Chapter 14
Temporal Logic: A Deductive System

This chapter defines the deductive system $\mathscr{L}$ for linear temporal logic. We will prove many of the formulas presented in the previous chapter, as well as the soundness and completeness of $\mathscr{L}$.

14.1 Deductive System $\mathscr{L}$

The operators of $\mathscr{L}$ are the Boolean operators of propositional logic together with the temporal operators $\square$ and $\bigcirc$. The operator $\Diamond$ is defined as an abbreviation for $\neg \square \neg$.

Definition 14.1 The axioms of $\mathscr{L}$ are:

Axiom 0	**Prop**	Any substitution instance of a valid propositional formula.
Axiom 1	**Distribution of $\square$**	$\vdash \square(A \to B) \to (\square A \to \square B)$.
Axiom 2	**Distribution of $\bigcirc$**	$\vdash \bigcirc(A \to B) \to (\bigcirc A \to \bigcirc B)$.
Axiom 3	**Expansion of $\square$**	$\vdash \square A \to (A \wedge \bigcirc A \wedge \bigcirc \square A)$.
Axiom 4	**Induction**	$\vdash \square(A \to \bigcirc A) \to (A \to \square A)$.
Axiom 5	**Linearity**	$\vdash \bigcirc A \leftrightarrow \neg \bigcirc \neg A$.

The rules of inference are ***modus ponens*** and ***generalization***: $\dfrac{\vdash A}{\vdash \square A}$. ∎

In order to simplify proofs of formulas in LTL, the deductive system $\mathscr{L}$ takes all substitution instances of valid formulas of propositional logic as axioms. Validity in propositional logic is decidable and by the completeness of $\mathscr{H}$ we can produce a proof of any valid formula if asked to do so. In fact, we will omit justifications of deductions in propositional logic and just write *Prop* if a step in a proof is justified by propositional reasoning.

The distributive axioms are valid in virtually all modal and temporal logics (Theorem 13.15). The expansion axiom expresses the basic properties of $\square$ that were

used to construct semantic tableaux, as well as $\vdash \Box A \to \bigcirc A$ (Theorem 13.25), which holds because all interpretations are infinite paths. The linearity axiom for $\bigcirc$ (Theorem 13.25) captures the restriction of LTL to linear interpretations.

The induction axiom is fundamental in $\mathscr{L}$: since interpretations in LTL are infinite paths, proofs of non-trivial formulas usually require induction. In a proof by induction, the inductive step is $A \to \bigcirc A$, that is, we assume that A is true today and prove that A is true tomorrow. If this inductive step is always true, $\Box(A \to \bigcirc A)$, then $A \to \Box A$ by the induction axiom. Finally, if A is true today (the base case), then A is always true $\Box A$.

The rules of inference are the familiar *modus ponens* and generalization using $\Box$, which is similar to generalization using $\forall$ in first-order logic.

Derived Rules

Here are some useful derived rules:

$$\frac{\vdash A \to B}{\vdash \Box A \to \Box B}, \qquad \frac{\vdash A \to B}{\vdash \bigcirc A \to \bigcirc B}, \qquad \frac{\vdash A \to \bigcirc A}{\vdash A \to \Box A}.$$

The first is obtained by applying generalization and then the distribution axiom; the second is similar except that the expansion axiom is used between the generalization and the distribution. When using these rules, we write the justification as *generalization*. The third rule will be called *induction* because it is a shortcut for generalization followed by the induction axiom.

14.2 Theorems of $\mathscr{L}$

The theorems and their proofs will be stated and proved for atomic propositions p and q although the intention is that they hold for arbitrary LTL formulas.

Distributivity

This subsection explores in more detail the distributivity of the temporal operators over proposition operators. The results will not be surprising, because $\Box$ and $\Diamond$ behave similarly to $\forall$ and $\exists$ in first-order logic. $\bigcirc$ is a special case because of linearity.

Theorem 14.2 $\vdash \bigcirc(p \land q) \leftrightarrow (\bigcirc p \land \bigcirc q)$.

