<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VERIFICATION OF SEQUENTIAL PROGRAMS: TEMPORAL AXIOMATIZATION</td>
<td>Z Manna</td>
<td>SEP 81</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

UNCLASSIFIED

STAN-CS-81-877
Verification of Sequential Programs: Temporal Axiomatization

by

Zohar Manna

Department of Computer Science
Stanford University
Stanford, CA  94305
VERIFICATION OF SEQUENTIAL PROGRAMS:  
TEMPORAL AXIOMATIZATION

by

ZOI MANNA

Computer Science Dept.  
Applied Mathematics Dept.

Stanford University  
The Weizmann Institute

Stanford, CA  
Rehovot, Israel

Abstract

This is one in a series of reports describing the application of temporal logic to the specification and verification of computer programs.

In earlier reports, we introduced temporal logic as a tool for reasoning about concurrent programs and specifying their properties [MP1] and presented proof principles for establishing these properties ([MP2]). Here, we restrict ourselves to deterministic, sequential programs. We present a proof system in which properties of such programs, expressed as temporal formulas, can be proved formally.

Our proof system consists of three parts: a general part elaborating the properties of temporal logic, a domain part giving an axiomatic description of the data domain, and a program part giving an axiomatic description of the program under consideration.

We illustrate the use of the proof system by giving two alternative formal proofs of the total correctness of a simple program.


This research was supported in part by the National Science Foundation under grants MCS80-06930, in part by the Office of Naval Research under Contract N00014-76-C-0687, and in part by the United States Air Force Office of Scientific Research under Contract AFOSR-81-0014.
1. INTRODUCTION

Temporal logic is a modal logic in which we impose special restrictions on the models of interpretation ([PnU], [PnU], [PnU], [GPSS], [MP1]). A universe for temporal logic consists of a collection of states (worlds). A state \( s' \) is accessible from a state \( s \) if through development in time, \( s \) can change into \( s' \). We concentrate on histories of development which are linear and discrete. Thus, the models of temporal logic consist of \( \omega \)-sequences, i.e., infinite sequences of the form \( \sigma = s_0, s_1, \ldots \). In such a sequence, \( s_j \) is accessible from \( s_i \) if \( i \leq j \). On these states we define an immediate accessibility relation \( p \) which is required to be a function. That means that every state \( s \) has exactly one other state \( s' \) such that \( p(s, s') \). This corresponds to our intuition that in a discrete time model each instant has exactly one immediate successor. The transitive reflexive closure of \( p \), \( R = p^* \), is the accessibility relation; intuitively, \( R(s, s') \) holds when \( s' \) is either identical to \( s \) or lies in the future of \( s \).

We first describe the temporal language we are going to use. This language is designed specifically for the application we have in mind, namely reasoning about programs, and is not necessarily the most general temporal language possible.

The language uses a set of basic symbols consisting of individual variables and constants, and proposition, function and predicate symbols. The set is partitioned into two subsets: global and local symbols. The global symbols have a uniform interpretation over the complete universe and do not change their values or meanings from one state to another. The local symbols, on the other hand, may assume different meanings and values in different states of the universe. For our purpose, the only local symbols that interest us are local individual variables. We will have global symbols of all types.

We use the regular set of boolean connectives: \( \land, \lor, \equiv, \neg \) together with the equality operator \( = \) and the first-order quantifiers \( \forall \) and \( \exists \). This set is referred to as the classical operators. The quantifiers \( \forall \) and \( \exists \) are applied only to global individual variables.

The modal operators used are: \( \Box, \Diamond, O, \) and \( U \), which are called respectively the always, sometime, next and until operators. The first three operators are unary while the \( U \) operator is binary. We use the next operator \( O \) in two different ways — as a temporal operator applied to formulas and as a temporal operator applied to terms.

A model \( (I, \alpha, \sigma) \) for our language consists of a (global) interpretation \( I \), a (global) assignment \( \alpha \) and a sequence of states \( \sigma \).

- The interpretation \( I \) specifies a nonempty domain \( D \) and assigns concrete elements, functions and predicates to the (global) individual constants, function, predicate symbols.

- The assignment \( \alpha \) assigns a value over the appropriate domain to each of the global free individual variables.

- The sequence \( \sigma = s_0, s_1, \ldots \) is an infinite sequence of states. Each state \( s_i \) assigns values to the local free individual variables and propositions.

For a sequence

\[ \sigma = s_0, s_1, \ldots \]
we denote by
\[ \sigma^{(i)} = s_i, s_{i+1}, \ldots \]
the $i$-truncated suffix of $\sigma$.

Given a temporal formula $w$, we present below an inductive definition of the truth value of $w$ in a model $(I, \alpha, \sigma)$. The value of a subformula or term $\tau$ under $(I, \alpha, \sigma)$ is denoted by $\tau|_{\sigma}^I$, $I$ being implicitly assumed.

Consider first the evaluation of terms:

- For a local individual variable or local proposition $y$:
  \[ y|_{\sigma}^\alpha = y_{s_0}, \]
  i.e., the value assigned to $y$ in $s_0$, the first state of $\sigma$.

- For a global individual variable or global proposition $u$:
  \[ u|_{\sigma}^\alpha = \alpha[u], \]
  i.e., the value assigned to $u$ by $\alpha$.

- For an individual constant the evaluation is given by $I$
  \[ c|_{\sigma}^\alpha = I[c]. \]

- For a $k$-ary function $f$:
  \[ f(t_1, \ldots, t_k)|_{\sigma}^\alpha = I[f](t_1|_{\sigma}^\alpha, \ldots, t_k|_{\sigma}^\alpha), \]
  i.e., the value is given by the application of the interpreted function $I[f]$ to the values of $t_1, \ldots, t_k$ evaluated in the environment $(I, \alpha, \sigma)$.

- For a term $t$:
  \[ O|_{\sigma}^\alpha = d|_{\sigma}^\alpha(t_1), \]
  i.e., the value of $O\ t$ in $\sigma = s_0, s_1, \ldots$ is given by the value of $t$ in the shifted sequence $\sigma^{(i)} = s_1, s_2, \ldots$.

Consider now the evaluation of formulas:

- For a $k$-ary predicate $p$ (including equality):
  \[ p(t_1, \ldots, t_k)|_{\sigma}^\alpha = I[p](t_1|_{\sigma}^\alpha, \ldots, t_k|_{\sigma}^\alpha). \]
Here again, we evaluate the arguments in the environment and then test $I[p]$ on them.

- For a disjunction:
  \[ (w_1 \lor w_2)_{I}^\alpha = true \iff w_1{I}_{\alpha}^\sigma = true \text{ or } w_2{I}_{\alpha}^\sigma = true. \]

- For a negation:
  \[ (\sim w)_{I}^\alpha = true \iff w{I}_{\alpha}^\sigma = false. \]

- For a next-time application:
  \[ \Box w{I}_{\alpha}^\sigma = w{I}_{\alpha}(1). \]
  Thus $\Box w$ means: $w$ will be true in the next instant -- read “next $w$”.

- For an all-times application:
  \[ \Diamond w{I}_{\alpha}^\sigma = true \iff \text{ for every } k \geq 0, w{I}_{\alpha(k)} = true, \]
  i.e., $w$ is true for all suffix sequences of $\sigma$. Thus $\Diamond w$ means: $w$ is true for all future instants (including the present) -- read “always $w$” or “henceforth $w$”.

- For a some-time application:
  \[ \Diamond w{I}_{\alpha}^\sigma = true \iff \text{ there exists a } k \geq 0 \text{ such that } w{I}_{\alpha(k)} = true, \]
  i.e., $w$ is true on at least one suffix of $\sigma$. Thus $\Diamond w$ means: $w$ will be true for some future instant (possibly the present) -- read “sometimes $w$” or “eventually $w$”.

