logic $\mathcal{L}_0$ need not have a simpler proof system than $\mathcal{L}_0$; in fact, there is no a priori guarantee that $\mathcal{L}_1$ can be (finitely) axiomatized at all, even if there is a complete axiomatization of $\mathcal{L}_0$.

The proof system Σ_{RTLA} shown in figure 1 contains some standard axioms from modal logic that concern the $\Box$ operator and some TLA-specific axioms that concern the interplay of $\Box$ and prime. Specifically, axioms (ax0)–(ax5) and

Axioms:	(ax0)	any instance of a propositional tautology
	(ax1)	$\Box(F \to G) \to (\Box F \to \Box G)$
	(ax2)	$\Box F \to F$
	(ax3)	$\Box F \to \Box\Box F$
	(ax4)	$\Box(\Box F \to G) \vee \Box(\Box G \to F)$
	(ax5)	$\Box(\Box(F \to \Box F) \to F) \to (\Diamond\Box F \to F)$
	(ax6)	$\Box P \to P'$
	(ax7)	$\Box(P \to \Box F) \to (P' \to (F \to \Box F))$
	(ax8)	$\Box(P \to (\neg P' \to \Box F)) \to (P \to \Box(\neg P \to \Box F))$
Rules:	(mp)	$F, F \to G \vdash G$
	(alw)	$F \vdash \Box F$

Figure 1: The axiom system Σ_{RTLA}

the rules form a well-known system of modal logic that is usually denoted as D [4] or S4.3*Dum* [3]. Axiom (ax1) is the usual K-axiom of modal logic; axioms (ax2) and (ax3) assert that the future is reflexive and transitive. Axiom (ax4) expresses that time is linear; in any normal modal logic, (ax4) could equivalently be replaced by the perhaps more intuitive axiom

$$\text{(LIN)} \quad \Diamond F \wedge \Diamond G \to \Diamond(F \wedge \Diamond G) \vee \Diamond(G \wedge \Diamond F)$$

(see section A.2 in the appendix for a derivation of this equivalence). Finally, the Geach axiom (ax5) expresses that time is discrete; an alternative formulation is

$$\text{(DISC)} \quad \Box(F \to \Diamond(\neg F \wedge \Diamond F)) \to (F \to \Box\Diamond F)$$

which asserts that if F holds now and if every state where F holds is followed by a state where $\neg F \wedge \Diamond F$ holds, then F holds infinitely often.

The remaining axioms (ax6)–(ax8) are specific to RTLA. Axiom (ax6) expresses that the next state is included in the future, while axiom (ax7) intuitively asserts that P' refers to the following state. Finally, axiom (ax8) is an induction axiom; for example, the basic induction principle for state predicates

$$\text{(INV1)} \quad P \wedge \Box(P \to P') \to \Box P$$

is an easy consequence of axiom (ax8). Again, axioms (ax6)–(ax8) are not without alternatives. For example, we prove in section A.3 in the appendix that (ax8) could be replaced by

$$\text{(IND)} \quad \Box(P \to (P' \wedge F) \vee \Box F) \to (P \to \Box F)$$

which is the RTLA analogue to the induction principle proposed in (the conference version of) [1].It is even possible to merge (ax7) and (IND) in the single axiom

$$\Box(P \to (P' \wedge F) \vee \Box F) \to (P' \wedge F \to \Box F)$$

as suggested in (the revised version of) [1]. The rules of Σ_{RTLA} are standard.

As usual, a derivation of formula F from a set $\mathcal{F}$ of formulas in Σ_{RTLA} is a sequence $F_1, F_2, \ldots, F_n$ of formulas that ends with F such that every formula F_i is either some formula from $\mathcal{F}$ or an instance of one of the axioms (ax0)–(ax8), or is obtained by an application of the rules (mp) or (alw) to formulas that occur earlier in the sequence. We say that F is derivable from $\mathcal{F}$ and write $\mathcal{F} \vdash F$ (or simply $\vdash F$ in case $\mathcal{F} = \emptyset$) if there is a derivation of F from $\mathcal{F}$. Note that Σ_{RTLA} includes all instances of propositional tautologies and the rule (mp) and therefore subsumes propositional logic. In actual derivations, we will not explicitly justify purely propositional steps.

The following theorem asserts the soundness of Σ_{RTLA}.

Theorem 1 *For any formula F and set of formulas $\mathcal{F}$, if $\mathcal{F} \vdash F$ then $\mathcal{F} \models F$.*

PROOF The proof is by induction on the assumed derivation of F from $\mathcal{F}$. As an example for the base cases, we show the soundness of axiom (ax8).

Let $\mathcal{K}$ be some interpretation such that $\mathcal{K} \models G$ holds for all formulas $G \in \mathcal{F}$, and $i \in \mathbb{N}$ be such that $\mathcal{K}_i \models P$ and $\mathcal{K}_i \models \Box(P \wedge P' \rightarrow \Box F)$ (for an arbitrary state formula P and temporal formula F). We have to show $\mathcal{K}_i \models \Box(\neg P \rightarrow \Box F)$. So, assume that $j \geq i$ and $\mathcal{K}_j \models \neg P$. By the assumption that $\mathcal{K}_i \models P$ holds, it must be the case that $j > i$. Let k be the largest number less than j such that $\mathcal{K}_k \models P$ holds (hence $i \leq k < j$). This choice of k implies that $\mathcal{K}_k \models P \wedge \neg P'$, and since $k \geq i$ it follows that $\mathcal{K}_k \models \Box F$, which in turn implies $\mathcal{K}_j \models \Box F$ as desired.

The induction step for rule (alw) uses the fact that $\mathcal{F} \models \Box F$ holds whenever $\mathcal{F} \models F$ holds. $\lhd$

Unlike classical propositional and first-order logic, where implication and consequence commute, modal logics with the floating semantics do not validate the deduction theorem in its classical form. Instead, a formula may be brought to the right-hand side of the turnstile by "boxing" it. In particular, using axiom (ax3), it follows that implication and entailment commute for boxed formulas.

Theorem 2 *For any set $\mathcal{F}$ of formulas and formulas F, G, we have*

$$\mathcal{F} \cup \{F\} \vdash G \qquad \textit{iff} \qquad \mathcal{F} \vdash \Box F \rightarrow G$$

PROOF Assume that $\mathcal{F} \cup \{F\} \vdash G$. We show that $\mathcal{F} \vdash \Box F \rightarrow G$, by induction on the assumed derivation of G from $\mathcal{F} \cup \{F\}$.

1. If G is an axiom or $G \in \mathcal{F}$, then we have $\mathcal{F} \vdash G$. Now, $G \rightarrow (\Box F \rightarrow G)$ is an instance of (ax0), so an application of (mp) yields the assertion.

2. If G is F, then $\Box F \rightarrow F$ is an instance of (ax2).

3. If G results from an application of (mp) to premises H and $H \rightarrow G$, then by induction hypothesis we know $\mathcal{F} \vdash \Box F \rightarrow H$ and $\mathcal{F} \vdash \Box F \rightarrow (H \rightarrow G)$, and the assertion follows propositionally.

(H1)	$F \to G \vdash \Box F \to \Box G$	(H8)	$P \land \Box(P \to P') \leftrightarrow \Box P$
(H2)	$F \to G \vdash \Diamond F \to \Diamond G$	(H9)	$\Box P \leftrightarrow P \land \Box P'$
(H3)	$\Box F \to G \vdash \Box F \to \Box G$	(H10)	$P \to \Box Q \vdash P' \to \Box Q'$
(H4)	$\Box F \land \Box G \leftrightarrow \Box(F \land G)$	(H11)	$P \to \Diamond Q \vdash P' \to \Diamond Q'$
(H5)	$\Diamond F \land \Box G \to \Diamond(F \land G)$	(H12)	$P \land P' \to F \vdash \Box P \to \Box F$
(H6)	$\Diamond\Box F \land \Diamond\Box G \leftrightarrow \Diamond\Box(F \land G)$	(H13)	$\Box\Diamond P \leftrightarrow \Box\Diamond P'$
(H7)	$\Box\Diamond F \leftrightarrow \Diamond\Box\Diamond F$	(H14)	$P \to \Diamond P' \vdash P \to \Box\Diamond P$

Figure 2: Some consequences of system Σ_{RTLA}

4. If G is of the form $\Box H$ and results from an application of (alw) to premise H, then by induction hypothesis we obtain $\mathcal{F} \vdash \Box F \to H$. We give a derivation of $\Box F \to \Box H$ from $\Box F \to H$:

(1)	$\Box F \to H$	(assumption)
(2)	$\Box(\Box F \to H)$	(alw)(1)
(3)	$\Box(\Box F \to H) \to (\Box\Box F \to \Box H)$	(ax1)
(4)	$\Box\Box F \to \Box H$	(mp)(2)(3)
(5)	$\Box F \to \Box\Box F$	(ax3)
(6)	$\Box F \to \Box H$	(4)(5)

Conversely, if $\mathcal{F} \vdash \Box F \to G$ (and therefore $\mathcal{F} \cup \{F\} \vdash \Box F \to G$), then by rule (alw) we have $\mathcal{F} \cup \{F\} \vdash \Box F$ and an application of (mp) therefore yields the assertion $\mathcal{F} \cup \{F\} \vdash G$. $\lhd$

We conclude this section with a list of some consequences of our system Σ_{RTLA}, shown in figure 2. The derivations are given in section A.1 in the appendix. Some of these formulas are familiar from Lamport's axioms in [6]. For example, (H12) is similar to Lamport's rule (TLA2). Formula (H9) gives a "recursive" characterization of $\Box P$ for a state predicate P. The derived rule (H14) represents an induction principle that can be used to prove that a state predicate is true infinitely often.

3 Completeness of Σ_{RTLA}

Abadi [1] has given a completeness proof for a slightly different version of propositional TLA as an extension of a classical completeness proof from [3] for system S4.3*Dum*. This section gives a direct completeness proof for Σ_{RTLA}. Although Abadi's proof is somewhat shorter, a direct proof may provide better insight into which axioms are actually needed in the completeness proof; in fact, the motivation for finding a new proof was to simplify Abadi's system (we have unfortunately failed to achieve this goal). In our proof, we follow the usual Henkin-Hasenjäger strategy and construct a model for a consistent formula. The main technical difficulty compared to classical PTL completeness proofs [2, 5] comes from the absence of a full next-time operator in TLA and the corresponding relative weakness of the induction axiom (ax8).

We start by recalling some standard definitions and facts. Throughout, we will deal with finite sets of formulas and will identify a set $\mathcal{F} = \{F_1, \ldots, F_n\}$ of formulas with the conjunction $F_1 \wedge \ldots \wedge F_n$ of its elements. In particular, the empty set is identified with TRUE. If $\mathcal{F}$ is a set of formulas, $\mathcal{F}^\Box$ will denote the subset that contains all boxed formulas from $\mathcal{F}$:

$$\mathcal{F}^\Box = \{\Box F : \Box F \in \mathcal{F}\}$$

Definition 3 *A finite set $\mathcal{F}$ of formulas is* inconsistent *if* $\vdash \neg\mathcal{F}$. *Otherwise, $\mathcal{F}$ is* consistent.