Proof

1.	$\vdash (p \land q) \to p$	Prop
2.	$\vdash \bigcirc(p \land q) \to \bigcirc p$	Generalization
3.	$\vdash (p \land q) \to q$	Prop
4.	$\vdash \bigcirc(p \land q) \to \bigcirc q$	Generalization
5.	$\vdash \bigcirc(p \land q) \to (\bigcirc p \land \bigcirc q)$	2, 4, Prop
6.	$\vdash \bigcirc(p \to \neg q) \to (\bigcirc p \to \bigcirc \neg q)$	Distribution
7.	$\vdash \neg(\bigcirc p \to \bigcirc \neg q) \to \neg \bigcirc(p \to \neg q)$	6, Prop
8.	$\vdash \neg \bigcirc p \lor \bigcirc \neg q \lor \neg \bigcirc(p \to \neg q)$	7, Prop
9.	$\vdash \neg \bigcirc p \lor \neg \bigcirc q \lor \bigcirc \neg(p \to \neg q)$	8, Linearity
10.	$\vdash (\bigcirc p \land \bigcirc q) \to \bigcirc(p \land q)$	9, Prop
11.	$\vdash \bigcirc(p \land q) \leftrightarrow (\bigcirc p \land \bigcirc q)$	5, 10, Prop

∎

By linearity, $\bigcirc$ is self-dual, while $\lor$ is the dual of $\land$, so we immediately have $\vdash \bigcirc(p \lor q) \leftrightarrow (\bigcirc p \lor \bigcirc q)$.

Theorem 14.3 (Distribution) $\vdash \Box(p \land q) \leftrightarrow (\Box p \land \Box q)$.

The proof of the forward implication $\vdash \Box(p \land q) \to (\Box p \land \Box q)$ is similar to that of Theorem 14.2 and is left as an exercise. Before proving the converse, we need to prove the converse of the expansion axiom; the proof uses the forward implication of Theorem 14.3, which we assume that you have already proved.

Theorem 14.4 (Contraction) $\vdash p \land \bigcirc \Box p \to \Box p$.

Proof

1.	$\vdash \Box p \to p \land \bigcirc \Box p$	Expansion
2.	$\vdash \bigcirc \Box p \to \bigcirc(p \land \bigcirc \Box p)$	1, Generalization
3.	$\vdash p \land \bigcirc \Box p \to \bigcirc(p \land \bigcirc \Box p)$	2, Prop
4.	$\vdash p \land \bigcirc \Box p \to \Box(p \land \bigcirc \Box p)$	3, Induction
5.	$\vdash p \land \bigcirc \Box p \to (\Box p \land \Box \bigcirc \Box p)$	4, Distribution
6.	$\vdash p \land \bigcirc \Box p \to \Box p$	5, Prop

∎

For symmetry with the expansion axiom, $\bigcirc p$ could have been included in the premise of this theorem, but it is not needed.

Now we can prove the converse of Theorem 14.3. The structure of the proof is typical of inductive proofs in $\mathscr{L}$. An explanation of some of the more difficult steps of the formal proof is given at its end.

Proof Let $r = \Box p \land \Box q \land \neg\Box(p \land q)$.

1.	$\vdash r \rightarrow (p \land \bigcirc\Box p) \land (q \land \bigcirc\Box q) \land$	Expansion
	$\neg((p \land q) \land \bigcirc\Box(p \land q))$	Contraction
2.	$\vdash r \rightarrow (p \land \bigcirc\Box p) \land (q \land \bigcirc\Box q) \land$	1, Prop
	$(\neg(p \land q) \lor \neg\bigcirc\Box(p \land q))$	
3.	$\vdash r \rightarrow (p \land \bigcirc\Box p) \land (q \land \bigcirc\Box q) \land \neg\bigcirc\Box(p \land q)$	2, Prop
4.	$\vdash r \rightarrow \bigcirc\Box p \land \bigcirc\Box q \land \neg\bigcirc\Box(p \land q)$	3, Prop
5.	$\vdash r \rightarrow \bigcirc\Box p \land \bigcirc\Box q \land \bigcirc\neg\Box(p \land q)$	4, Linearity
6.	$\vdash r \rightarrow \bigcirc r$	5, Distribution
7.	$\vdash r \rightarrow \Box r$	6, Induction
8.	$\vdash r \rightarrow \Box p \land \Box q$	Def. of r, Prop
9.	$\vdash r \rightarrow p \land q$	8, Expansion
10.	$\vdash \Box r \rightarrow \Box(p \land q)$	9, Generalization
11.	$\vdash r \rightarrow \Box(p \land q)$	7, 10, Prop
12.	$\vdash r \rightarrow \neg\Box(p \land q)$	Def. of r, Prop
13.	$\vdash r \rightarrow false$	11, 12, Prop
14.	$\vdash \Box p \land \Box q \land \neg\Box(p \land q) \rightarrow false$	13, Def. of r
15.	$\vdash \Box p \land \Box q \rightarrow \Box(p \land q)$	14, Prop

∎

Steps 1–7 prove that r is invariant, meaning that r is true initially and remains true in any interpretation. The second line of Step 1 is justified by the contrapositive of contraction $\neg\Box(p \land q) \rightarrow \neg((p \land q) \land \bigcirc\Box(p \land q))$. Step 3 follows from Step 2 because $\neg(p \land q)$ is inconsistent with p and q that must be true by the expansion of $\Box p$ and $\Box q$.