- For an until application:
  \[ w_1 \uuntil w_2{I}_{\alpha}^\sigma = true \iff \text{ for some } k \geq 0, w_2{I}_{\alpha(k)} = true \text{ and } \text{ for all } i, 0 \leq i < k, w_1{I}_{\alpha(i)} = true. \]
  Thus $w_1 \uuntil w_2$ means: there is a future instant in which $w_2$ holds, and such that until that instant $w_1$ continuously holds -- read “$w_1$ until $w_2$”.

- For a universal quantification:
  \[ (\forall u.w)_{I}^\alpha = true \iff \text{ for every } d \in D, w{I}_{\alpha'} = true, \]
  where $\alpha' = \alpha \circ [u \leftarrow d]$ is the assignment obtained from $\alpha$ by assigning $d$ to $u$.

- For an existential quantification:
  \[ (\exists u.w)_{I}^\alpha = true \iff \text{ for some } d \in D, w{I}_{\alpha'} = true, \]
  where $\alpha' = \alpha \circ [u \leftarrow d]$.  

4
A formula \( w \) is valid if it is true in every model \((I, \alpha, \sigma)\).

Having defined valid formulas, we naturally look for a deductive system. In such a system we take some of the valid formulas as basic axioms and provide a set of sound inference rules by which we hope to be able to prove the other valid formulas as theorems. In order to denote the fact that a formula \( w \) is a theorem derivable in our deductive system we will write \( \vdash w \). This will be the case if \( w \) is an axiom or is derivable from the axioms by a proof using the inference rules of the system.

We partition our deductive system into a general part dealing with the general temporal properties of discrete linear sequences, a domain part which gives an axiomatic description of the necessary knowledge about the domain, and a program part which gives an axiomatic description of a particular program.

We start with the general part, describing first the axiomatic system for propositional temporal logic in which we do not admit predicates or quantification. We treat first the "classical" modal operators \( \Box \) and \( \Diamond \) (the modal system), and later add the special operators \( \Box \) and \( \ulcorner \) (the temporal system).

2. THE \( \Box \) ("ALWAYS") AND \( \Diamond \) ("SOMETIMES") OPERATORS

Axioms:

\[
\begin{align*}
A1. \quad & \vdash \sim \Diamond w \equiv \Box \sim w \\
A2. \quad & \vdash \Box(w_1 \supset w_2) \supset (\Box w_1 \supset \Box \Box w_2) \\
A3. \quad & \vdash \Box w \supset w \\
A4. \quad & \vdash \Box w \supset \Box \Box w
\end{align*}
\]

Axiom A1 defines \( \Diamond \) as the dual of \( \Box \); it states that at all times \( w \) is false if it is not the case that sometime \( w \) holds. Axiom A2 states that if universally \( w_1 \) implies \( w_2 \) then if at all times \( w_1 \) is true then so is \( w_2 \). Axiom A3 establishes the present as part of the future by stating that if \( w \) is true at all future times it must be true of the present. Axiom A4 states that if \( w \) holds in the future, it holds in the future of the future.
Inference rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
</table>
| R1.  | If \( w \) is an instance of a propositional tautology then \( \vdash w \)  
\((\text{Propositional Tautology - PT})\) |
| R2.  | If \( \vdash w_1 \supset w_2 \) and \( \vdash w_1 \) then \( \vdash w_2 \)  
\((\text{Modus Ponens - MP})\) |
| R3.  | If \( \vdash w \) then \( \vdash \Box w \)  
\((\Box \text{Insertion - } \Box I)\) |

All these rules are sound. The soundness of \( R1 \) and \( R2 \) is obvious. Note that in \( R1 \) we also include modal instances of tautologies; we may substitute an arbitrary modal formula for a proposition letter in obtaining an instance. For example \( \Box w \supset \Box w \) is a modal instance of the tautology \( p \supset p \).

To justify \( R3 \), we recall that validity of \( w \) means that \( w \) is true in all models, hence \( \Box w \) is also valid.

This system provides a logical basis for "propositional" modal reasoning. In Modal Logic circles, this system is known as \( S4 \) (see, e.g., [HC]). This system constrains \( R \) to be reflexive \((A3)\) and transitive \((A4)\).

Before demonstrating some theorems that can be proved in this system, we develop several useful derived rules:

<table>
<thead>
<tr>
<th>Propositional Reasoning -- PR</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdash (w_1 \land w_2 \land \ldots \land w_n) \supset w )</td>
</tr>
<tr>
<td>( \vdash w_1, \vdash w_2, \ldots, \text{ and } \vdash w_n )</td>
</tr>
<tr>
<td>( \vdash w )</td>
</tr>
</tbody>
</table>

The notation above is used to describe inference rules. It has the general form

\[
\vdash \varphi_1, \vdash \varphi_2, \ldots, \vdash \varphi_m
\]

\[\vdash \psi\]

and means that if we have already proved \( \varphi_1, \ldots, \varphi_m \) (the assumptions of the rule), we are allowed by this rule to infer \( \psi \) (the conclusion of the rule).

**proof:**

The rule follows from the propositional tautology (Rule \( R1 \))

\[
\vdash [(w_1 \land w_2 \land \ldots \land w_n) \supset w] \supset [w_1 \supset (w_2 \supset (\ldots (w_n \supset w) \ldots))]
\]

by applying \( MP \) (Rule \( R2 \)) \( n + 1 \) times.

Whenever we apply this derived rule without indicating the antecedent

\[
\vdash (w_1 \land w_2 \ldots \land w_n) \supset w,
\]
it means that this formula is simply an instance of a propositional tautology.

\[
\begin{align*}
\text{(a)} & \quad \vdash w_1 \supset w_2 \\
\text{(b)} & \quad \vdash w_1 \equiv w_2 \\
\text{(c)} & \quad \vdash \Box w_1 \supset \Box w_2 \\
\text{Rule (b) then follows by propositional reasoning, since} & \\
[(w_1 \supset w_2) \land (w_2 \supset w_1)] & \equiv (w_1 \equiv w_2)
\end{align*}
\]

is a tautology.

\[
\begin{align*}
\text{(a)} & \quad \vdash w_1 \supset w_2 \\
\text{(b)} & \quad \vdash w_1 \equiv w_2 \\
\text{Rule (b) then follows by propositional reasoning.}
\end{align*}
\]

\[
\begin{align*}
\text{(a)} & \quad \vdash w_1 \supset w_2 \\
\text{(b)} & \quad \vdash w_1 \equiv w_2 \\
\text{Equivalence Rule – ER} & \\
\text{Let } w' \text{ be the result of replacing an occurrence of a subformula } v_1 \\
\text{in } w \text{ by } v_2. \text{ Then} & \\
\vdash v_1 \equiv v_2 & \\
\vdash w \equiv w'
\end{align*}
\]

proof:

By induction on the structure of \( w \).
Case: $w$ is $v_1$. Then $w'$ is $v_2$ and $\vdash v_1 \equiv v_2$ implies $\vdash w \equiv w'$.

Case: $w$ is of the form $\neg u$. We assume that $\vdash v_1 \equiv v_2$ implies $\vdash u \equiv u'$. Then by propositional reasoning $\vdash \neg u \equiv \neg u'$, i.e., $\vdash w \equiv w'$.

Case: $w$ is of the form $u_1 \lor u_2$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u_1 \equiv u_1'$ and $\vdash u_2 \equiv u_2'$. Then by propositional reasoning $\vdash (u_1 \lor u_2) \equiv (u_1' \lor u_2')$, i.e., $\vdash w \equiv w'$.

The cases where $w$ is of form $u_1 \land u_2, u_1 \supset u_2$, etc. are similar.