Lemma 4 *For any consistent set $\mathcal{F}$ and formula F, one of $\mathcal{F} \cup \{F\}$ or $\mathcal{F} \cup \{\neg F\}$ is consistent.*

PROOF From $\vdash \neg(\mathcal{F} \wedge F)$ and $\vdash \neg(\mathcal{F} \wedge \neg F)$, propositional reasoning yields $\vdash \neg\mathcal{F}$, that is, the inconsistency of $\mathcal{F}$. $\lhd$

Similar to a tableau method (which is, in fact, implicit in the proof), our model construction decomposes the given set of formulas. The following definition, which defines a Fischer-Ladner closure for RTLA, formally introduces the notion of subformulas.

Definition 5 *With every formula F, we inductively associate a set $\tau(F)$ of subformulas, as follows:*

1. $\tau(v) = \{v, v'\} = \tau(v')$ *for* $v \in \mathcal{V}$
2. $\tau(\neg F) = \{\neg F\} \cup \tau(F)$
3. $\tau(F \to G) = \{F \to G\} \cup \tau(F) \cup \tau(G)$
4. $\tau(\Box F) = \{\Box F\} \cup \tau(F)$

This definition is extended to sets of formulas in the canonical way by

$$\tau(\mathcal{F}) = \{G : G \in \tau(F) \text{ for some } F \in \mathcal{F}\}$$

Observe that $\tau(F)$ is a finite set of formulas, for any formula F, and therefore $\tau(\mathcal{F})$ is finite for any finite set $\mathcal{F}$ of formulas. Moreover, $\tau(F)$ contains exactly those proposition symbols that occur (primed or unprimed) in F. Finally, the notion of subformula is "reflexive" in the sense that $F \in \tau(F)$ and "transitive" in that $H \in \tau(F)$ whenever $H \in \tau(G)$ for some $G \in \tau(F)$.

Definition 6 *A finite set $\mathcal{F}$ of formulas is called* complete *if for every formula $G \in \tau(\mathcal{F})$, either $G \in \mathcal{F}$ or $\neg G \in \mathcal{F}$ holds.*

Proposition 7 *For any consistent set $\mathcal{F}$ of formulas there exists some consistent and complete set $\mathcal{F}^* \supseteq \mathcal{F}$ such that $\tau(\mathcal{F}^*) = \tau(\mathcal{F})$. Any such set $\mathcal{F}^*$ is called a* completion *of $\mathcal{F}$.*

Proof Standard consequence of lemma 4. $\lhd$

The following standard propositions collect the essential properties of complete sets of formulas; observe that there can only be finitely many different completions of a given finite set $\mathcal{F}$ of formulas, because $\tau(\mathcal{F})$ is finite.

Proposition 8 *Let $\mathcal{F}$ be some complete and consistent set of formulas and F, G be formulas.*

1. *If $\vdash F \to G$, $F \in \mathcal{F}$, and $G \in \tau(\mathcal{F})$, then $G \in \mathcal{F}$.*
2. *If $F \to G \in \tau(\mathcal{F})$, then $F \to G \in \mathcal{F}$ if and only if $F \notin \mathcal{F}$ or $G \in \mathcal{F}$.*

Proposition 9 *If $\mathcal{F}$ is a finite set of formulas and $\mathcal{F}_1^*, \ldots, \mathcal{F}_n^*$ are all different completions of $\mathcal{F}$, then*

$$\vdash \mathcal{F} \to \mathcal{F}_1^* \vee \ldots \vee \mathcal{F}_n^*$$

Proposition 9 in particular implies that if $F \in \mathcal{F}^*$ holds for every completion $\mathcal{F}^*$ of $\mathcal{F}$, then $\vdash \mathcal{F} \to F$ holds.

While the set $\tau(\mathcal{F})$ of subformulas collects those formulas that are relevant to satisfying $\mathcal{F}$ in the current state, our construction also needs information about which formulas to satisfy in the successor state. That information is provided by the set $\sigma(\mathcal{F})$, defined as

$$\begin{array}{rl} \sigma(\mathcal{F}) = & \mathcal{F}^{\Box} \\ & \cup \{v : v' \in \mathcal{F}\} \cup \{\neg v : \neg v' \in \mathcal{F}\} \\ & \cup \{\neg\Box F : \{\neg\Box F, F\} \subseteq \mathcal{F}\} \end{array}$$

Observe that this definition ensures that $\tau(\sigma(\mathcal{F})) \subseteq \tau(\mathcal{F})$. In particular, the set of proposition symbols that occur in $\sigma(\mathcal{F})$ is a subset of those in $\mathcal{F}$; the sets of proposition symbols are the same if $\mathcal{F}$ is complete (because then either $v' \in \mathcal{F}$ or $\neg v' \in \mathcal{F}$ holds for every proposition symbol v that occurs in $\mathcal{F}$).

Lemma 10 *If $\mathcal{F}$ is a consistent set of formulas, then $\sigma(\mathcal{F})$ is consistent.*

Proof Define the sets $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ by

$$\begin{array}{rcl} \mathcal{G}_1 & = & \{\Box(F_1 \wedge \ldots \wedge F_n) : \mathcal{F}^{\Box} = \Box F_1 \wedge \ldots \wedge \Box F_n\} \\ \mathcal{G}_2 & = & \{v : v' \in \mathcal{F}\} \cup \{\neg v : \neg v' \in \mathcal{F}\} \\ \mathcal{G}_3 & = & \{\neg\Box F : \{\neg\Box F, F\} \subseteq \mathcal{F}\} \end{array}$$

Observe that (the formula that corresponds to) $\mathcal{G}_2$ is a state predicate. For a set $\mathcal{H} = \{\neg\Box F_1, \ldots, \neg\Box F_n\}$ such as $\mathcal{G}_3$, we denote the set $\{F_1, \ldots, F_n\}$ by $\overline{\mathcal{H}}$. By the definition of $\sigma(\mathcal{F})$ and $(H4)$, we have

$$\vdash \sigma(\mathcal{F}) \leftrightarrow \mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \mathcal{G}_3 \qquad \text{and} \qquad \vdash \mathcal{F} \to \mathcal{G}_1 \wedge \mathcal{G}_2' \wedge \mathcal{G}_3 \wedge \overline{\mathcal{G}_3}$$

In the following proof, we assume that $\sigma(\mathcal{F})$ is inconsistent (and therefore, by propositional reasoning, $\vdash \mathcal{G}_1 \wedge \mathcal{G}_2 \rightarrow \neg\mathcal{G}_3$ holds) and derive

$$\mathcal{G}_1 \wedge \mathcal{G}_2' \wedge \overline{\mathcal{G}_3} \rightarrow \neg\mathcal{G}_3 \tag{3.1}$$

from this assumption. This implies the inconsistency of $\mathcal{F}$ and therefore the assertion of the lemma.

The proof of (3.1) is by induction on $|\mathcal{G}_3|$.

Case $|\mathcal{G}_3| = 0$. The assumption that $\sigma(\mathcal{F})$ is inconsistent implies $\vdash \mathcal{G}_1 \rightarrow \neg\mathcal{G}_2$. We derive (3.1) as follows:

(1)	$\mathcal{G}_1 \rightarrow \neg\mathcal{G}_2$	(assumption)
(2)	$\Box\mathcal{G}_1 \rightarrow \Box\neg\mathcal{G}_2$	(H1)(1)
(3)	$\Box\neg\mathcal{G}_2 \rightarrow \neg\mathcal{G}_2'$	(ax6)
(4)	$\mathcal{G}_1 \rightarrow \Box\mathcal{G}_1$	(ax3)
(5)	$\mathcal{G}_1 \rightarrow \neg\mathcal{G}_2'$	(4)(2)(3)

Case $|\mathcal{G}_3| = 1$. There exists some formula F such that $\{\neg\Box F, F\} \subseteq \mathcal{F}$, $\mathcal{G}_3 \equiv \neg\Box F$, and $\overline{\mathcal{G}_3} \equiv F$. The derivation of (3.1) is as follows:

(1)	$\mathcal{G}_1 \rightarrow (\mathcal{G}_2 \rightarrow \Box F)$	(assumption)
(2)	$\Box\mathcal{G}_1 \rightarrow \Box(\mathcal{G}_2 \rightarrow \Box F)$	(H1)(1)
(3)	$\Box(\mathcal{G}_2 \rightarrow \Box F) \rightarrow (\mathcal{G}_2' \rightarrow (F \rightarrow \Box F))$	(ax7)
(4)	$\mathcal{G}_1 \rightarrow \Box\mathcal{G}_1$	(ax3)
(5)	$\mathcal{G}_1 \wedge \mathcal{G}_2' \wedge \overline{\mathcal{G}_3} \rightarrow \neg\mathcal{G}_3$	(4)(2)(3)

Case $|\mathcal{G}_3| > 1$. Let F, G be formulas such that $\{\neg\Box F, \neg\Box G\} \subseteq \mathcal{G}_3$, and define the sets

$$\begin{aligned} \mathcal{H}_1 &= (\mathcal{G}_3 \setminus \{\neg\Box F, \neg\Box G\}) \cup \{\neg\Box(F \vee \Box G)\} \\ \mathcal{H}_2 &= (\mathcal{G}_3 \setminus \{\neg\Box F, \neg\Box G\}) \cup \{\neg\Box(G \vee \Box F)\} \end{aligned}$$

By (LIN), which we have shown to be a consequence of Σ_{RTLA} (cf. section A.2), it follows that $\vdash \mathcal{G}_3 \leftrightarrow \mathcal{H}_1 \vee \mathcal{H}_2$, and obviously, $|\mathcal{H}_1| = |\mathcal{H}_2| < |\mathcal{G}_3|$. By the assumption that $\mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \mathcal{G}_3$ is inconsistent, both $\mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \mathcal{H}_1$ and $\mathcal{G}_1 \wedge \mathcal{G}_2 \wedge \mathcal{H}_2$ must be inconsistent, and the induction hypothesis implies

$$\vdash \mathcal{G}_1 \wedge \mathcal{G}_2' \wedge \overline{\mathcal{H}_1} \rightarrow \neg\mathcal{H}_1 \qquad \text{and} \qquad \vdash \mathcal{G}_1 \wedge \mathcal{G}_2' \wedge \overline{\mathcal{H}_2} \rightarrow \neg\mathcal{H}_2$$

and therefore, by propositional reasoning,

$$\vdash \mathcal{G}_1 \wedge \mathcal{G}_2' \wedge (\overline{\mathcal{H}_1} \wedge \overline{\mathcal{H}_2}) \rightarrow \neg(\mathcal{H}_1 \vee \mathcal{H}_2)$$

Now, $\overline{\mathcal{H}_1}$ is equivalent to $(\overline{\mathcal{G}_3} \setminus \{F, G\}) \cup \{F \vee \Box G\}$ and, similarly, $\overline{\mathcal{H}_2}$ is equivalent to $(\overline{\mathcal{G}_3} \setminus \{F, G\}) \cup \{G \vee \Box F\}$. Since $\{F, G\} \subseteq \overline{\mathcal{G}_3}$, we have $\vdash \overline{\mathcal{G}_3} \rightarrow \overline{\mathcal{H}_1} \wedge \overline{\mathcal{H}_2}$ and therefore obtain assertion (3.1). $\lhd$

Lemma 10 is weaker than the corresponding lemma in the completeness proof for standard PTL, where one proves $\mathcal{F} \rightarrow \bigcirc \sigma(\mathcal{F})$, a formula that is not expressible in RTLA. Nevertheless, we may continue as usual with the inductive definition of a tree $\mathcal{T}(\mathcal{F})$ of sets of formulas that will contain the desired model for $\mathcal{F}$ whenever $\mathcal{F}$ is consistent.