The operator $\Box$ distributes over disjunction only in one direction. We leave the proof as an exercise, together with the task of showing that the converse is not valid.

Theorem 14.5 (Distribution) $\vdash (\Box p \lor \Box q) \rightarrow \Box(p \lor q)$.

Transitivity of $\Box$

Induction is used to prove that $\Box$ is transitive.

Theorem 14.6 (Transitivity) $\vdash \Box\Box p \leftrightarrow \Box p$

Proof

1.	$\vdash \Box\Box p \rightarrow \Box p$	Expansion
2.	$\vdash \Box p \rightarrow \bigcirc\Box p$	Expansion
3.	$\vdash \Box p \rightarrow \Box\Box p$	2, Induction
4.	$\vdash \Box\Box p \leftrightarrow \Box p$	1, 3, Prop

∎

Commutativity

Another expected result is that $\square$ and $\bigcirc$ commute:

Theorem 14.7 (Commutativity) $\vdash \square\bigcirc p \leftrightarrow \bigcirc\square p$.

Proof

|		
1.	$\vdash \square p \to \bigcirc p$	Expansion
2.	$\vdash \square\square p \to \square\bigcirc p$	1, Generalization
3.	$\vdash \square p \to \square\bigcirc p$	2, Transitivity
4.	$\vdash \square p \to p$	Expansion
5.	$\vdash \square p \to p \wedge \square\bigcirc p$	3, 4, Prop
6.	$\vdash \bigcirc\square p \to \bigcirc(p \wedge \square\bigcirc p)$	5, Generalization
7.	$\vdash \bigcirc\square p \to \bigcirc p \wedge \bigcirc\square\bigcirc p$	6, Distribution
8.	$\vdash \bigcirc\square p \to \square\bigcirc p$	7, Contraction
9.	$\vdash \square\bigcirc p \to \bigcirc p \wedge \bigcirc\square\bigcirc p$	Expansion
10.	$\vdash p \wedge \square\bigcirc p \to \bigcirc p \wedge \bigcirc\square\bigcirc p$	9, Prop
11.	$\vdash p \wedge \square\bigcirc p \to \bigcirc(p \wedge \square\bigcirc p)$	10, Distribution
12.	$\vdash p \wedge \square\bigcirc p \to \square(p \wedge \square\bigcirc p)$	11, Induction
13.	$\vdash p \wedge \square\bigcirc p \to \square p$	12, Distribution, Prop
14.	$\vdash \bigcirc(p \wedge \square\bigcirc p) \to \bigcirc\square p$	13, Generalization
15.	$\vdash \bigcirc p \wedge \bigcirc\square\bigcirc p \to \bigcirc\square p$	14, Distribution
16.	$\vdash \square\bigcirc p \to \bigcirc\square p$	9, 15, Prop
17.	$\vdash \square\bigcirc p \leftrightarrow \bigcirc\square p$	8, 16, Prop

∎

$\square$ and $\diamond$ commute in only one direction.

Theorem 14.8 $\vdash \diamond\square p \to \square\diamond p$.

We leave the proof as an exercise.

Example 14.9 Consider the interpretation where $s_i(p) = T$ for even i and $s_i(p) = F$ for odd i:
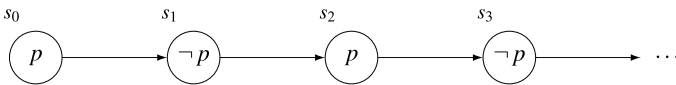
The formula $\square\diamond p$ is true, since for any i, $\sigma_{2i} \models p$. Obviously, $\diamond\square p$ is false in all states of the diagram, because for any i, $\sigma_i \models \neg p$ if i is odd and $\sigma_{i+1} \models \neg p$ if i is even. ∎

Dual Theorems for $\Diamond$

We leave it as an exercise to prove the following theorems using the duality of $\Box$ and $\Diamond$ and the linearity of $\bigcirc$.