Case: $w$ is of the form $\Box u$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u \equiv u'$. By the $\Box \Box$-rule, $\vdash \Box u \equiv \Box u'$, i.e., $\vdash w \equiv w'$.

The case in which $w$ is of the form $\Diamond u$ is treated similarly, using the $\Diamond \Diamond$-rule.

Some theorems that can be derived in the system are:

T1. $\vdash w \supset \Diamond w$

proof:

1. $\vdash (\Box \neg w) \supset \neg w$ by A3
2. $\vdash w \supset (\neg \Box \neg w)$
3. $\vdash w \supset \Diamond w$ by A1 and PR

The theorem implies (by MP)

<table>
<thead>
<tr>
<th>$\Diamond Insertion \ - \ \Diamond I$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\vdash w$</td>
</tr>
<tr>
<td>$\vdash \Diamond w$</td>
</tr>
</tbody>
</table>

We can derive the converse of axiom $A4$ as stated in the modal system, and thus prove:

T2. $\vdash \Box w \equiv \Box \Box w$

proof:

1. $\vdash \Box w \supset \Box \Box w$ by A4
2. $\vdash \Box w \supset w$ by A3
3. $\vdash \Box \Box w \supset \Box w$ by $\Box \Box$
4. $\vdash \Box w \equiv \Box \Box w$ by 1, 3, and PR

T3. $\vdash \Diamond w \equiv \Diamond \Diamond w$

proof:

1. $\vdash \Box \neg w \equiv \Box \Box \neg w$ by T2
2. \( \vdash \neg \square \neg w \equiv \neg \square \neg \neg w \) \hspace{1cm} \text{by PR}

3. \( \vdash \Diamond w \equiv \neg \square \neg \Diamond w \) \hspace{1cm} \text{by A1 and ER}

4. \( \vdash \Diamond w \equiv \Diamond \Diamond w \) \hspace{1cm} \text{by A1 and PR}

Because of these last two theorems we can collapse any string of consecutive identical modalities such as \( \square \cdots \square \) or \( \Diamond \cdots \Diamond \) into a single modality of the same type.

Note that to derive line 3 from line 2 we could not use propositional reasoning (PR), but we had to use the equivalence rule (ER). The subformula \( \neg \square \neg w \) in

\[ 2. \vdash \text{...} \equiv \neg \square \neg \text{...} \]

was replaced by the equivalent subformula \( \neg \Diamond w \) to obtain

\[ 3. \vdash \text{...} \equiv \neg \Diamond \text{...} \]

But this replacement is inside \( \square \) and thus cannot be justified by propositional reasoning. The replacement done on the left-hand side of the equivalence can be justified by propositional reasoning.

**T4.** \( \vdash (\Diamond \neg w) \equiv (\neg \square w) \)

**proof:**

1. \( \vdash (\Diamond \neg w) \equiv w \) \hspace{1cm} \text{by PT}

2. \( \vdash (\neg w) \equiv \square w \) \hspace{1cm} \text{by \( \square \square \)}

3. \( \vdash (\neg \Diamond w) \equiv \Diamond w \) \hspace{1cm} \text{by A1 and PR}

4. \( \vdash (\Diamond \neg w) \equiv (\neg \Diamond w) \) \hspace{1cm} \text{by PR}

**T5.** \( \vdash \square (w_1 \supset w_2) \supset (\Diamond w_1 \supset \Diamond w_2) \)

**proof:**

1. \( \vdash (w_1 \supset w_2) \equiv (\neg w_2 \supset \neg w_1) \) \hspace{1cm} \text{by PT}

2. \( \vdash \square (w_1 \supset w_2) \equiv \square (\neg w_2 \supset \neg w_1) \) \hspace{1cm} \text{by \( \square \square \)}

3. \( \vdash (\neg w_2 \supset \neg w_1) \equiv (\neg w_2 \supset \neg \Diamond w_1) \) \hspace{1cm} \text{by A1 and PR}

4. \( \vdash (\square \neg w_2 \supset \square \neg w_1) \equiv (\Diamond \neg w_2 \supset \Diamond \Diamond w_1) \) \hspace{1cm} \text{by A1 and PR}

5. \( \vdash (\neg \Diamond w_2 \supset \neg \Diamond w_1) \equiv (\Diamond w_1 \supset \Diamond w_2) \) \hspace{1cm} \text{by PT}

6. \( \vdash \square (w_1 \supset w_2) \supset (\Diamond w_1 \supset \Diamond w_2) \) \hspace{1cm} \text{by \( \square \square \), \( \square \square \), and PR}

**T6.** \( \vdash \square (w_1 \lor w_2) \equiv (\square w_1 \lor \square w_2) \)

**proof:**

1. \( \vdash (w_1 \lor w_2) \supset w_1 \) \hspace{1cm} \text{by PT}

2. \( \vdash \square (w_1 \lor w_2) \supset \square w_1 \) \hspace{1cm} \text{by \( \square \square \)}

3. \( \vdash (w_1 \lor w_2) \supset w_2 \) \hspace{1cm} \text{by PT}

4. \( \vdash \square (w_1 \lor w_2) \supset \square w_2 \) \hspace{1cm} \text{by \( \square \square \)}

5. \( \vdash \square (w_1 \lor w_2) \supset (\square w_1 \lor \square w_2) \) \hspace{1cm} \text{by \( \square \square \), \( \square \square \), and PR}

6. \( \vdash w_1 \supset (w_2 \supset w_1 \lor w_2) \) \hspace{1cm} \text{by PT}
7. \( \vdash \Box w_1 \supset \Box (w_1 \land w_2) \)
   by \( \Box \Box \)

8. \( \vdash \Box (w_2 \supset (w_1 \land w_2)) \supset (\Box w_2 \supset \Box (w_1 \land w_2)) \)
   by \( A2 \)

9. \( \vdash \Box w_1 \supset (\Box w_2 \supset \Box (w_1 \land w_2)) \)
   by 7, 8, and \( PR \)

10. \( \vdash (\Box w_1 \land \Box w_2) \supset \Box (w_1 \land w_2) \)
   by \( PR \)

11. \( \vdash (w_1 \land w_2) \equiv (\Box w_1 \land \Box w_2) \)
   by 5, 10, and \( PR \)

**T7.** \( \vdash \Diamond (w_1 \lor w_2) \equiv (\Diamond w_1 \land \Diamond w_2) \)

*proof:*

1. \( \vdash \Box (\sim w_1 \land \sim w_2) \equiv (\Box \sim w_1 \land \Box \sim w_2) \)
   by \( T6 \)

2. \( \vdash \Box \sim (w_1 \lor w_2) \equiv \sim (\Box \sim w_1 \lor \Box \sim w_2) \)
   by \( ER \)

3. \( \vdash \Diamond (w_1 \lor w_2) \equiv (\Diamond w_1 \lor \Diamond w_2) \)
   by \( A1 \) and \( PR \)

4. \( \vdash (w_1 \lor w_2) \equiv (\Diamond w_1 \lor \Diamond w_2) \)
   by \( PR \)

Note that because of the universal character of \( \Box \) it can be distributed over \( \land \) (Theorem \( T6 \)), while \( \Diamond \), which is of existential character can be distributed over \( \lor \) (Theorem \( T7 \)).