Definition 11 *For any finite set of formulas $\mathcal{F}$, we define the tree $\mathcal{T}(\mathcal{F})$ as follows:*

- *The root of $\mathcal{T}(\mathcal{F})$ is $\mathcal{F}$.*
- *If $\mathcal{N}$ is a node in $\mathcal{T}(\mathcal{F})$, then its children are all possible completions of $\sigma(\mathcal{N})$.*

Lemma 10 ensures that $\mathcal{T}(\mathcal{F})$ is an infinite tree of consistent and complete sets of formulas whenever $\mathcal{F}$ is consistent. Moreover, a simple inductive argument shows that $\tau(\mathcal{N}) \subseteq \tau(\mathcal{F})$ holds for every node $\mathcal{N}$ of $\mathcal{T}(\mathcal{F})$, and that all nodes in $\mathcal{T}(\mathcal{F})$ contain the same set of proposition symbols.

As usual in completeness proofs of this kind, not every path in $\mathcal{T}(\mathcal{F})$ gives rise to a model for $\mathcal{F}$; rather, we have to make sure that all formulas $\neg\Box F$ that occur in nodes along the path will eventually be satisfied along the path. For the remainder of the proof, we choose, for every consistent and complete set $\mathcal{F}$ of formulas, an infinite sequence $\eta(\mathcal{F}) = \langle\langle \eta_0, \eta_1, \ldots \rangle\rangle$ of formulas such that every formula η_i is of the form[1] $\Box F \in \tau(\mathcal{F}) \cup \{\Box \text{TRUE}\}$ and that every formula $\Box F \in \tau(\mathcal{F})$ occurs infinitely often in $\eta(\mathcal{F})$.

Definition 12

1. *A* path *in $\mathcal{T}(\mathcal{F})$ is an infinite sequence $\langle\langle (\mathcal{N}_0, k_0), (\mathcal{N}_1, k_1), \ldots \rangle\rangle$ such that*
   - *$\mathcal{N}_0$ is the root of $\mathcal{T}(\mathcal{F})$ and $k_0 = 0$,*
   - *$\mathcal{N}_{i+1}$ is a child of $\mathcal{N}_i$ and $k_{i+1} = k_i$ if (for $\eta_{k_i} \equiv \Box F$) both $\neg\Box F \in \mathcal{N}_i$ and $F \in \mathcal{N}_i$, otherwise $k_{i+1} = k_i + 1$.*
2. *For a path $\pi = \langle\langle (\mathcal{N}_0, k_0), (\mathcal{N}_1, k_1), \ldots \rangle\rangle$ in $\mathcal{T}(\mathcal{F})$, we define the interpretation $\mathcal{K}^\pi$ by $\mathcal{K}^\pi(v) = \{i \in \mathbb{N} : v \in \mathcal{N}_i\}$ for every proposition symbol $v \in \mathcal{V}$.*
3. *A path $\pi = \langle\langle (\mathcal{N}_0, k_0), (\mathcal{N}_1, k_1), \ldots \rangle\rangle$ is* admissible *if the sequence $k_0, k_1, \ldots$ grows without bound, that is, for every $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $k_m \geq n$.*

[1] The formula $\Box$TRUE is included to ensure that some such sequence $\eta(\mathcal{F})$ exists.

The definition of an admissible path ensures that if π is an admissible path and $\neg\Box G \in \mathcal{N}_i$ for some $i \in I\!N$, then there exists some $j \geq i$ such that $\neg G \in \mathcal{N}_j$, because $\eta_n \equiv \Box G$, for some $n \geq k_i$. The following lemma shows that the interpretation associated with an admissible path indeed satisfies $\mathcal{F}$ at state 0.

Lemma 13 *Let $\pi = \langle\!\langle(\mathcal{N}_0, k_0), (\mathcal{N}_1, k_1), \ldots\rangle\!\rangle$ be an admissible path in $\mathcal{T}(\mathcal{F})$ and $\mathcal{K}^\pi$ be the interpretation associated with π. Then, for every $i \in I\!N$, $\mathcal{K}^\pi_i \models \mathcal{N}_i$.*

PROOF More generally, we prove for every $i \in I\!N$ and every formula $F \in \tau(\mathcal{N}_i)$ that

$$(*) \qquad F \in \mathcal{N}_i \quad \text{iff} \quad \mathcal{K}^\pi_i \models F$$

by induction on F.

Case $F \equiv v \in \mathcal{V}$. Immediate by the definition of $\mathcal{K}^\pi$.

Case $F \equiv v'(v \in \mathcal{V})$. If $v' \in \mathcal{N}_i$, then the definition of $\sigma(\mathcal{N}_i)$ implies $v \in \sigma(\mathcal{N}_i)$ and therefore $v \in \mathcal{N}_{i+1}$. By the definition of $\mathcal{K}^\pi$, we obtain $i+1 \in \mathcal{K}^\pi(v)$, hence $\mathcal{K}^\pi_i \models v'$. Conversely, if $v' \notin \mathcal{N}_i$, then $\neg v' \in \mathcal{N}_i$ (by the assumptions that $\mathcal{N}_i$ is complete and $v' \in \tau(\mathcal{N}_i)$), and therefore $\neg v \in \sigma(\mathcal{N}_i) \subseteq \mathcal{N}_{i+1}$. Since $\mathcal{N}_{i+1}$ is consistent, this implies $v \notin \mathcal{N}_{i+1}$ and therefore $i+1 \notin \mathcal{K}^\pi(v)$, hence $\mathcal{K}^\pi_i \not\models v'$.

Case $F \equiv \neg G$. The assumption $F \in \tau(\mathcal{N}_i)$ implies $G \in \tau(\mathcal{N}_i)$, and by the consistency of $\mathcal{N}_i$ we conclude $G \notin \mathcal{N}_i$ iff $F \in \mathcal{N}_i$. The assertion now follows from the induction hypothesis.

Case $F \equiv G \to H$. Similar.

Case $F \equiv \Box G$. If $\Box G \in \mathcal{N}_i$, then the definitions of $\sigma(\mathcal{N})$ and $\mathcal{T}(\mathcal{F})$ imply $\Box G \in \mathcal{N}_j$ for all $j \geq i$, by a simple inductive argument, hence in particular $G \in \tau(\mathcal{N}_j)$. By axiom (ax2) and proposition 8, it follows that $G \in \mathcal{N}_j$ for all $j \geq i$. The induction hypothesis thus yields $\mathcal{K}^\pi_j \models G$ for all $j \geq i$, and therefore $\mathcal{K}^\pi_i \models F$.

Conversely, if $\Box G \notin \mathcal{N}_i$, then $\neg\Box G \in \mathcal{N}_i$, by the assumption $\Box G \in \tau(\mathcal{N}_i)$ and the fact that $\mathcal{N}_i$ is complete. The assumption that π is an admissible path implies that $\neg G \in \mathcal{N}_j$, for some $j \geq i$. The consistency of $\mathcal{N}_j$ yields $G \notin \mathcal{N}_j$ and therefore $\mathcal{K}^\pi_j \not\models G$, by the induction hypothesis. But this means $\mathcal{K}^\pi_i \not\models \Box G$. $\lhd$

It remains to prove that there exists some admissible path in $\mathcal{T}(\mathcal{F})$ if $\mathcal{F}$ is consistent and complete. For this proof we need to look a little closer at the structure of $\mathcal{T}(\mathcal{F})$. First of all, the observations that $\tau(\sigma(\mathcal{N})) \subseteq \tau(\mathcal{N})$ for any set $\mathcal{N}$ of formulas, and that $\tau(\mathcal{N}^*) = \tau(\mathcal{N})$ whenever $\mathcal{N}^*$ is a completion of $\mathcal{N}$ imply that every node in $\mathcal{T}(\mathcal{F})$ is a set of (possibly negated) formulas from $\tau(\mathcal{F})$, which is a finite set. Therefore, $\mathcal{T}(\mathcal{F})$ can contain only finitely many different nodes.

Lemma 14 *Let $\mathcal{N}$ be some consistent and complete set of formulas, and let $\mathcal{S}$ be some completion of $\sigma(\mathcal{N})$. For any formula F, if $\neg\Box F \in \mathcal{S}$ then $\neg\Box F \in \mathcal{N}$.*

PROOF By the definition of $\sigma(\mathcal{N})$, we know that $\tau(\sigma(\mathcal{N})) \subseteq \tau(\mathcal{N})$; moreover, proposition 7 (which defines the notion of completion) implies $\tau(\mathcal{S}) = \tau(\sigma(\mathcal{N}))$. If $\neg\Box F \in \mathcal{S}$, then $\Box F \in \tau(\mathcal{S})$, hence $\Box F \in \tau(\mathcal{N})$. Because $\mathcal{N}$ is complete, it must either be the case that $\Box F \in \mathcal{N}$ or that $\neg\Box F \in \mathcal{N}$. But the former case is impossible, because it would imply $\Box F \in \sigma(\mathcal{N}) \subseteq \mathcal{S}$, contradicting the consistency of $\mathcal{S}$. $\lhd$

If we denote by $\mathcal{G}^\Diamond$ the set of formulas of the form $\neg\Box F$ contained in $\mathcal{G}$ (for an arbitrary set $\mathcal{G}$ of formulas), lemma 14 asserts that $\mathcal{S}^\Diamond \subseteq \mathcal{N}^\Diamond$ holds whenever $\mathcal{S}$ is a child of $\mathcal{N}$ in $\mathcal{T}(\mathcal{F})$. Let us call a subtree $\mathcal{T}$ of $\mathcal{T}(\mathcal{F})$ *saturated* if the following two conditions are both satisfied:

- $\mathcal{N}^\Diamond = \mathcal{S}^\Diamond$ holds for any two nodes $\mathcal{N}, \mathcal{S}$ of $\mathcal{T}$.
- Every node of $\mathcal{T}$ occurs infinitely often in $\mathcal{T}$.