Theorem 14.10

    (a) $\vdash p \to \Diamond p$ (b) $\vdash \bigcirc p \to \Diamond p$

    (c) $\vdash \Box p \to \Diamond p$ (d) $\vdash \Box(p \to q) \to (\Diamond p \to \Diamond q)$

    (e) $\vdash \Diamond(p \vee q) \leftrightarrow (\Diamond p \vee \Diamond q)$ (f) $\vdash \Diamond(p \wedge q) \to (\Diamond p \wedge \Diamond q)$

    (g) $\vdash \Diamond p \leftrightarrow p \vee \bigcirc\Diamond p$ (h) $\vdash \Diamond\bigcirc p \leftrightarrow \bigcirc\Diamond p$

    (i) $\vdash \Diamond\Diamond p \leftrightarrow \Diamond p$

From Theorem 14.10(d), we obtain a generalization rule for $\Diamond$:

$$\frac{\vdash A \to B}{\vdash \Diamond A \to \Diamond B}.$$

Collapsing Sequences of Operators

The transitivity of $\Box$ (Theorem 14.6) and its dual for $\Diamond$ (Theorem 14.10(i)) show that any string of $\Box$'s or $\Diamond$'s can be collapsed. No expressive power is gained by using more than two operators in sequence, as shown by the following theorem.

Theorem 14.11

        (a) $\vdash \Box\Diamond\Box p \leftrightarrow \Diamond\Box p$ (b) $\vdash \Diamond\Box\Diamond p \leftrightarrow \Box\Diamond p.$

We prove (a) and then (b) follows by duality.

Proof

1.	$\vdash \Box\Diamond\Box p \to \Diamond\Box p$	Expansion
2.	$\vdash \Box p \to \bigcirc\Box p$	Expansion
3.	$\vdash \Diamond\Box p \to \Diamond\bigcirc\Box p$	2, Generalization
4.	$\vdash \Diamond\Box p \to \bigcirc\Diamond\Box p$	3, Commutativity
5.	$\vdash \Diamond\Box p \to \Box\Diamond\Box p$	4, Induction
6.	$\vdash \Box\Diamond\Box p \leftrightarrow \Diamond\Box p$	1, 5, Prop

■

14.3 Soundness and Completeness of $\mathscr{L}$ *

Soundness

Theorem 14.12 (Soundness of $\mathscr{L}$) *Let A be a formula of LTL. If $\vdash_{\mathscr{L}} A$ then $\models A$.*

Proof We need to show that each axiom is a valid LTL formula and that the two rules of inference preserve validity. By definition, valid formulas of propositional logic are valid, and the soundness of *MP* was shown in Theorem 3.37. The soundness of Axioms 1 and 5 was shown in Theorems 13.15 and 13.25, respectively. We leave the soundness of Axioms 2 and 3 as an exercise and show the soundness of the induction axiom and the generalization rule.

Axiom 4: $\vdash \Box(A \to \bigcirc A) \to (A \to \Box A)$.

If the formula is not valid, there exists an interpretation σ such that:

$$\sigma \models \Box(A \to \bigcirc A) \land A \land \neg \Box A.$$

Since $\sigma \models A$ and $\sigma \models \neg \Box A$ there exists a smallest value $i > 0$ such that $\sigma_i \models \neg A$ and $\sigma_j \models A$ for $0 \leq j < i$. In particular, $\sigma_{i-1} \models A$. But we also have that $\sigma \models \Box(A \to \bigcirc A)$, so by definition of the $\Box$ operator, $\sigma_{i-1} \models A \to \bigcirc A$. By *MP* we have $\sigma_{i-1} \models \bigcirc A$ and thus $\sigma_i \models A$, contradicting $\sigma_i \models \neg A$.

Generalization: If $\models A$, then $\models \Box A$.

We need to show that for all interpretations σ, $\sigma \models \Box A$. This means that for all $i \geq 0$, it is true that $\sigma_i \models A$. But $\models A$ implies that for *all* interpretation σ', $\sigma' \models A$, in particular, this must hold for $\sigma' = \sigma_i$. ∎

Completeness

Theorem 14.13 (Completeness of $\mathscr{L}$) *Let A be a formula of LTL. If $\models A$ then $\vdash_{\mathscr{L}} A$.*

Proof If A is valid, the construction of a semantic tableau for $\neg A$ will fail, either because it closes or because all the MSCCs are non-fulfilling and were deleted. We show by induction that for every node in the tableau, the disjunction of the negations of the formulas labeling the node is provable in $\mathscr{L}$. Since the formula labeling the root is $\neg A$, it follows that $\vdash \neg \neg A$, from which $\vdash A$ follows by propositional logic.