**T8.** \( \vdash \Diamond (w_1 \land w_2) \equiv (\Diamond w_1 \land \Diamond w_2) \)

*proof:*

1. \( \vdash \Diamond (w_1 \land w_2) \equiv \Diamond w_1 \)
   by \( PT \) and \( \Diamond \Diamond \)

2. \( \vdash \Diamond (w_1 \land w_2) \equiv \Diamond w_2 \)
   by \( PT \) and \( \Diamond \Diamond \)

3. \( \vdash \Diamond (w_1 \land w_2) \equiv (\Diamond w_1 \land \Diamond w_2) \)
   by 1, 2, and \( PR \)

**T9.** \( \vdash \Box (w_1 \lor w_2) \equiv \Box (w_1 \land w_2) \)

*proof:*

1. \( \vdash \Box w_1 \equiv \Box (w_1 \lor w_2) \)
   by \( PT \) and \( \Box \Box \)

2. \( \vdash \Box w_2 \equiv \Box (w_1 \lor w_2) \)
   by \( PT \) and \( \Box \Box \)

3. \( \vdash (\Box w_1 \lor \Box w_2) \equiv (\Box w_1 \land \Box w_2) \)
   by 1, 2, and \( PR \)

**T10.** \( \vdash (\Box w_1 \lor \Diamond w_2) \equiv \Diamond (w_1 \land w_2) \)

*proof:*

1. \( \vdash (w_1 \lor w_2) \equiv (\Box w_1 \lor \Box w_2) \)
   by \( A2 \)

2. \( \vdash \Box \sim (w_1 \lor \Box w_2) \equiv \sim (\Box w_1 \lor \Box w_2) \)
   by \( ER \)

3. \( \vdash \Diamond (w_1 \land w_2) \equiv \Diamond (w_1 \lor \Diamond w_2) \)
   by \( A1 \) and \( PR \)

4. \( \vdash (\Box w_1 \lor \Diamond w_2) \equiv \Diamond (w_1 \land w_2) \)
   by \( PR \)

*another proof (without using \( ER \):*

1. \( \vdash w_1 \equiv (w_2 \equiv (w_1 \land w_2)) \)
   by \( PT \)

2. \( \vdash \Box w_1 \equiv \Box (w_2 \equiv (w_1 \land w_2)) \)
   by \( \Box \Box \)
The following derived rules correspond to proof rules existing in most axiomatic verification systems:

Consequence Rules - $\Diamond Q$ and $\Box Q$

\[
\begin{array}{c|c}
\hline
\text{Consequence Rules} & \text{Consequence Rules} \\
\hline
\vdash w_1 \supset w_2 & \vdash w_1 \supset w_2 \\
\vdash w_2 \supset \Diamond w_3 & \vdash w_2 \supset \Box w_3 \\
\vdash w_3 \supset w_4 & \vdash w_3 \supset w_4 \\
\hline
\vdash w_1 \supset \Diamond w_4 & \vdash w_1 \supset \Box w_4 \\
\end{array}
\]

proof of $\Diamond Q$:

1. $\vdash w_1 \supset w_2$ \\
2. $\vdash w_2 \supset \Diamond w_3$ \\
3. $\vdash w_3 \supset w_4$ \\
4. $\vdash \Diamond w_3 \supset \Diamond w_4$ \\
5. $\vdash w_1 \supset \Diamond w_4$

The $\Box Q$ rule is proved similarly by the $\Box \Box$-rule.

Concatenation Rule - $\Diamond C$ and $\Box C$

\[
\begin{array}{c|c}
\hline
\text{Concatenation Rule} & \text{Concatenation Rule} \\
\hline
\vdash w_1 \supset \Diamond w_2 & \vdash w_1 \supset \Box w_2 \\
\vdash w_2 \supset \Diamond w_3 & \vdash w_2 \supset \Box w_3 \\
\hline
\vdash w_1 \supset \Diamond w_3 & \vdash w_1 \supset \Box w_3 \\
\end{array}
\]

proof of $\Diamond C$:

1. $\vdash w_1 \supset \Diamond w_2$ \\
2. $\vdash w_2 \supset \Diamond w_3$ \\
3. $\vdash \Diamond w_2 \supset \Diamond \Diamond w_3$ \\
4. $\vdash \Diamond w_2 \supset \Diamond w_3$ \\
5. $\vdash w_1 \supset \Diamond w_3$

The $\Box C$ rule is proved similarly by the $\Box \Box$-rule.
3. THE $\square$ ("NEXT") AND $\Diamond$ ("UNTIL") OPERATORS

Axioms:

<table>
<thead>
<tr>
<th>Axiom</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.</td>
<td>$\vdash \sim \Diamond w \equiv \Box \sim w$</td>
</tr>
<tr>
<td>C2.</td>
<td>$\vdash \Box(w_1 \supset w_2) \supset (\Box w_1 \supset \Box w_2)$</td>
</tr>
<tr>
<td>C3.</td>
<td>$\vdash \Box w \supset w$</td>
</tr>
<tr>
<td>C4.</td>
<td>$\vdash \Diamond \sim w \equiv \sim \Diamond w$</td>
</tr>
<tr>
<td>C5.</td>
<td>$\vdash \Diamond (w_1 \supset w_2) \supset (\Diamond w_1 \supset \Diamond w_2)$</td>
</tr>
<tr>
<td>C6.</td>
<td>$\vdash \Box w \supset \Diamond w$</td>
</tr>
<tr>
<td>C7.</td>
<td>$\vdash \Box w \supset \Box \Box w$</td>
</tr>
<tr>
<td>C8.</td>
<td>$\vdash \Box (w \supset \Diamond w) \supset (w \supset \Box w)$</td>
</tr>
<tr>
<td>C9.</td>
<td>$\vdash w_1 \mathbin{\sqcup} w_2 \equiv [w_2 \lor (w_1 \land \Diamond (w_1 \mathbin{\sqcup} w_2))]$</td>
</tr>
<tr>
<td>C10.</td>
<td>$\vdash w_1 \mathbin{\sqcup} w_2 \supset \Diamond w_2$.</td>
</tr>
</tbody>
</table>

Axioms C1 – C3 are the same as A1 – A3 in the modal system.

Axiom C4 establishes $\Box$ as self-dual. Consequently it implies that the next instant exists and is unique, and restricts our models to linear sequences (no branching).

Axiom C5 is the analogue of C2 for the $\Diamond$ operator. Axiom C6 states that the next instant is one of the reachable states, i.e., it is also part of the future. Axiom C7 is a weaker version of A4, $\vdash \Box w \supset \Box \Box w$, and can be used together with C8 to prove A4 as a theorem in this system.

Axiom C8 is the "computational induction" axiom; it states that if a property is inherited over one step transitions, it is invariant over any suffix sequence whose first state satisfies $w$. Axiom C9 defines the until operator by distributing its effect into what is implied for the present and what is implied for the next instant. Axiom C10 simply states that "$w_1$ until $w_2$" implies that $w_2$ will eventually happen.
Inference rules:

R1. If \( w \) is an instance of a propositional tautology then \( \vdash w \)
    \((Propositional Tautology - PT)\)

R2. If \( \vdash w_1 \supset w_2 \) and \( \vdash w_1 \) then \( \vdash w_2 \)
    \((Modus Ponens - MP)\)

R3. If \( \vdash w \) then \( \vdash \Box w \)
    \((\Box Insertion - \Box I)\)

These rules are identical to R1 – R3 of the modal system. Since axioms C1, C2 and C3 are identical to axioms A1, A2 and A3 and we will show later that axiom A4 is derivable in this system, it follows that all the derived rules of inference and the theorems in the modal system are also derivable in this system. Here are several additional derived rules:

\( \Box \) Insertion - \( \Box I \):

\[
\begin{array}{c}
\vdash w \\
\hline
\vdash \Box w
\end{array}
\]

proof:

1. \( \vdash w \) 
   \( \) given
2. \( \vdash \Box w \) 
   \( \) by \( \Box I \)
3. \( \vdash \Box w \) 
   \( \) by C6 and \( MP \)

\( \Box \Box \) Rules

(a) \[
\begin{array}{c}
\vdash w_1 \supset w_2 \\
\hline
\vdash \Box w_1 \supset \Box w_2
\end{array}
\]

(b) \[
\begin{array}{c}
\vdash w_1 \equiv w_2 \\
\hline
\vdash \Box w_1 \equiv \Box w_2
\end{array}
\]

proof of (a):

1. \( \vdash w_1 \supset w_2 \) 
   \( \) given
2. \( \vdash \Box (w_1 \supset w_2) \) 
   \( \) by \( \Box I \)
3. \( \vdash \Box w_1 \supset \Box w_2 \) 
   \( \) by C5 and \( MP \)

Rule (b) follows by propositional reasoning.