The observation that $\mathcal{S}^\Diamond \subseteq \mathcal{N}^\Diamond$ holds whenever $\mathcal{S}$ is a child of $\mathcal{N}$, together with the finiteness of $\mathcal{F}$ (and therefore, a fortiori, of $\mathcal{F}^\Diamond$) and the fact that the number of different nodes in $\mathcal{T}(\mathcal{F})$ is finite imply that for every node $\mathcal{N}$ of $\mathcal{T}(\mathcal{F})$, the subtree of $\mathcal{T}(\mathcal{F})$ rooted at $\mathcal{N}$ contains a saturated subtree.

Lemma 15 *If $\mathcal{N}$ is a node in some saturated subtree $\mathcal{T}$ of $\mathcal{T}(\mathcal{F})$, and $\mathcal{S}$ is a child of $\mathcal{N}$, then $\mathcal{S}^\Box = \mathcal{N}^\Box$.*

PROOF The definition of $\sigma(\mathcal{N})$ immediately implies $\mathcal{N}^\Box = (\sigma(\mathcal{N}))^\Box \subseteq \mathcal{S}^\Box$.

Conversely, assume $\Box F \in \mathcal{S}$. Since $\tau(\mathcal{S}) = \tau(\sigma(\mathcal{N})) \subseteq \tau(\mathcal{N})$, we have $\Box F \in \tau(\mathcal{N})$, and because $\mathcal{N}$ is complete, either $\Box F \in \mathcal{N}$ or $\neg\Box F \in \mathcal{N}$. But the latter case would imply $\neg\Box F \in \mathcal{S}$, because $\mathcal{N}$ is assumed to be a node in a saturated subtree of $\mathcal{T}(\mathcal{F})$, and contradict the consistency of $\mathcal{S}$. $\lhd$

Lemmas 14 and 15 imply that, essentially, the nodes of a saturated subtree differ only in the primed and unprimed proposition symbols. The following lemma asserts that all eventualities that occur in a saturated subtree may be boxed; this is the central step in proving the existence of an admissible path.

Lemma 16 *If $\mathcal{N}$ is the root of a saturated subtree $\mathcal{T}$ of $\mathcal{T}(\mathcal{F})$ then $\vdash \mathcal{N} \rightarrow \Box\mathcal{N}^\Diamond$.*

PROOF We know that $\mathcal{T}(\mathcal{F})$ contains only finitely many different nodes; let $\mathcal{N}_1, \ldots, \mathcal{N}_m$ be all nodes that occur in $\mathcal{T}$. By lemma 15 and the definition of a saturated subtree, we know that $\mathcal{N}_i^\Box = \mathcal{N}_j^\Box$ and $\mathcal{N}_i^\Diamond = \mathcal{N}_j^\Diamond$ for all $i, j \in \{1, \ldots, m\}$; using (H4), there exists some formula I such that $\vdash \mathcal{N}_j^\Box \leftrightarrow \Box I$. For concreteness, assume that $\mathcal{N}_j^\Diamond = \{\neg\Box F_1, \ldots, \neg\Box F_n\}$. Let $\mathcal{V}^0 \subseteq \mathcal{V}$ denote the set of proposition symbols that occur in $\mathcal{T}(\mathcal{F})$. (We have observed above that this is exactly the set of proposition symbols that occur in $\mathcal{F}$.) Let $\mathcal{N}_j^0$ denote the valuation of symbols in $\mathcal{V}^0$ determined by node $\mathcal{N}_j$, that is,

$$\mathcal{N}_j^0 \equiv \bigwedge_{v \in \mathcal{N}_j} v \quad \wedge \quad \bigwedge_{v \in \mathcal{V}^0 \setminus \mathcal{N}_j} \neg v$$

The disjunction of all $\mathcal{N}_j^0$ describes all valuations that occur in $\mathcal{T}$; it will be denoted by Q in the remainder of this proof.

Since all nodes $\mathcal{N}_j$ contain the formulas $\neg\Box F_i$ and are complete sets of formulas, they must also contain either F_i or $\neg F_i$. For every subset $M \subseteq \{1,\ldots,n\}$, let $\overline{M}$ denote the set $\{1,\ldots,n\} \setminus M$ and $\mathcal{E}_M \subseteq \{1,\ldots,m\}$ the set of indices of nodes such that $j \in \mathcal{E}_M$ iff $\mathcal{N}_j$ contains exactly the formulas $\neg F_i$ for $i \in M$ (and F_i for $i \in \overline{M}$). The set $\mathcal{E}_M$ indicates the set of nodes that immediately satisfy the eventualities $\neg\Box F_i$ for $i \in M$. Observe that for every node $\mathcal{N}_k$ there is exactly one set M such that $k \in \mathcal{E}_M$. Finally, let P_M denote the disjunction of valuations of primed variables (in $\mathcal{V}^0$) associated with nodes $\mathcal{N}_j$ for $j \in \mathcal{E}_M$:

$$P_M \equiv \bigvee_{i \in \mathcal{E}_M} \Big(\bigwedge_{v' \in \mathcal{N}_j} v \quad \wedge \quad \bigwedge_{\neg v' \in \mathcal{N}_j} \neg v \Big)$$

(We adopt the usual convention that an empty disjunction is identified with FALSE.) These definitions ensure that for every node $\mathcal{N}_j$ in $\mathcal{T}$, the formula

$$\mathcal{N}_j \rightarrow \bigvee_{M \subseteq \{1,\ldots,n\}} \Big(P'_M \wedge \bigwedge_{i \in \overline{M}} F_i \Big) \tag{3.2}$$

is a tautology.

We now claim the following assertions, whose proof appears below, where assertion (3.4) is claimed for every $M \subseteq \{1,\ldots,n\}$:

$$\vdash Q \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \rightarrow \bigvee_{M \subseteq \{1,\ldots,n\}} \Big(P'_M \wedge \bigwedge_{i \in \overline{M}} F_i \Big) \tag{3.3}$$

$$\vdash P_M \wedge \Box I \wedge \bigwedge_{i \in \overline{M}} \neg\Box F_i \rightarrow Q \wedge \bigwedge_{i \in M} \neg\Box F_i \tag{3.4}$$

Section A.4 in the appendix shows that from (3.3) and (3.4) one can derive

$$\vdash Q \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \rightarrow \bigwedge_{i=1}^{n} \Box\neg\Box F_i$$

On the other hand, we obviously have

$$\vdash \mathcal{N} \rightarrow Q \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i$$

which (using (H4)) completes the proof of the lemma.

Proof of assertion (3.3). For every $j \in \{1, \ldots, n\}$, we will prove

$$\vdash \mathcal{N}_j^0 \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \rightarrow \bigvee_{l=1}^{n} \mathcal{N}_l$$

which implies the assertion by the definition of Q, (3.2), and propositional reasoning.

Consider some occurrence of $\mathcal{N}_j$ strictly below $\mathcal{N}$ (such an occurrence must exist by the definition of a saturated subtree), and the parent of $\mathcal{N}_j$ in $\mathcal{T}(\mathcal{F})$; this is then also a node, say $\mathcal{N}_k$, of the saturated subtree, and therefore we have $k \in \mathcal{E}_N$ for some $N \subseteq \{1, \ldots, n\}$. From the definition of $\sigma(\mathcal{N}_k)$, we observe that

$$\sigma(\mathcal{N}_k) = \{v : v' \in \mathcal{N}_k\} \cup \{\neg v : \neg v' \in \mathcal{N}_k\} \cup \mathcal{N}_k^{\Box} \cup \{\neg\Box F_i : i \in \overline{N}\}$$

Besides, we have $\mathcal{N}_j^0 = \{v : v' \in \mathcal{N}_k\} \cup \{\neg v : \neg v' \in \mathcal{N}_k\}$ and therefore

$$\vdash \mathcal{N}_j^0 \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \rightarrow \sigma(\mathcal{N}_k) \tag{3.5}$$

Now consider all children $\mathcal{S}$ of node $\mathcal{N}_k$; these are all different completions of $\sigma(\mathcal{N}_k)$ and are among the nodes of $\mathcal{T}$, and we therefore know

$$\mathcal{S} \rightarrow \bigvee_{l=1}^{n} \mathcal{N}_l$$

for every child $\mathcal{S}$. Proposition 9 implies

$$\sigma(\mathcal{N}_k) \rightarrow \bigvee_{l=1}^{n} \mathcal{N}_l$$

and the assertion follows with (3.5).

Proof of assertion (3.4). For every $j \in \mathcal{E}_M$, we prove

$$\vdash \Box I \wedge \bigwedge_{v' \in \mathcal{N}_j} v \wedge \bigwedge_{v' \in \mathcal{V}^0 \setminus \mathcal{N}_j} \neg v \wedge \bigwedge_{i \in \overline{M}} \neg\Box F_i \rightarrow Q \wedge \bigwedge_{i \in M} \neg\Box F_i$$

The assertion follows by the definition of P_M and propositional reasoning.

By the definition of $\mathcal{E}_M$ and the fact that $\mathcal{N}_j$ is a node of $\mathcal{T}$, we know that $\mathcal{N}_j^{\Diamond} = \{\neg\Box F_1, \ldots, \neg\Box F_n\}$, that $\mathcal{N}_j$ contains the formulas $\neg F_i$ for $i \in M$ and F_i for $i \in \overline{M}$, and that $\mathcal{N}_j^{\Box}$ is provably equivalent to $\Box I$. By the definition of $\sigma(\mathcal{N}_j)$, it follows that

$$\vdash \Box I \wedge \bigwedge_{v' \in \mathcal{N}_j} v \wedge \bigwedge_{v' \in \mathcal{V}^0 \setminus \mathcal{N}_j} \neg v \wedge \bigwedge_{i \in \overline{M}} \neg\Box F_i \;\leftrightarrow\; \sigma(\mathcal{N}_j)$$

Now consider the children of node $\mathcal{N}_j$ in $\mathcal{T}(\mathcal{F})$; these are all different completions of $\sigma(\mathcal{N}_j)$. The valuation of all proposition symbols in $\mathcal{V}^0$ in these children is given by $\sigma(\mathcal{N}_j)$, and because all children are contained in $\mathcal{T}$, the definition of Q implies $\vdash \sigma(\mathcal{N}_j) \to Q$. Moreover, because $\mathcal{T}$ is saturated, we know that all children contain the same eventualities as node $\mathcal{N}_j$; in particular, they all contain $\neg\Box F_i$ for $i \in M$. By proposition 9, we conclude $\vdash \sigma(\mathcal{N}_j) \to \neg\Box F_i$ for every $i \in M$. $\triangleleft$

Lemma 17 *For any finite and consistent set $\mathcal{F}$ of formulas, $\mathcal{T}(\mathcal{F})$ contains an admissible path.*

PROOF We will prove that for every node $\mathcal{N}$ in $\mathcal{T}(\mathcal{F})$ and every formula $\neg\Box F \in \mathcal{N}$ there exists some node $\mathcal{N}'$ below $\mathcal{N}$ in $\mathcal{T}(\mathcal{F})$ such that $\neg F \in \mathcal{N}'$. This assertion inductively guarantees the existence of an admissible path.