The base case of the leaves and the inductive steps for the rules for α- and β-formulas follow by propositional reasoning together with the expansion axiom.

Suppose that the rule for an X-formula is used:

$$\bigcirc A_1, \ldots, \bigcirc A_n, \; B_1, \ldots, B_k$$
$$\downarrow$$
$$A_1, \ldots, A_n$$

where we assume that negations are pushed inwards as justified by the linearity axiom. By the inductive hypothesis, $\vdash \neg A_1 \vee \cdots \vee \neg A_n$. The following deduction proves the formula associated with the parent node:

1. $\vdash \neg A_1 \vee \cdots \vee \neg A_n$ Inductive hypothesis
2. $\vdash \square(\neg A_1 \vee \cdots \vee \neg A_n)$ 1, Generalization
3. $\vdash \bigcirc(\neg A_1 \vee \cdots \vee \neg A_n)$ 2, Expansion
4. $\vdash \bigcirc\neg A_1 \vee \cdots \vee \bigcirc\neg A_n$ 3, Distribution
5. $\vdash \neg\bigcirc A_1 \vee \cdots \vee \neg\bigcirc A_n$ 4, Linearity
6. $\vdash \neg\bigcirc A_1 \vee \cdots \vee \neg\bigcirc A_n \vee \neg B_1 \vee \cdots \vee \neg B_k$ 5, Prop

There remains the case of a node that is part of a non-fulfilling MSCC. We demonstrate the technique on a specific example, proving $\vdash \square p \rightarrow \bigcirc\square p$ by constructing a semantic tableau for the negation of the formula.
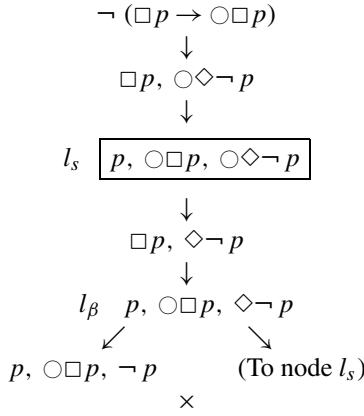
The crucial part of the proof is to define the *invariant* of the loop, that is, a formula A such that $\vdash A \rightarrow \bigcirc A$. The invariant will be the conjunction of the formulas A_i, where $\bigcirc A_i$ are the next formulas in the states of the SCC, as these represent what must be true from one state to the next. In the example, for invariant is $\square p \wedge \Diamond\neg p$. We proceed to prove that this formula is inductive.

1. $\vdash (\square p \wedge \Diamond\neg p) \rightarrow (p \wedge \bigcirc\square p) \wedge (\neg p \vee \bigcirc\Diamond\neg p)$ Expansion
2. $\vdash (\square p \wedge \Diamond\neg p) \rightarrow (p \wedge \bigcirc\square p \wedge \bigcirc\Diamond\neg p)$ 1, Prop
3. $\vdash (\square p \wedge \Diamond\neg p) \rightarrow (\bigcirc\square p \wedge \bigcirc\Diamond\neg p)$ 2, Prop
4. $\vdash (\square p \wedge \Diamond\neg p) \rightarrow \bigcirc(\square p \wedge \Diamond\neg p)$ 3, Distribution
5. $\vdash (\square p \wedge \Diamond\neg p) \rightarrow \square(\square p \wedge \Diamond\neg p)$ 4, Induction

The leaf on the left of the tableau has a complementary pair of literals, so $\vdash \neg p \vee \neg\bigcirc\square p \vee \neg\neg p$ is an axiom. We use this formula together with formula (5) to prove the formula associated with l_β.