Computational Induction Rule - CI

\[
\begin{array}{c}
\vdash w \supset \Box w \\
\hline
\vdash w \supset \Box w
\end{array}
\]

13
proof:

1. $\vdash w \supset O w$ given
2. $\vdash \Box(w \supset O w)$ by $\Box I$
3. $\vdash \Box(w \supset O w) \supset (w \supset \Box w)$ by $C8$
4. $\vdash w \supset \Box w$ by 2, 3, and $MP$

Backward Induction Rule – BI

$\vdash O w \supset w$

$\vdash \Diamond w \supset w$

proof:

1. $\vdash O w \supset w$ given
2. $\vdash \sim w \supset \sim O w$ by $PR$
3. $\vdash \sim w \supset O \sim w$ by $C4$ and $PR$
4. $\vdash \sim w \supset \Box \sim w$ by $CI$
5. $\vdash \sim w \supset \sim \Diamond w$ by $CI$ and $PR$
6. $\vdash \Diamond w \supset w$ by $PR$

$O$ Consequence Rule – $O Q$

$\vdash w_1 \supset w_2$

$\vdash w_2 \supset O w_3$

$\vdash w_3 \supset w_4$

$\vdash w_1 \supset O w_4$

proof:

1. $\vdash w_1 \supset w_2$ given
2. $\vdash w_2 \supset O w_3$ given
3. $\vdash w_3 \supset w_4$ given
4. $\vdash O w_3 \supset O w_4$ by $OO$
5. $\vdash w_1 \supset O w_4$ by 1, 2, 4, and $PR$

Note that we do not have a $O$ concatenation rule.

A simple theorem of this system is:

$TII. \vdash O w \supset \Diamond w$

proof:

1. $\vdash (\Box \sim w) \supset (O \sim w)$ by $C8$
2. $\vdash (\sim O \sim w) \supset (\sim \Box \sim w)$ by $PR$
3. \( \vdash \Box w \supset \Diamond w \) by C1, C4, and PR

**T12.** \( \vdash \Box w \supset \Box \Box w \)

*proof:*

1. \( \vdash \Box w \supset \Box \Box w \) by C7
2. \( \vdash \Box w \supset \Box \Box w \) by CI

This is the "missing" axiom A4. We have all axioms and rules of the previous system, therefore we can deduce all theorems and derived rules of the modal system.

The following special rule is very useful in proving until theorems:

**Next to Present Rule - NP**

\[
\begin{align*}
\vdash (\Box w_1 & \equiv \Box w_2) \supset (w_1 \equiv w_2) \\
\vdash w_1 & \supset \Diamond (w_1 \land w_2) \\
\vdash w_2 & \supset \Diamond (w_1 \land w_2)
\end{align*}
\]

\[\vdash w_1 \equiv w_2\]

*proof:*

1. \( \vdash w_1 \supset \Diamond (w_1 \land w_2) \) given
2. \( \vdash w_2 \supset \Diamond (w_1 \land w_2) \) given
3. \( \vdash (w_1 \lor w_2) \supset \Diamond (w_1 \land w_2) \) by 1, 2, and PR
4. \( \vdash (w_1 \land w_2) \supset (w_1 \equiv w_2) \) by PT
5. \( \vdash \Diamond (w_1 \land w_2) \supset \Diamond (w_1 \equiv w_2) \) by \( \Diamond \Diamond \)
6. \( \vdash \Box (w_1 \equiv w_2) \supset (w_1 \equiv w_2) \) given
7. \( \vdash \Diamond (w_1 \equiv w_2) \supset (w_1 \equiv w_2) \) by BI
8. \( \vdash (w_1 \lor w_2) \supset (w_1 \equiv w_2) \) by 3, 5, 7, and PR
9. \( \vdash w_1 \equiv w_2 \) by PR

We extend now the Equivalence Rule (ER) to handle the \( \Box \) and \( \uparrow \) operators.

**Equivalence Rule - ER**

Let \( w' \) be the result of replacing an occurrence of a subformula \( v_1 \) in \( w \) by \( v_2 \). Then

\[
\vdash v_1 \equiv v_2
\]

\[\vdash w \equiv w'\]
proof:

As before, the proof is by induction on the structure of \( w \). The cases where \( w \) is \( w_1 \) or of form \( \sim u, u_1 \lor u_2, u_1 \Rightarrow u_2 \), etc. are treated as in the ER derived rule above.

Case: \( w \) is of form \( O u \). We assume that if \( \vdash v_1 \equiv v_2 \), then \( \vdash u \equiv u' \). Then by the \( O O \)-rule \( \vdash O u \equiv O u' \), i.e. \( \vdash w \equiv w' \).

The cases where \( w \) is of form \( \Box u \) and \( \Diamond u \) are proved similarly by the \( \Box \Box \)-rule and \( \Diamond \Diamond \)-rule, respectively. The case that \( w \) is of form \( u_1 \cup u_2 \) needs a more detailed proof.

Case: \( w \) is of form \( u_1 \cup u_2 \). We assume that if \( \vdash v_1 \equiv v_2 \), then \( \vdash u_1 \equiv u'_1 \) and \( \vdash u_2 \equiv u'_2 \). We attempt to use the Next to Present derived rule \( (NP) \) taking \( w_1 \) to be \( u_1 \cup u_2 \) and \( w_2 \) to be \( u'_1 \cup u'_2 \).

\[
\begin{align*}
1. & \quad \vdash u_1 \equiv u'_1, \quad \text{induction hypothesis} \\
2. & \quad \vdash u_2 \equiv u'_2, \quad \text{induction hypothesis} \\
3. & \quad \vdash u_1 \cup u_2 \equiv [u_2 \lor (u_1 \land O(u_1 \cup u_2))] \quad \text{by C9} \\
4. & \quad \vdash u'_1 \cup u'_2 \equiv [u'_2 \lor (u'_1 \land O(u'_1 \cup u'_2))] \quad \text{by C9} \\
5. & \quad \vdash u'_1 \cup u'_2 \equiv [u'_2 \lor (u'_1 \land O(u'_1 \cup u'_2))] \quad \text{by 1, 2, 4, and PR} \\
6. & \quad \vdash [O(u_1 \cup u_2) \equiv O(u'_1 \cup u'_2)] \lor [(u_1 \cup u_2) \equiv (u'_1 \cup u'_2)] \quad \text{by 3, 5, and PR} \\
7. & \quad \vdash u_1 \cup u_2 \equiv \Diamond u_2 \quad \text{by C10} \\
8. & \quad \vdash u_2 \equiv [(u_1 \cup u_2) \land (u'_1 \cup u'_2)] \quad \text{by 3, 5, and PR} \\
9. & \quad \vdash u_1 \cup u_2 \equiv \Diamond [(u_1 \cup u_2) \land (u'_1 \cup u'_2)] \quad \text{by 7, 8, and \( \Diamond Q \)} \\
10. & \quad \vdash u'_1 \cup u'_2 \equiv \Diamond u'_2 \quad \text{by C10} \\
11. & \quad \vdash u'_2 \equiv \Diamond u'_2 \quad \text{by 2 and \( \Diamond \Diamond \)} \\
12. & \quad \vdash u'_1 \cup u'_2 \equiv \Diamond u_2 \quad \text{by 10, 11, and PR} \\
13. & \quad \vdash u'_1 \cup u'_2 \equiv \Diamond [(u_1 \cup u_2) \land (u'_1 \cup u'_2)] \quad \text{by 8, 12, and \( \Diamond Q \)} \\
14. & \quad \vdash (u_1 \cup u_2) \equiv (u'_1 \cup u'_2) \quad \text{by 6, 9, 13, and \( NP \)}
\end{align*}
\]

This concludes the proof. 