Consider any saturated subtree $\mathcal{T}$ of $\mathcal{T}(\mathcal{F})$ below $\mathcal{N}$; we know that such a subtree must exist. Then $\mathcal{T}$ contains only finitely many different nodes $\mathcal{N}_1, \ldots, \mathcal{N}_m$. Without loss of generality, assume that $\mathcal{N}_1$ is the root of the saturated subtree. All nodes $\mathcal{N}_j$ contain the same sets $\mathcal{N}_j^{\Box}$ and $\mathcal{N}_j^{\Diamond}$ of formulas of the form $\Box F$ and $\neg\Box F$, respectively. By (H4), $\mathcal{N}_j^{\Box}$ is equivalent to some formula $\Box I$, and by (LIN), $\mathcal{N}_j^{\Diamond}$ is equivalent to some formula $\neg\Box G$ (see also section A.4 in the appendix for the concrete shape of that formula). If $\neg\Box F$ is not among the formulas in $\mathcal{N}_1^{\Diamond}$, the construction of $\mathcal{T}(\mathcal{F})$ ensures that $\neg F$ must have been contained in some node on the path from $\mathcal{N}$ to $\mathcal{N}_1$ and the assertion is proved.

So assume that $\neg\Box F$ is an element of $\mathcal{N}_1^{\Diamond}$. As in the proof of lemma 16, let $\mathcal{N}_j^0$ denote the valuation of the proposition symbols determined by node $\mathcal{N}_j^0$, and let Q denote the disjunction of all $\mathcal{N}_j^0$. Exactly as in the proof of assertion (3.3), one proves

$$\vdash Q \wedge \Box I \wedge \mathcal{N}_1^{\Diamond} \to Q'$$

which by propositional logic, the definition of G above, and (H3) implies

$$\vdash \Box I \to \Box(Q \wedge \neg Q' \to \Box G)$$

Using the induction axiom (ax8), we conclude

$$\vdash Q \wedge \Box I \to \Box(\neg\Box G \to Q)$$

hence, by axiom (ax1) and the definition of G,

$$\vdash Q \wedge \Box I \wedge \Box\mathcal{N}_1^{\Diamond} \to \Box Q \tag{3.6}$$

On the other hand, lemma 16, the equivalence (H4), the fact that $\mathcal{N}_1^{\Box} \subseteq \mathcal{N}_1$ and $\mathcal{N}_1^0 \subseteq \mathcal{N}_1$, and the definition of Q imply

$$\vdash \mathcal{N}_1 \to Q \wedge \Box I \wedge \Box\mathcal{N}_1^{\Diamond} \tag{3.7}$$

The nodes of $\mathcal{T}$ are all different consistent completions of the sets $\sigma(\mathcal{N}_k) \subseteq \mathcal{N}_k^0 \cup \mathcal{N}_k^\Box \cup \mathcal{N}_k^\Diamond$. If it were the case that $F \in \mathcal{N}_j$ for all nodes $\mathcal{N}_j$ in $\mathcal{T}$, this would by proposition 9 imply

$$\vdash \mathcal{N}_k^0 \wedge \Box I \wedge \mathcal{N}_1^\Diamond \to F$$

for all k, and therefore, using the definition of Q, (H1), (ax3), and (H4),

$$\vdash \Box Q \wedge \Box I \wedge \Box \mathcal{N}_1^\Diamond \to \Box F \tag{3.8}$$

From (3.6), (3.7), and (3.8), we obtain $\vdash \mathcal{N}_1 \to \Box F$, while on the other hand we have $\vdash \mathcal{N}_1 \to \neg\Box F$ by the assumption that $\neg\Box F \in \mathcal{N}_1^\Diamond \subseteq \mathcal{N}_1$. But this means that $\mathcal{N}_1$ is inconsistent, contradicting the definition of $\mathcal{T}(\mathcal{F})$. So we must have $\neg F \in \mathcal{N}_j$ for some node $\mathcal{N}_j$ in $\mathcal{T}$, which proves the assertion. $\lhd$

The completeness result for RTLA is now obtained as a standard corollary.

Theorem 18 *For any* RTLA *formula F, if $\models F$ then $\vdash F$.*

PROOF Assume that $\models F$, and therefore $\neg F$ is unsatisfiable. Then $\mathcal{T}(\neg F)$ cannot contain an admissible path (because by lemma 13 any such path would give rise to an interpretation that satisfied $\neg F$). But then lemma 17 implies that $\{\neg F\}$ must be inconsistent, that is, $\vdash \neg\neg F$, and therefore also $\vdash F$. $\lhd$

Note on the Geach axiom. Σ_{RTLA} contains the axiom (ax5) due to Dummett, Lemmon, and Geach, which is a standard axiom of modal logic to express the discreteness of time. In standard PTL proof systems, discreteness is a consequence of the induction axiom

$$\Box(F \to \bigcirc F) \to (F \to \Box F)$$

(A typical derivation is given by Goldblatt [3].) It seems impossible to find a similarly general finitary induction axiom for RTLA. However, examining the proof of lemma 16 (and, in particular, the derivation of (A.1) in section A.4 in the appendix), we may observe that (ax5) could be replaced by an infinite set of axiom schemes, as follows: For state formulas $P_0, P_1, \ldots$ and arbitrary formula $F_1, F_2, \ldots$, let $\mathcal{F}_i$ denote the formula $P_i \wedge \Diamond F_i$ (or just P_0 for $i = 0$), and $\overline{\mathcal{F}_i}$ denote the formula $P_i' \wedge \neg F_i \wedge \Diamond F_i$ (or just P_0'). We could then replace (ax5) by the set of axioms (ax5'$_n$) for every $n \in \mathbb{N}$:

$$\Box\left(\bigvee_{i=0}^{n} \mathcal{F}_i \to \bigvee_{i=0}^{n} \overline{\mathcal{F}_i}\right) \to \left(\bigvee_{i=0}^{n} \mathcal{F}_i \to \Box \bigvee_{i=0}^{n} \mathcal{F}_i\right)$$

Choosing $P_0 \equiv$ TRUE, (ax5'$_1$) subsumes the induction axiom (IND), and we could therefore suppress (ax8) from Σ_{RTLA} as well.

I do not know if a similar remark applies to the linearity axiom (ax4), which is also a derived theorem in axiom systems for PTL.

Acknowledgement. Martín Abadi made a number of useful comments that helped to improve the exposition of this note.

References

[1] Martín Abadi. An axiomatization of Lamport's Temporal Logic of Actions. In Jos C. M. Baeten and Jan W. Klop, editors, *CONCUR '90, Theories of Concurrency: Unification and Extension*, volume 458 of *Lecture Notes in Computer Science*, pages 57–69, Berlin, 1990. Springer-Verlag. A revised version is available on the Web at http://www.research.digital.com/SRC/personal/Martin_Abadi/allpapers.html.

[2] Dov Gabbay, Amir Pnueli, S. Shelah, and Jonathan Stavi. On the temporal analysis of fairness. In *Proceedings of the 7th Annual ACM Symposium on Principles of Programming Languages*, pages 163–173. ACM, 1980.

[3] Robert Goldblatt. *Logics of Time and Computation*, volume 7 of *CSLI Lecture Notes*. CSLI, Stanford, California, 1987.

[4] G. E. Hughes and M. J. Cresswell. *A New Introduction to Modal Logic*. Routledge, London, 1996.

[5] Fred Kröger. *Temporal Logic of Programs*, volume 8 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1987.

[6] Leslie Lamport. The Temporal Logic of Actions. *ACM Transactions on Programming Languages and Systems*, 16(3):872–923, May 1994.

[7] Zohar Manna and Amir Pnueli. *The temporal logic of reactive and concurrent systems—Specification*. Springer-Verlag, New York, 1992.

A Derivations

A.1 Auxiliary formulas

This section contains derivations for the consequences of Σ_{RTLA} listed in figure 2.

(H1) $F \to G \vdash \Box F \to \Box G$

(1)	$F \to G$	(assumption)
(2)	$\Box(F \to G)$	(alw)(1)
(3)	$\Box(F \to G) \to (\Box F \to \Box G)$	(ax1)
(4)	$\Box F \to \Box G$	(mp)(2)(3)

(H2) $F \to G \vdash \Diamond F \to \Diamond G$

(1)	$F \to G$	(assumption)
(2)	$\neg G \to \neg F$	(1)
(3)	$\Box\neg G \to \Box\neg F$	(H1)(2)
(4)	$\Diamond F \to \Diamond G$	(3)

(H3) $\Box F \to G \vdash \Box F \to \Box G$

(1)	$\Box F \to G$	(assumption)
(2)	$\Box\Box F \to \Box G$	(H1)(1)
(3)	$\Box F \to \Box\Box F$	(ax3)
(4)	$\Box F \to \Box G$	(2)(3)

(H4) $\Box F \wedge \Box G \ \leftrightarrow\ \Box(F \wedge G)$

(1)	$F \to (G \to F \wedge G)$	(ax0)
(2)	$\Box F \to \Box(G \to F \wedge G)$	(H1)(1)
(3)	$\Box(G \to F \wedge G) \to (\Box G \to \Box(F \wedge G))$	(ax1)
(4)	$\Box F \wedge \Box G \to \Box(F \wedge G)$	(2)(3)
(5)	$F \wedge G \to F$	(ax0)
(6)	$\Box(F \wedge G) \to \Box F$	(H1)(5)
(7)	$F \wedge G \to G$	(ax0)
(8)	$\Box(F \wedge G) \to \Box G$	(H1)(7)
(9)	$\Box F \wedge \Box G \ \leftrightarrow\ \Box(F \wedge G)$	(4)(6)(8)

(H5) $\Diamond F \wedge \Box G \to \Diamond(F \wedge \Box G)$

(1)	$\Box G \wedge (\Box G \to \neg F) \to \neg F$	(ax0)
(2)	$\Box(\Box G \wedge (\Box G \to \neg F)) \to \Box\neg F$	(H1)(1)
(3)	$\Box\Box G \wedge \Box(\Box G \to \neg F) \to \Box\neg F$	(H4)(2)
(4)	$\Box G \to \Box\Box G$	(ax3)
(5)	$\Box G \wedge \Box(\Box G \to \neg F) \to \Box\neg F$	(4)(3)
(6)	$\Diamond F \wedge \Box G \to \Diamond\neg(\Box G \to \neg F)$	(5)
(7)	$\neg(\Box G \to \neg F) \to F \wedge \Box G$	(ax0)
(8)	$\Diamond\neg(\Box G \to \neg F) \to \Diamond(F \wedge \Box G)$	(H2)(7)
(9)	$\Diamond F \wedge \Box G \to \Diamond(F \wedge \Box G)$	(6)(9)

(H6) $\Diamond\Box F \wedge \Diamond\Box G \;\leftrightarrow\; \Diamond\Box(F \wedge G)$