6. $\vdash \neg\, p \vee \neg \bigcirc \square p \vee \neg\, \neg\, p$ Axiom 0
7. $\vdash (p \wedge \bigcirc \square p) \rightarrow \neg\, \neg\, p$ 6, Prop
8. $\vdash \square p \rightarrow \neg\, \neg\, p$ 7, Contraction
9. $\vdash (\square p \wedge \Diamond \neg\, p) \rightarrow \neg\, \neg\, p$ 8, Prop
10. $\vdash \square(\square p \wedge \Diamond \neg\, p) \rightarrow \square \neg\, \neg\, p$ 9, Generalization
11. $\vdash (\square p \wedge \Diamond \neg\, p) \rightarrow \square \neg\, \neg\, p$ 5, 10, Prop
12. $\vdash (p \wedge \bigcirc \square p \wedge \Diamond \neg\, p) \rightarrow \square \neg\, \neg\, p$ 11, Expansion
13. $\vdash (p \wedge \bigcirc \square p \wedge \Diamond \neg\, p) \rightarrow \neg \Diamond \neg\, p$ 12, Duality
14. $\vdash \neg\, p \vee \neg \bigcirc \square p \vee \neg \Diamond \neg\, p$ 13, Prop

Line 14 is the disjunction of the complements of the formulas at node l_β.   ■

The method used in the proof will almost certainly not yield the shortest possible proof of a formula, but it is an algorithmic procedure for discovering a proof of a valid LTL formula.

14.4 Axioms for the Binary Temporal Operators *

Section 13.6 presented several binary temporal operators, any one of which can be chosen as a basic operator and the others defined from it. If we choose $\mathscr{U}$ as the basic operator, a complete axiom system is obtained by adding the following two axioms to the axioms of Definition 14.1:

Axiom 6   Expansion of $\mathscr{U}$ $\vdash A \mathscr{U} B \leftrightarrow (B \vee (A \wedge \bigcirc(A \mathscr{U} B)))$.
Axiom 7   Eventuality $\vdash A \mathscr{U} B \rightarrow \Diamond B$.

$\mathscr{U}$ is similar to $\Diamond$: Axiom 6 requires that either B is true today or A is true today and $A \mathscr{U} B$ will be true tomorrow. Axiom 7 requires that B eventually be true.

14.5 Summary

The deductive system $\mathscr{L}$ assumes that propositional reasoning can be informally applied. There are five axioms: the distributive and expansion axioms are straight-forward, while the duality axiom for $\bigcirc$ is essential to capture the linearity of interpretations of LTL. The central axiom of $\mathscr{L}$ is the induction axiom: since interpretations in LTL are infinite paths, proofs of non-trivial formulas usually require induction. The rules of inference are the familiar *modus ponens* and generalization using $\square$. As usual, the proof of soundness is straightforward. Proving completeness is based on the existence of a non-fulfilling MSCC in a tableau. The formulas labeling the nodes of the MSCC can be used to construct a formula that can be proved by induction.

14.6 Further Reading

The deductive system $\mathscr{L}$ and the proof of its soundness and completeness is based on Ben-Ari et al. (1983), although that paper used a different system of temporal logic. The definitive reference for the specification and verification of concurrent programs using temporal logic is Manna and Pnueli (1992, 1995). The third volume was never completed, but a partial draft is available (Manna and Pnueli, 1996). Axioms for the various binary temporal operators are given in Kröger and Merz (2008, Chap. 3).

14.7 Exercises

14.1 Prove $\vdash \Box(p \land q) \to (\Box p \land \Box q)$ (Theorem 14.3).

14.2 Prove $\vdash (\Box p \lor \Box q) \to \Box(p \lor q)$ (Theorem 14.5) and show that the converse is not valid.

14.3 Prove the future formulas in Theorem 14.10.

14.4 Prove that Axioms 2 and 3 are valid.

14.5 Prove $\vdash \Diamond\Box\Diamond p \leftrightarrow \Box\Diamond p$ (Theorem 14.11) and $\vdash \Diamond\Box p \to \Box\Diamond p$ (Theorem 14.8).

14.6 Prove $\vdash \Box(\Box\Diamond p \to \Diamond q) \leftrightarrow (\Box\Diamond q \lor \Diamond\Box\neg p)$.

14.7 Fill in the details of the proof of $\vdash \Box((p \lor \Box q) \land (\Box p \lor q)) \leftrightarrow (\Box p \lor \Box q)$.

References

M. Ben-Ari, Z. Manna, and A. Pnueli. The temporal logic of branching time. *Acta Informatica*, 20:207–226, 1983.

F. Kröger and S. Merz. *Temporal Logic and State Systems*. Springer, 2008.

Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems. Vol. I: Specification*. Springer, New York, NY, 1992.

Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems. Vol. II: Safety*. Springer, New York, NY, 1995.

Z. Manna and A. Pnueli. Temporal verification of reactive systems: Progress. Draft available at http://www.cs.stanford.edu/~zm/tvors3.html, 1996.