\textit{\textbf{\textit{next} theorems}}

\textbf{T13.} \quad \vdash O(w_1 \land w_2) \equiv (O w_1 \land O w_2)

proof:

\[
\begin{align*}
1. & \quad \vdash O(w_1 \lor \sim w_2) \equiv (O w_1 \lor O \sim w_2) \quad \text{by C5} \\
2. & \quad \vdash \sim (O w_1 \lor O \sim w_2) \equiv \sim (O w_1 \lor O \sim w_2) \quad \text{by PR} \\
3. & \quad \vdash \sim (O w_1 \lor \sim O w_2) \equiv \sim (O w_1 \lor \sim O w_2) \quad \text{by C4 and PR} \\
4. & \quad \vdash (O w_1 \land O w_2) \equiv O(w_1 \land w_2) \quad \text{by ER} \\
5. & \quad \vdash (w_1 \land w_2) \equiv w_1 \quad \text{by PT}
\end{align*}
\]
6. \( \vdash O(w_1 \land w_2) \supset O w_1 \)

7. \( \vdash (w_1 \land w_2) \supset w_2 \)

8. \( \vdash O(w_1 \land w_2) \supset O w_3 \)

9. \( \vdash O(w_1 \land w_2) \supset (O w_1 \land O w_2) \)

10. \( \vdash O(w_1 \land w_2) \equiv (O w_1 \land O w_2) \)

\[ T14. \quad \vdash O(w_1 \lor w_2) \equiv (O w_1 \lor O w_2) \]

\[ \text{proof:} \]

1. \( \vdash O(\neg w_1 \land \neg w_2) \equiv (O \neg w_1) \land (O \neg w_2) \) by \( T13 \)

2. \( \vdash O(\neg w_1 \land \neg w_2) \equiv (\neg O w_1) \land (\neg O w_2) \) by \( C4 \) and \( PR \)

3. \( \vdash O(\neg w_1 \lor w_2) \equiv (\neg O w_1) \land (\neg O w_2) \) by \( ER \) and \( PR \)

4. \( \vdash O(\neg w_1 \lor w_2) \equiv \neg (O w_1 \lor O w_2) \) by \( C4 \) and \( PR \)

5. \( \vdash O(w_1 \lor w_2) \equiv (O w_1 \lor O w_2) \) by \( PR \)

\[ T15. \quad \vdash O(w_1 \vdash w_2) \equiv (O w_1 \vdash O w_2) \]

\[ \text{proof:} \]

1. \( \vdash O(\neg w_1 \lor w_2) \equiv (O \neg w_1) \lor (O w_2) \) by \( T14 \)

2. \( \vdash O(\neg w_1 \lor w_2) \equiv (\neg O w_1) \lor (O w_2) \) by \( C4 \) and \( PR \)

3. \( \vdash O(w_1 \vdash w_2) \equiv (O w_1 \vdash O w_2) \) by \( ER \) and \( PR \)

\[ T16. \quad \vdash O(w_1 \equiv w_2) \equiv (O w_1 \equiv O w_2) \]

\[ \text{proof:} \]

1. \( \vdash [O(w_1 \vdash w_2) \land O(w_2 \vdash w_1)] \equiv [(O w_1 \vdash O w_2) \land (O w_2 \vdash O w_1)] \)

2. \( \vdash [O(w_1 \vdash w_2) \land (w_2 \vdash w_1)] \equiv [(O w_1 \vdash O w_2) \land (O w_2 \vdash O w_1)] \)

3. \( \vdash O(w_1 \equiv w_2) \equiv (O w_1 \equiv O w_2) \) by \( T13 \) and \( PR \)

\[ T17. \quad \vdash \Box w \equiv \Box \Box w \]

\[ \text{proof:} \]

1. \( \vdash O w \vdash (w \supset O w) \) by \( PT \)

2. \( \vdash \Box \Box w \vdash \Box (w \supset O w) \) by \( \Box \Box \) and \( O O \)

3. \( \vdash \Box (w \supset O w) \vdash \Box \Box (w \supset O w) \) by \( C7 \)

4. \( \vdash O \Box (w \supset O w) \vdash O (w \supset \Box w) \) by \( C8 \) and \( O O \)

5. \( \vdash O (w \supset \Box w) \vdash (O w \supset O \Box w) \) by \( C5 \)

6. \( \vdash \Box \Box w \vdash (O w \supset \Box \Box w) \) by \( C3 \)

7. \( \vdash \Box \Box w \vdash O w \)

8. \( \vdash \Box \Box w \vdash \Box \Box w \)

17
9. \( \vdash \Box \Box w \supset \Box \Box \Box w \) by \( C7 \) and \( \Box \Box \)
10. \( \vdash \Box \Box w \supset \Box \Box \Box w \) by \( CI \)
11. \( \vdash \Box \Box w \supset w \) by \( C3 \) and \( \Box \Box \)
12. \( \vdash \Box \Box \Box w \supset \Box \Box w \) by \( CI \)
13. \( \vdash \Box \Box w \supset \Box \Box w \) by 10, 12, and \( PR \)
14. \( \vdash \Box \Box w \equiv \Box \Box w \) by 8, 13, and \( PR \)

**T18.** \( \vdash \Box \diamond w \equiv \Box \Box w \)

**proof:**
1. \( \vdash \Box \Box \sim w \equiv \Box \Box \sim w \) by \( T17 \)
2. \( \vdash \sim \Box \diamond w \equiv \sim \Box \Box w \) by \( C1, C4, \) and \( ER \)
3. \( \vdash \Box \diamond w \equiv \Box \Box w \) by \( PR \)

**T19.** \( \vdash \Box w \equiv (w \land \Box \Box w) \)

**proof:**
1. \( \vdash \Box w \supset w \) by \( C3 \)
2. \( \vdash \Box w \supset \Box \Box w \) by \( C7 \)
3. \( \vdash \Box w \supset (w \land \Box \Box w) \) by 1, 2, and \( PR \)
4. \( \vdash \Box \Box w \supset \Box (w \land \Box \Box w) \) by \( \Box \Box \)
5. \( \vdash (w \land \Box \Box w) \supset \Box (w \land \Box \Box w) \) by \( PR \)
6. \( \vdash (w \land \Box \Box w) \supset \Box (w \land \Box \Box w) \) by \( CI \)
7. \( \vdash \Box (w \land \Box \Box w) \supset (\Box \Box w \land \Box \Box \Box w) \) by \( T6 \)
8. \( \vdash \Box (w \land \Box \Box w) \supset \Box w \) by \( PR \)
9. \( \vdash (w \land \Box \Box w) \supset \Box w \) by 6, 8, and \( PR \)
10. \( \vdash \Box w \equiv (w \land \Box \Box w) \) by 3, 9, and \( PR \)

**T20.** \( \vdash \Box \Diamond w \equiv (w \lor \Box \Diamond w) \)

**proof:**
1. \( \vdash \Box \sim w \equiv (\sim w \land \Box \Box \sim w) \) by \( T19 \)
2. \( \vdash \sim \Box \Diamond w \equiv \sim (w \lor \Box \Box \sim w) \) by \( C1 \) and \( PR \)
3. \( \vdash \sim \Diamond w \equiv \sim (w \lor \Box \Diamond w) \) by \( C4, CI, \) and \( ER \)
4. \( \vdash \Diamond w \equiv (w \lor \Box \Diamond w) \) by \( PR \)

**T21.** \( \vdash (w \land \Diamond \sim w) \supset \Diamond (w \land \Box \sim w) \).

This is the dual of the "computational induction" axiom \( C8 \). It states that if \( w \) is true now and false in the future, then there exists some instant such that \( w \) is true at that instant and false at the next.