(1)	$\Diamond\Box F \wedge \Box(\Box F \to G) \to \Diamond(\Box F \wedge \Box(\Box F \to G))$	(H5)
(2)	$\Box F \wedge \Box(\Box F \to G) \to \Box(\Box F \wedge (\Box F \to G))$	(ax3)(H4)
(3)	$\Diamond(\Box F \wedge \Box(\Box F \to G)) \to \Diamond\Box(\Box F \wedge (\Box F \to G))$	(H2)(2)
(4)	$\Box F \wedge (\Box F \to G) \to F \wedge G$	(ax2)
(5)	$\Diamond\Box(\Box F \wedge (\Box F \to G)) \to \Diamond\Box(F \wedge G)$	(H1)(H2)(4)
(6)	$\Diamond\Box F \wedge \Box(\Box F \to G) \to \Diamond\Box(F \wedge G)$	(1)(5)
(7)	$\Diamond\Box G \wedge \Box(\Box G \to F) \to \Diamond\Box(F \wedge G)$	(similar)
(8)	$\Diamond\Box F \wedge \Diamond\Box G \wedge (\Box(\Box F \to G) \vee \Box(\Box G \to F))$	
	$\to \Diamond\Box(F \wedge G)$	(6)(7)
(9)	$\Box(\Box F \to G) \vee \Box(\Box G \to F)$	(ax4)
(10)	$\Diamond\Box F \wedge \Diamond\Box G \to \Diamond\Box(F \wedge G)$	(8)(9)
(11)	$F \wedge G \to F$	(ax0)
(12)	$\Diamond\Box(F \wedge G) \to \Diamond\Box F$	(H2)(H1)(11)
(13)	$F \wedge G \to G$	(ax0)
(14)	$\Diamond\Box(F \wedge G) \to \Diamond\Box G$	(H2)(H1)(13)
(15)	$\Diamond\Box(F \wedge G) \;\leftrightarrow\; \Diamond\Box F \wedge \Diamond\Box G$	(10)(12)(14)

(H7) $\Box\Diamond F \;\leftrightarrow\; \Diamond\Box\Diamond F$

(1)	$\Box\Diamond F \to \Diamond\Box\Diamond F$	(ax2)(dual)
(2)	$\Box\neg F \to \Box\Box\neg F$	(ax3)
(3)	$\Diamond\Box\neg F \to \Diamond\Box\Box\neg F$	(H2)(2)
(4)	$\Diamond\Box\Diamond F \wedge \Diamond\Box\Box\neg F \to \Diamond\Box(\Diamond F \wedge \Box\neg F)$	(H6)
(5)	$\neg(\Diamond F \wedge \Box\neg F)$	(ax0)
(6)	$\Box(\Diamond F \wedge \Box\neg F) \to (\Diamond F \wedge \Box\neg F)$	(ax2)
(7)	$\neg\Box(\Diamond F \wedge \Box\neg F)$	(5)(6)
(8)	$\Box\neg\Box(\Diamond F \wedge \Box\neg F)$	(alw)(7)
(9)	$\Diamond\Box\Diamond F \to \neg\Diamond\Box\neg F$	(8)(4)(3)
(10)	$\Box\Diamond F \;\leftrightarrow\; \Diamond\Box\Diamond F$	(1)(9)

(H8) $P \wedge \Box(P \to P') \;\leftrightarrow\; \Box P$

(1)	$(P \to P') \to (P \to (\neg P' \to \Box P))$	(ax0)
(2)	$\Box(P \to P') \to \Box(P \to (\neg P' \to \Box P))$	(H1)(1)
(3)	$\Box(P \to (\neg P' \to \Box P)) \to (P \to \Box(\neg P \to \Box P))$	(ax8)
(4)	$\Box P \to P$	(ax2)
(5)	$(\neg P \to \Box P) \to (\neg P \to P)$	(4)
(6)	$(\neg P \to \Box P) \to P$	(5)
(7)	$\Box(\neg P \to \Box P) \to \Box P$	(H1)(6)
(8)	$\Box(P \to P') \to (P \to \Box P)$	(2)(3)(7)
(9)	$\Box P \to P'$	(ax6)
(10)	$\Box P \to \Box P'$	(H3)(9)
(11)	$P' \to (P \to P')$	(ax0)
(12)	$\Box P' \to \Box(P \to P')$	(H1)(11)
(13)	$P \wedge \Box(P \to P') \;\leftrightarrow\; \Box P$	(8)(4)(10)(12)

(H9) $\Box P \;\leftrightarrow\; P \wedge \Box P'$

(1)	$\Box P \to P$	(ax2)
(2)	$\Box P \to \Box P'$	(H3)(ax6)
(3)	$P' \to (P \to P')$	(ax0)
(4)	$\Box P' \to \Box(P \to P')$	(H1)(3)
(5)	$P \wedge \Box(P \to P') \to \Box P$	(H8)
(6)	$\Box P \;\leftrightarrow\; P \wedge \Box P'$	(1)(2)(4)(5)

(H10) $P \to \Box Q \vdash P' \to \Box Q'$

(1)	$P \to \Box Q$	(assumption)
(2)	$\Box Q \to \Box Q'$	(H9)
(3)	$P \to \Box Q'$	(1)(2)
(4)	$\Box(P \to \Box Q')$	(alw)(3)
(5)	$P' \to (Q' \to \Box Q')$	(4)(ax7)
(6)	$\Box Q \to Q$	(ax2)
(7)	$P \to Q$	(1)(6)
(8)	$\Box(P \to Q)$	(alw)(7)
(9)	$P' \to Q'$	(8)(ax6)
(10)	$P' \to \Box Q'$	(5)(9)

(H11) $P \to \Diamond Q \vdash P' \to \Diamond Q'$

(1)	$P \to \Diamond Q$	(assumption)
(2)	$P \to Q \vee \Diamond Q'$	(1)(H9)(dual)
(3)	$\Box\neg Q' \to (P \to Q)$	(2)
(4)	$\Box\neg Q' \to \Box(P \to Q)$	(H3)(3)
(5)	$\Box\neg Q' \to (P' \to Q')$	(4)(ax6)
(6)	$P' \wedge \Box\neg Q' \to \Diamond Q'$	(5)(ax2)(dual)
(7)	$P' \to \Diamond Q'$	(6)

(H12) $P \wedge P' \to F \vdash \Box P \to \Box F$

(1)	$P \wedge P' \to F$	(assumption)
(2)	$\Box(P \wedge P') \to \Box F$	(H1)(1)
(3)	$\Box P \wedge \Box P' \to \Box F$	(H4)(2)
(4)	$\Box P \to \Box F$	(H9)(3)

(H13) $\Box\Diamond P \leftrightarrow \Box\Diamond P'$

(1)	$\Diamond P' \to \Diamond P$	(H9)(dual)
(2)	$\Box\Diamond P' \to \Box\Diamond P$	(H1)(1)
(3)	$\Box\Diamond P \wedge \Diamond\Box\neg P' \to \Diamond(\Box\Diamond P \wedge \Box\neg P')$	(H5)
(4)	$\Diamond P \wedge \Box\neg P' \to P$	(H9)(dual)
(5)	$\Box(\Diamond P \wedge \Box\neg P') \to \Box P$	(H1)(4)
(6)	$\Box\Diamond P \wedge \Box\neg P' \to \Box P$	(5)(H4)(ax3)
(7)	$\Box P \to \Box P'$	(H9)
(8)	$\Diamond(\Box\Diamond P \wedge \Box\neg P') \to \Diamond\Box P'$	(6)(7)(H2)
(9)	$P' \to \Diamond P'$	(ax2)(dual)
(10)	$\Diamond\Box P' \to \Diamond\Box\Diamond P'$	(H1)(H2)(9)
(11)	$\Diamond\Box\Diamond P' \leftrightarrow \Box\Diamond P'$	(H7)
(12)	$\Box\Diamond P \wedge \Diamond\Box\neg P' \to \Box\Diamond P'$	(3)(8)(10)(11)
(13)	$\Box\Diamond P \leftrightarrow \Box\Diamond P'$	(12)(2)

(H14) $P \to \Diamond P' \vdash P \to \Box\Diamond P$

(1)	$P \to \Diamond P'$	(assumption)
(2)	$\Box(\neg P \to \Box\neg P) \to (\neg P' \to \Box\neg P')$	(H10)(thm.2)
(3)	$(\neg P' \to \Box\neg P') \to (\Diamond P' \to P')$	(ax0)
(4)	$\Box(\neg P \to \Box\neg P) \to (P \to P')$	(2)(3)(1)
(5)	$\Box(\neg P \to \Box\neg P) \to \Box(P \to P')$	(H3)(4)
(6)	$\Box(\neg P \to \Box\neg P) \to (P \to \Box P)$	(5)(H8)
(7)	$\neg\Box P \to (\Box(\neg P \to \Box\neg P) \to \neg P)$	(6)
(8)	$\Box\neg\Box P \to \Box(\Box(\neg P \to \Box\neg P) \to \neg P)$	(H1)(7)
(9)	$\Box\neg\Box P \to (\Diamond\Box\neg P \to \neg P)$	(8)(ax5)
(10)	$\Box\neg\Box P \to (P \to \Box\Diamond P)$	(9)
(11)	$P \to \Diamond P$	(ax2)(dual)
(12)	$\Diamond\Box P \to \Diamond\Box\Diamond P$	(H1)(H2)(11)
(13)	$\Diamond\Box P \to \Box\Diamond P$	(12)(H7)
(14)	$P \to \Box\Diamond P$	(10)(13)

A.2 Axioms for linearity

We show that axiom (ax4) of Σ_{RTLA} could equivalently be replaced by

$$\text{(LIN)} \qquad \Diamond F \wedge \Diamond G \to \Diamond(F \wedge \Diamond G) \vee \Diamond(G \wedge \Diamond F)$$

in any extension of system K of normal modal logic. The first derivation shows that (LIN) follows from (ax4) in system K. Observe that (H1) can be derived in K and is, in particular, independent of axiom (ax4):

(1)	$\Box(\Box\neg G \to \neg F) \vee \Box(\Box\neg F \to \neg G)$	(ax4)
(2)	$(F \to \Box\neg G) \to ((\Box\neg G \to \neg F) \to \neg F)$	(ax0)
(3)	$\Box(F \to \Box\neg G) \to (\Box(\Box\neg G \to \neg F) \to \Box\neg F)$	(2)(H1)(ax1)
(4)	$(G \to \Box\neg F) \to ((\Box\neg F \to \neg G) \to \neg G)$	(ax0)
(5)	$\Box(G \to \Box\neg F) \to (\Box(\Box\neg F \to \neg G) \to \Box\neg G)$	(4)(H1)(ax1)
(6)	$\Box(F \to \Box\neg G) \wedge \Box(G \to \Box\neg F)$	
	$\quad \wedge\ (\Box(\Box\neg G \to \neg F) \vee \Box(\Box\neg F \to \neg G))$	
	$\to\ \Box\neg F \vee \Box\neg G$	(3)(5)
(7)	$\Box(F \to \Box\neg G) \wedge \Box(G \to \Box\neg F) \to \Box\neg F \vee \Box\neg G$	(6)(1)
(8)	$\Diamond F \wedge \Diamond G \to \Diamond(F \wedge \Diamond G) \vee \Diamond(G \wedge \Diamond F)$	(7)

The converse derivation shows that (ax4) follows from (LIN) in system K.