**proof:**
1. \( \vdash \Box \Diamond (w \lor \Box w) \supset (w \lor \Box \Diamond w) \) by \( C8 \)
2. \( \vdash \neg (w \circ w) \supset \neg (w \circ w) \) \hspace{1cm} \text{by PR}

3. \( \vdash (w \land \neg w) \supset \Diamond (w \land \neg w) \) \hspace{1cm} \text{by T4 and ER}

4. \( \vdash (w \land \Diamond w) \supset \Diamond (w \land \neg w) \) \hspace{1cm} \text{by T4, C4, and ER}

"until" theorems

\textbf{T22.} \( \vdash (O w_1) U (O w_2) \equiv O (w_1 U w_2) \)

Denoting

\( w_1^* : (O w_1) U (O w_2) \)

\( w_2^* : O (w_1 U w_2) \)

we have to show \( \vdash w_1^* \equiv w_2^* \). We will use the Next to Present derived rule \((NP)\).

\textbf{proof:}

1. \( \vdash w_1^* \equiv O w_2 \lor (O w_1 \land O w_1^*) \) \hspace{1cm} \text{by C9}

2. \( \vdash O (w_1 U w_2) \equiv O (w_2 \lor (w_1 \land O (w_1 U w_2))) \) \hspace{1cm} \text{by C9 and } O O

3. \( \vdash w_2^* \equiv O w_2 \lor (O w_1 \land O w_1^*) \) \hspace{1cm} \text{by 2, T13, T14, and PR}

4. \( \vdash (O w_1^* \equiv O w_2^*) \supset (w_1^* \equiv w_2^*) \) \hspace{1cm} \text{by 1, 3 and PR}

5. \( \vdash O w_2 \supset (w_1^* \land w_2^*) \) \hspace{1cm} \text{by 1, 3 and PR}

6. \( \vdash \Diamond O w_2 \supset \Diamond (w_1^* \land w_2^*) \) \hspace{1cm} \text{by } \Diamond \Diamond

7. \( \vdash (O w_1 U w_2) \supset \Diamond O w_2 \) \hspace{1cm} \text{by C10}

8. \( \vdash w_1 \supset \Diamond (w_1^* \land w_2^*) \) \hspace{1cm} \text{by 6, 7 and PR}

9. \( \vdash w_1 U w_2 \supset \Diamond w_2 \) \hspace{1cm} \text{by C10}

10. \( \vdash O (w_1 U w_2) \supset \Diamond \Diamond O w_2 \) \hspace{1cm} \text{by 9, } \Diamond \Diamond, \text{ and T18}

11. \( \vdash w_2^* \supset \Diamond (w_1^* \land w_2^*) \) \hspace{1cm} \text{by 6, 10, and PR}

12. \( \vdash w_1^* \equiv w_2^* \) \hspace{1cm} \text{by 4, 8, 11 and } NP

\textbf{T23.} \( \vdash (w_1 \land w_2) U w_3 \equiv [(w_1 U w_2) \land (w_2 U w_3)] \)

Denoting

\( w_1^* : (w_1 \land w_2) U w_3 \)

\( w_2^* : (w_1 U w_3) \land (w_2 U w_3) \)
we have to show \( \vdash w_1^* \equiv w_2^* \). We will again use the derived rule \( NP \).

**proof:**

1. \( \vdash w_1^* \equiv w_3 \lor ((w_1 \land w_2) \land \Diamond w_1^*) \quad \text{by C9} \)
2. \( \vdash w_1 \Diamond w_3 \equiv w_3 \lor (w_1 \land \Box (w_1 \land w_3)) \quad \text{by C9} \)
3. \( \vdash w_2 \Diamond w_3 \equiv w_3 \lor (w_2 \land \Box (w_2 \land w_3)) \quad \text{by C9} \)
4. \( \vdash (w_1 \Diamond w_3) \land (w_2 \Diamond w_3) \equiv w_3 \lor ((w_1 \land w_2) \land \Box(w_1 \land w_3) \land \Box(w_2 \land w_3)) \quad \text{by 2, 3, and PR} \)
5. \( \vdash w_2^* \equiv w_3 \lor ((w_1 \land w_2) \land \Diamond w_2^*) \quad \text{by C9} \)
6. \( \vdash (\Box w_1^* \equiv \Box w_2^*) \lor (w_1^* \equiv w_2^*) \quad \text{by 1, 5, and PR} \)
7. \( \vdash w_3 \lor (w_1^* \land w_2^*) \quad \text{by 1, 5, and PR} \)
8. \( \vdash \Diamond w_3 \lor (\Diamond w_1^* \land w_2^*) \quad \text{by } \Diamond \Diamond \)
9. \( \vdash (w_1 \land w_2) \Diamond w_3 \lor \Diamond w_3 \quad \text{by C10} \)
10. \( \vdash w_1^* \lor (w_1^* \land w_2^*) \quad \text{by 7, 9, and PR} \)
11. \( \vdash w_1 \Diamond w_3 \lor \Diamond w_3 \quad \text{by C10} \)
12. \( \vdash (w_1 \Diamond w_3) \land (w_2 \Diamond w_3) \lor \Diamond w_3 \quad \text{by PR} \)
13. \( \vdash w_2^* \lor (\Diamond w_1^* \land w_2^*) \quad \text{by 8, 12, and PR} \)
14. \( \vdash w_1^* \equiv w_2^* \quad \text{by 6, 10, 13, and NP} \)

**4. QUANTIFIERS**

Since we intend to use terms and predicates in our reasoning we have to extend our system to admit individual variables, terms and quantification. Let us consider additional axioms involving quantifiers and their interaction with modalities.

Axioms:

\[
\begin{align*}
D1. \quad & \vdash \neg \exists x.w \equiv \forall x.\neg w \\
D2. \quad & \vdash (\forall x.w(x)) \lor w(t) \\
& \quad \text{where } t \text{ is any term globally free for } x \text{ in } w \\
D3. \quad & \vdash (\forall x.\Box w) \lor (\Box \forall x.w) \\
D4. \quad & \vdash (\forall x.\Diamond w) \lor (\Diamond \forall x.w)
\end{align*}
\]
In these axioms \( x \) is any global individual variable. Axioms \( D1 \) and \( D2 \) are the usual predicate calculus axioms: \( D1 \) defines \( \exists \) as the dual of \( \forall \) and \( D2 \) is the instantiation axiom. Axiom \( D3 \) is known as the Barcan formula connecting the two universal operators \( \forall \) and \( \Box \). Axiom \( D4 \) is the Barcan formula for the \( \Box \) operator. The axioms state that since both operators have universal characteristics they commute.

A term \( t \) is said to be **globally free for** \( x \) in \( w \) if substitution of \( t \) for all free occurrences of \( x \) in \( w \): (a) does not create new bound occurrences of (global) variables, and (b) does not create new occurrences of local variables in the scope of a modal operator. A trivial case: if \( t \) is \( x \) itself, then \( t \) is free for \( x \). Condition (b) in this definition is essential. For, otherwise, we could derive the formula

\[
(\forall x. \Box(x < y)) \supset \Box(y < y),
\]

which is not valid for a local variable \( y \).

An additional rule of inference is:

**Inference rule:**

\[
R4. \quad \forall \text{ Insertion} - \forall I
\]

\[
\begin{array}{c}
\vdash w_1 \supset w_2 \\
\vdash w_1 \supset \forall x. w_2
\end{array}
\]

where \( x \) is not free in \( w_1 \).