(1)	$\Diamond(\Box F \wedge \neg G) \wedge \Diamond(\Box G \wedge \neg F)$	
	$\to \quad \Diamond(\Box F \wedge \neg G \wedge \Diamond(\Box G \wedge \neg F))$	
	$\quad \vee\ \Diamond(\Box G \wedge \neg F \wedge \Diamond(\Box F \wedge \neg G))$	(LIN)
(2)	$F \to \neg(\Box G \wedge \neg F)$	(ax0)
(3)	$\Box F \to \Box\neg(\Box G \wedge \neg F)$	(H1)(2)
(4)	$\neg(\Box F \wedge \neg G \wedge \Diamond(\Box G \wedge \neg F))$	(3)
(5)	$\Box\neg(\Box F \wedge \neg G \wedge \Diamond(\Box G \wedge \neg F))$	(alw)(4)
(6)	$G \to \neg(\Box F \wedge \neg G)$	(ax0)
(7)	$\Box G \to \Box\neg(\Box F \wedge \neg G)$	(H1)(6)
(8)	$\neg(\Box G \wedge \neg F \wedge \Diamond(\Box F \wedge \neg G))$	(7)
(9)	$\Box\neg(\Box G \wedge \neg F \wedge \Diamond(\Box F \wedge \neg G))$	(alw)(8)
(10)	$\Diamond(\Box F \wedge \neg G) \to \neg\Diamond(\Box G \wedge \neg F)$	(1)(5)(9)
(11)	$\Box(\Box F \to G) \vee \Box(\Box G \to F)$	(10)

A.3 Induction axioms

We show that axiom (ax8) from figure 1 could be replaced by

$$\text{(IND)} \qquad \Box(P \to (P' \wedge F) \vee \Box F) \to (P \to \Box F)$$

For the derivation of (IND) from (ax8), it suffices by theorem 2 to prove

$$P \to (P' \wedge F) \vee \Box F \vdash P \to \Box F$$

(1)	$P \to (P' \wedge F) \vee \Box F$	(assumption)
(2)	$\Box F \to F$	(ax2)
(3)	$P \to F$	(1)(2)
(4)	$\Box(P \to F)$	(alw)(3)
(5)	$P \wedge \neg P' \to \Box F$	(1)
(6)	$P \to \Box(\neg P \to \Box F)$	(alw)(5)(ax8)
(7)	$(P \to F) \wedge (\neg P \to \Box F) \to F$	(2)
(8)	$\Box((P \to F) \wedge (\neg P \to \Box F)) \to \Box F$	(H1)(7)
(9)	$\Box(P \to F) \wedge \Box(\neg P \to \Box F) \to \Box F$	(8)(H4)
(10)	$P \to \Box F$	(4)(6)(9)

Similarly, for the converse derivation, it suffices to prove

$$P \wedge \neg P' \to \Box F \vdash P \to \Box(\neg P \to \Box F)$$

using (IND) as an additional axiom, because theorem 2 could also be proved for a proof system similar to Σ_{RTLA}, but with (IND) instead of (ax8). Note that (H3) may be used in this derivation because its proof does not require (ax8).

(1)	$P \wedge \neg P' \to \Box F$	(assumption)
(2)	$\Box F \to (\neg P \to \Box F)$	(ax0)
(3)	$\Box F \to \Box(\neg P \to \Box F)$	(H3)(2)
(4)	$P \wedge \neg\Box(\neg P \to \Box F) \to P'$	(1)(3)
(5)	$P \wedge \neg\Box(\neg P \to \Box F) \to (\neg P \to \Box F)$	(ax0)
(6)	$P \to (P' \wedge (\neg P \to \Box F)) \vee \Box(\neg P \to \Box F)$	(4)(5)
(7)	$P \to \Box(\neg P \to \Box F)$	(alw)(6)(IND)

A.4 An auxiliary induction rule

In this section, we derive a rule used in the proof of lemma 16: Let $I, F_1, \ldots, F_n$ be formulas, and Q and P_M (for every set $M \subseteq \{1, \ldots, n\}$) be state formulas. Then the following rule is derivable:

$$\frac{\begin{array}{c} Q \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \to \bigvee_{M \subseteq \{1,\ldots,n\}} \Big(P'_M \wedge \bigwedge_{i \in \overline{M}} F_i\Big) \\ P_M \wedge \Box I \wedge \bigwedge_{i \in \overline{M}} \neg\Box F_i \to Q \wedge \bigwedge_{i \in M} \neg\Box F_i \quad \text{for every } M \subseteq \{1, \ldots, n\} \end{array}}{Q \wedge \Box I \wedge \bigwedge_{i=1}^{n} \neg\Box F_i \to \bigwedge_{i=1}^{n} \Box\neg\Box F_i} \tag{A.1}$$

(where $\overline{M}$ denotes the set $\{1, \ldots, n\} \setminus M$). We begin by deriving some auxiliary rules. Rule (H15) generalizes axiom (DISC), the dual version of the Geach axiom (ax5); rule (H16) is a simple consequence of (H15).

(H15) $P \wedge \Diamond G \to \Diamond(P' \wedge \neg G \wedge \Diamond G) \vdash P \wedge \Diamond G \to \Box\Diamond(P \wedge \Diamond G)$

(1)	$P \wedge \Diamond G \to \Diamond(P' \wedge \neg G \wedge \Diamond G)$	(assumption)
(2)	$\Box(P \wedge \Diamond G \to P' \wedge \neg G) \to (P \to \Box\neg G)$	(IND)
(3)	$P \wedge \Diamond G \to \Diamond(P \wedge \Diamond G \wedge \neg(P' \wedge \neg G))$	(2)
(4)	$\neg(P' \wedge \neg G) \wedge P \wedge \Diamond G$ $\to \neg(P' \wedge \neg G \wedge \Diamond G) \wedge \Diamond(P' \wedge \neg G \wedge \Diamond G)$	(1)
(5)	$\Diamond(\neg(P' \wedge \neg G) \wedge P \wedge \Diamond G)$ $\to \Diamond(\neg(P' \wedge \neg G \wedge \Diamond G) \wedge \Diamond(P' \wedge \neg G \wedge \Diamond G))$	(H2)(4)
(6)	$P \wedge \Diamond G$ $\to \Diamond(\neg(P' \wedge \neg G \wedge \Diamond G) \wedge \Diamond(P' \wedge \neg G \wedge \Diamond G))$	(3)(5)
(7)	$\Diamond(P \wedge \Diamond G)$ $\to \Diamond(\neg(P' \wedge \neg G \wedge \Diamond G) \wedge \Diamond(P' \wedge \neg G \wedge \Diamond G))$	(H2)(6)(ax3)
(8)	$P' \wedge \neg G \wedge \Diamond G \to \Diamond(P \wedge \Diamond G)$	(ax7)(dual)
(9)	$P' \wedge \neg G \wedge \Diamond G$ $\to \Diamond(\neg(P' \wedge \neg G \wedge \Diamond G) \wedge \Diamond(P' \wedge \neg G \wedge \Diamond G))$	(8)(7)
(10)	$P' \wedge \neg G \wedge \Diamond G \to \Box\Diamond(P' \wedge \neg G \wedge \Diamond G)$	(DISC)(thm. 2)(9)
(11)	$\Diamond(P' \wedge \neg G \wedge \Diamond G) \to \Box\Diamond(P' \wedge \neg G \wedge \Diamond G)$	(H2)(10)(H7)
(12)	$\Box\Diamond(P' \wedge \neg G \wedge \Diamond G) \to \Box\Diamond(P \wedge \Diamond G)$	(H1)(H2)(8)(ax3)
(13)	$P \wedge \Diamond G \to \Box\Diamond(P \wedge \Diamond G)$	(1)(11)(13)

(H16) $P \wedge \Diamond G \to F \vdash F \wedge \Box(F \to \Diamond(P' \wedge \neg G \wedge \Diamond G)) \to \Box\Diamond F$

By theorem 2, it suffices to derive

$$P \wedge \Diamond G \to F, F \to \Diamond(P' \wedge \neg G \wedge \Diamond G) \vdash F \to \Box\Diamond F$$

(1)	$P \wedge \Diamond G \to F$	(assumption)
(2)	$F \to \Diamond(P' \wedge \neg G \wedge \Diamond G)$	(assumption)
(3)	$P \wedge \Diamond G \to \Diamond(P' \wedge \neg G \wedge \Diamond G)$	(1)(2)
(4)	$P \wedge \Diamond G \to \Box\Diamond(P \wedge \Diamond G)$	(H15)(3)
(5)	$\Diamond(P \wedge \Diamond G) \to \Box\Diamond(P \wedge \Diamond G)$	(H2)(4)(H7)
(6)	$P' \wedge \neg G \wedge \Diamond G \to \Diamond(P \wedge \Diamond G)$	(ax7)(dual)
(7)	$\Diamond(P' \wedge \neg G \wedge \Diamond G) \to \Diamond(P \wedge \Diamond G)$	(H2)(6)(ax3)
(8)	$\Box\Diamond(P \wedge \Diamond G) \to \Box\Diamond F$	(H1)(H2)(1)
(9)	$F \to \Box\Diamond F$	(2)(7)(5)(8)

The following theorem (H17) shows how conjunction distributes over $\Box\Diamond$:

(H17) $\Box\Diamond A \wedge \Box\Diamond B \leftrightarrow \Box\Diamond(\Diamond A \wedge \Diamond B)$

(1)	$\Diamond A \wedge \Diamond B \rightarrow \Diamond(\Diamond A \wedge \Diamond B)$	(ax2)
(2)	$\Box(\Diamond A \wedge \Diamond B) \rightarrow \Box\Diamond(\Diamond A \wedge \Diamond B)$	(H1)(1)
(3)	$\Box\Diamond A \wedge \Box\Diamond B \rightarrow \Box\Diamond(\Diamond A \wedge \Diamond B)$	(2)(H4)
(4)	$\Diamond A \wedge \Diamond B \rightarrow \Diamond A$	(ax0)
(5)	$\Box\Diamond(\Diamond A \wedge \Diamond B) \rightarrow \Box\Diamond A$	(H1)(H2)(4)(ax3)
(6)	$\Box\Diamond(\Diamond A \wedge \Diamond B) \rightarrow \Box\Diamond B$	(similar)
(7)	$\Box\Diamond A \wedge \Box\Diamond B \leftrightarrow \Box\Diamond(\Diamond A \wedge \Diamond B)$	(3)(5)(6)

For $k \geq 1$, let K denote the set $\{1, \ldots, k\}$ and let $G_1, \ldots, G_k$ be formulas. We prove the equivalences

$$\bigwedge_{i=1}^{k} \Diamond G_i \quad \leftrightarrow \quad \Diamond \underbrace{\bigvee_{\emptyset \neq N \subseteq K} \left(\bigwedge_{j \in N} G_j \wedge \bigwedge_{j \in K \setminus N} (\neg G_j \wedge \Diamond G_j) \right)}_{\mathcal{G}_k} \tag{A.2}$$

$$\neg \mathcal{G}_k \wedge \Diamond \mathcal{G}_k \quad \leftrightarrow \quad \bigwedge_{i=1}^{k} (\neg G_i \wedge \Diamond G_i) \tag{A.3}$$

In particular, (A.2) shows that a conjunction of formulas $\Diamond G_i$ can be replaced by a single (more complex) formula $\Diamond \mathcal{G}$.

As a first step in the proof of (A.2) and (A.3), we show that (A.3) follows from (A.2), for any $k \geq 1$. In particular, we may use instances of (A.3) for $k' < k$ in the induction step for the proof of (A.2).

$$\begin{array}{lll}
& \Diamond \mathcal{G}_k \wedge \neg \mathcal{G}_k & \\
\leftrightarrow & \displaystyle\bigwedge_{i=1}^{k} \Diamond G_i \wedge \bigwedge_{\emptyset \neq N \subseteq K} \left(\neg \Big(\bigwedge_{j \in N} G_j \Big) \vee \neg \bigwedge_{j \in K \setminus N} (\neg G_j \wedge \Diamond G_j) \right) & (A.2), \text{def. } \mathcal{G}_k \\
\leftrightarrow & \displaystyle\bigwedge_{i=1}^{k} \Diamond G_i \wedge \bigwedge_{\emptyset \neq N \subseteq K} \left(\Big(\bigwedge_{j \in N} G_j \Big) \rightarrow \bigvee_{j \in K \setminus N} G_j \right) & \text{prop. logic} \\
\leftrightarrow & \displaystyle\bigwedge_{i=1}^{k} (\Diamond G_i \wedge \neg G_i) & \leftarrow\text{: tautology, } \rightarrow\text{: choose } N = K
\end{array}$$

The proof of (A.2) is by induction on k. For $k = 1$, the assertion is trivial. For $k > 1$, we let K^- denote the set $\{1, \ldots, k-1\}$ and reason as follows:

$$
\begin{array}{lll}
& \Diamond G_k \wedge \bigwedge_{i=1}^{k-1} \Diamond G_i & \\
\leftrightarrow & \Diamond G_k \wedge \Diamond \mathcal{G}_{k-1} & \text{(ind. hypothesis)} \\
\leftrightarrow & \Diamond (G_k \wedge \Diamond \mathcal{G}_{k-1}) \vee \Diamond (\mathcal{G}_{k-1} \wedge \Diamond G_k) & \text{(LIN)} \\
\leftrightarrow & \vee\, \Diamond (G_k \wedge (\mathcal{G}_{k-1} \vee \neg \mathcal{G}_{k-1}) \wedge \Diamond \mathcal{G}_{k-1}) & \\
& \vee\, \Diamond (\mathcal{G}_{k-1} \wedge (G_k \vee \neg G_k) \wedge \Diamond G_k) & \\
\leftrightarrow & \vee\, \Diamond ((G_k \wedge \mathcal{G}_{k-1}) \vee (G_k \wedge \neg \mathcal{G}_{k-1} \wedge \Diamond \mathcal{G}_{k-1})) & \\
& \vee\, \Diamond ((\mathcal{G}_{k-1} \wedge G_k) \vee (\mathcal{G}_{k-1} \wedge \neg G_k \wedge \Diamond G_k)) & \text{by the dual of (ax2)} \\
\leftrightarrow & \Diamond \big(\vee\, (G_k \wedge \mathcal{G}_{k-1}) & \\
& \quad \vee\, (G_k \wedge \neg \mathcal{G}_{k-1} \wedge \Diamond \mathcal{G}_{k-1}) & \\
& \quad \vee\, (\mathcal{G}_{k-1} \wedge \neg G_k \wedge \Diamond G_k) \big) & \text{by the dual of (H4)} \\
\leftrightarrow & \Diamond \Bigg(\vee \bigvee_{\emptyset \neq N \subseteq K^-} G_k \wedge \bigwedge_{j \in N} G_j \wedge \bigwedge_{j \in K^- \setminus N} (\neg G_j \wedge \Diamond G_j) & \\
& \quad \vee\, G_k \wedge \bigwedge_{j=1}^{k-1} (\neg G_j \wedge \Diamond G_j) & \\
& \quad \vee \bigvee_{\emptyset \neq N \subseteq K^-} \bigwedge_{j \in N} G_j \wedge (\neg G_k \wedge \Diamond G_k) & \\
& \qquad\qquad \wedge \bigwedge_{j \in K^- \setminus N} (\neg G_j \wedge \Diamond G_j) \Bigg) & \text{def. } \mathcal{G}_{k-1}\text{, (A.3)} \\
\leftrightarrow & \Diamond \bigvee_{\emptyset \neq N \subseteq K} \Bigg(\bigwedge_{j \in N} G_j \wedge \bigwedge_{j \in K \setminus N} (\neg G_j \wedge \Diamond G_j) \Bigg) & \text{prop. logic,(H2)}
\end{array}
$$

We now turn to the proof of rule (A.1). We will actually derive the slightly simplified rule

$$
\frac{\begin{array}{c} Q \wedge \bigwedge_{i=1}^{n} \Diamond F_i \rightarrow \bigvee_{M \subseteq \{1,\ldots,n\}} \Big(P'_M \wedge \bigwedge_{i \in \overline{M}} \neg F_i \Big) \\ P_M \wedge \bigwedge_{i \in \overline{M}} \Diamond F_i \rightarrow Q \wedge \bigwedge_{i \in M} \Diamond F_i \qquad \text{for every } M \subseteq \{1, \ldots, n\} \end{array}}{Q \wedge \bigwedge_{i=1}^{n} \Diamond F_i \rightarrow \bigwedge_{i=1}^{n} \Box \Diamond F_i} \tag{A.4}
$$

where we have omitted formula $\Box I$ and have substituted $\neg F_i$ for F_i. Rule (A.1) follows from (A.4) by theorem 2 and simple temporal reasoning.

(A.2) and (A.3) show that for every nonempty set $M \subseteq \{1, \ldots, n\}$ there exists a formula $\mathcal{F}_M$ such that

$$
\vdash \Diamond \mathcal{F}_M \ \leftrightarrow\ \textstyle\bigwedge_{i \in M} \Diamond F_i \tag{A.5}
$$

$$
\text{and} \qquad \vdash (\neg \mathcal{F}_M \wedge \Diamond \mathcal{F}_M) \ \leftrightarrow\ \textstyle\bigwedge_{i \in M} (\neg F_i \wedge \Diamond F_i) \tag{A.6}
$$

Writing $\mathcal{F}$ for $Q \wedge \Diamond\mathcal{F}_{\{1,\ldots,n\}}$, we can restate the premises of (A.4) as

$$\mathcal{F} \to \bigvee_{M\subseteq\{1,\ldots,n\}} \Big(P'_M \wedge \bigwedge_{i\in\overline{M}} \neg F_i\Big) \tag{A.7}$$

and

$$P_M \wedge \Diamond\mathcal{F}_{\overline{M}} \to \mathcal{F} \tag{A.8}$$

(where (A.8) holds for every $M \subseteq \{1,\ldots,n\}$ such that $\overline{M} \neq \emptyset$). From (A.8), (H16), and (A.6), we derive

$$\mathcal{F} \wedge \Diamond\Box\neg\mathcal{F} \to \Diamond(\mathcal{F} \wedge \neg\Diamond(P'_M \wedge \bigwedge_{i\in\overline{M}} \neg F_i \wedge \Diamond F_i)) \tag{A.9}$$

for every set $M \subseteq \{1,\ldots,n\}$ such that $\overline{M} \neq \emptyset$, which, by the definition of $\mathcal{F}$ and simple temporal reasoning, implies

$$\mathcal{F} \wedge \Diamond\Box\neg\mathcal{F} \to \Diamond(\mathcal{F} \wedge \Box(\mathcal{F} \to \neg(P'_M \wedge \bigwedge_{i\in\overline{M}} \neg F_i))) \tag{A.10}$$

From (A.10) and (A.7), an inductive argument establishes

$$\mathcal{F} \wedge \Diamond\Box\neg\mathcal{F} \to \Diamond(\mathcal{F} \wedge \Box(\mathcal{F} \to P'_{\{1,\ldots,n\}})) \tag{A.11}$$

Now, the second premise of (A.4) for $M = \{1,\ldots,n\}$ reads $P_{\{1,\ldots,n\}} \to \mathcal{F}$, and we continue our derivation as follows:

(1)	$\mathcal{F} \wedge \Diamond\Box\neg\mathcal{F} \to \Diamond(\mathcal{F} \wedge \Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}))$	(A.11)
(2)	$P_{\{1,\ldots,n\}} \to \mathcal{F}$	(assumption)
(3)	$\Box(P_{\{1,\ldots,n\}} \to \mathcal{F})$	(alw)(2)
(4)	$\Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}) \to \Box(P_{\{1,\ldots,n\}} \to P'_{\{1,\ldots,n\}})$	(3)
(5)	$\Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}) \to (P_{\{1,\ldots,n\}} \to \Box P_{\{1,\ldots,n\}})$	(4)(INV1)
(5)	$\Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}) \to (P_{\{1,\ldots,n\}} \to \Box\mathcal{F})$	(5)(2)(H1)
(6)	$\Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}) \to \Box(P_{\{1,\ldots,n\}} \to \Box\mathcal{F})$	(H3)(5)
(7)	$\Box(\mathcal{F} \to P'_{\{1,\ldots,n\}}) \to (\mathcal{F} \to \Box\mathcal{F})$	(6)(ax7)(ax2)
(8)	$\Diamond(\mathcal{F} \wedge \Box(\mathcal{F} \to P'_{\{1,\ldots,n\}})) \to \Diamond\Box\mathcal{F}$	(H2)(7)
(9)	$\Diamond\Box\mathcal{F} \to \Box\Diamond\mathcal{F}$	from (H6)
(10)	$\mathcal{F} \wedge \Diamond\Box\neg\mathcal{F} \to \Box\Diamond\mathcal{F}$	(1)(8)(9)
(11)	$\mathcal{F} \to \Box\Diamond\mathcal{F}$	(10)

From the definition of $\mathcal{F}$ and (A.5), (ax3), (H1), and (H2), we have

$$\Box\Diamond\mathcal{F} \to \Box\Diamond \bigwedge_{i=1}^{n} \Diamond F_i \tag{A.12}$$

and an inductive argument based on (H17) shows

$$\Box\Diamond \bigwedge_{i=1}^{n} \Diamond F_i \leftrightarrow \bigwedge_{i=1}^{n} \Box\Diamond F_i$$

which completes the proof of (A.4).