We have the derived rule

\[
\text{Instantiation Rule} - \text{INST}
\]

\[
\begin{array}{c}
\vdash w(x) \\
\vdash w(t)
\end{array}
\]

where \( t \) is any term globally free for \( x \) in \( w \).

**proof:**

1. \( \vdash w(x) \) given
2. \( \vdash \forall x. w(x) \) by \( \forall I \) (taking \( w_1 \) to be true)
3. \( \vdash (\forall x. w(x)) \supset w(t) \) by \( D2 \)
4. \( \vdash w(t) \) by 2, 3, and \( MP \)

The following are the duals of \( D2 \) and \( R4 \) for the existential quantifier \( \exists \):
$\text{T24. } \vdash w(t) \supset \exists x.w(x)$

where $t$ is any term globally free for $x$ in $w$.

proof:

1. $\vdash (\forall x. \sim w(x)) \supset \sim w(t)$ by $D2$
2. $\vdash (\sim \exists x.w(x)) \supset \sim w(t)$ by $D1$ and $PR$
3. $\vdash w(t) \supset \exists x.w(x)$ by $PR$

Note that we need here again the additional condition (b) that the substitution of $t$ for $x$ in $w$ does not create new occurrences of local variables in the scope of a modal operator. For otherwise, we could deduce from $T24$

$\Box(y \leq y) \supset \exists y.\Box(y \leq y)$,

which is not valid for a local variable $y$.

$\exists$ Insertion - EI

\[ \frac{\vdash w_1 \supset w_2}{\vdash \exists x.w_1 \supset w_2} \]

where $x$ is not free in $w_2$.

proof:

1. $\vdash w_1 \supset w_2$ given
2. $\vdash \sim w_2 \supset \sim w_1$ by $PR$
3. $\vdash \sim w_2 \supset \forall x.\sim w_1$ by $\forall I (R4)$
4. $\vdash \sim w_2 \supset \sim \exists x.w_1$ by $D1$ and $PR$
5. $\vdash \exists x.w_1 \supset w_2$ by $PR$

$\forall$ Rules

\[ \frac{\vdash w_1 \supset w_2}{\vdash \forall x.w_1 \supset \forall x.w_2} \]

proof of (a):

1. $\vdash \forall x.w_1 \supset w_1$ by $D2$
2. $\vdash w_1 \supset w_2$ given
3. $\vdash \forall x.w_1 \supset w_2$ by $PR$
4. $\vdash \forall x.w_1 \supset \forall x.w_2$ by $\forall I$

Rule (b) then follows by propositional reasoning.
\[ \exists \text{ Rules:} \]

\[
\begin{align*}
(a) & \quad \vdash w_1 \supset w_2 \\
(b) & \quad \vdash \exists x. w_1 \equiv \exists x. w_2
\end{align*}
\]

\textit{proof of (a):}

1. \( \vdash w_1 \supset w_2 \) \quad \text{given}
2. \( \vdash (\sim w_2) \supset (\sim w_1) \) \quad \text{by PR}
3. \( \vdash (\forall x. \sim w_2) \supset (\forall x. \sim w_1) \) \quad \text{by \( \forall \)}
4. \( \vdash (\sim \exists x. w_2) \supset (\sim \exists x. w_1) \) \quad \text{by D1 and PR}
5. \( \vdash \exists x. w_1 \supset \exists x. w_2 \) \quad \text{by PR}

Rule (b) then follows by propositional reasoning.

The last two rules are, of course, classical rules of the predicate calculus, and are brought here only for the sake of completeness and later reference.

We extend now the Equivalence Rule (ER), given above for propositional formulas, to handle predicate formulas as well.

\textit{Equivalence Rule - ER}

Let \( w' \) be the result of replacing an occurrence of a subformula \( v_1 \) in \( w \) by \( v_2 \). Then

\[ \vdash v_1 \equiv v_2 \]

\[ \vdash w \equiv w' \]

\textit{proof:}

The proof is by induction on the structure of \( w \). The cases where \( w \) is \( w_1 \) or of form \( \sim u \), \( u_1 \lor u_2 \), \( u_1 \supset u_2 \), \( u \), \( u \), \( u \), \( u \) and \( u_1 \supset u_2 \), are treated as before.

\textit{Case:} \( w \) is of form \( \forall x. u \). We assume that if \( \vdash v_1 \equiv v_2 \), then \( \vdash u \equiv u' \). Then by the \( \forall \)-rule \( \vdash \forall x. u \equiv \forall x. u' \), i.e. \( \vdash w \equiv w' \).

The case where \( w \) is of form \( \exists x. u \), is proved similarly by the \( \exists \)-rule.

\textit{Deduction Rule - DED}

\[ \begin{array}{c}
\vdash w_1' \supset w_2 \\
\vdash w_1' \supset w_2
\end{array} \]

\[ \vdash (\Box w_1) \supset w_2 \]

where the \( \forall \) rule (Rule R4) is never applied to a free variable of \( w_1 \) in the derivation of \( w_1 \vdash w_2 \).
That is, if under the assumption \( w_1 \) we can derive \( \vdash w_2 \), where rule \( R4 \) is never applied to a free variable of \( w_1 \), then there exists a proof establishing \( \vdash (\Box w_1) \supset w_2 \). We clearly must also be careful in using any theorem or derived rule such that the \( \forall I \) rule was used in its proof.

The additional \( \Box \) operator in the conclusion is obviously necessary since in general \( w_1 \vdash w_2 \) does not imply \( \vdash w_1 \supset w_2 \). For example, obviously \( w \vdash \Box w \) is true (an immediate application of Rule \( R3: \vdash w \) by assumption and therefore \( \Box w \) by \( \Box I \)); but \( \vdash w \supset \Box w \) is false.

**proof:**

The proof of the modal Deduction Rule follows the same arguments used in the proof of the classical Deduction Rule of Predicate Calculus. We replace each line \( \vdash u_i \) in the proof of \( w_1 \vdash w_2 \) by the line \( \vdash \Box w_1 \supset u_i \), and show that this transformation preserves soundness. That is

<table>
<thead>
<tr>
<th>given</th>
<th>show</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdash u_1 )</td>
<td>( \vdash (\Box w_1) \supset u_1 )</td>
</tr>
<tr>
<td>( \vdash u_2 )</td>
<td>( \vdash (\Box w_1) \supset u_2 )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>( \vdash u_i )</td>
<td>( \vdash (\Box w_1) \supset u_i )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>( \vdash u_m )</td>
<td>( \vdash (\Box w_1) \supset u_m )</td>
</tr>
<tr>
<td>i.e. ( \vdash w_2 )</td>
<td>i.e. ( \vdash (\Box w_1) \supset w_2 )</td>
</tr>
</tbody>
</table>

where \( u_i \) is either the assumption \( w_1 \), an axiom, or derived from previous \( u_j \)'s by some rule of inference.

The proof is by a complete induction on \( i \). We assume that for all \( k < i \), \( \vdash (\Box w_1) \supset u_k \), and prove that \( \vdash (\Box w_1) \supset u_i \).

**Case:** \( u_i \) is an axiom.

1. \( \vdash u_i \)  
2. \( \vdash (\Box w_1) \supset u_i \)  
alexm by \( PR \)

Note that \( \vdash w' \) implies \( \vdash w \supset w' \) for any \( w \), by propositional reasoning.

**Case:** \( u_i \) is \( w_1 \).

1. \( \vdash (\Box w_1) \supset w_1 \)  
by \( C3 \)

**Case:** \( u_i \) is obtained by Rule \( R1 \), i.e., \( u_i \) is an instance of a tautology.

1. \( \vdash u_i \)  
by \( PT \)
2. \( \vdash (\Box w_1) \supset u_i \)  
by \( PR \)

**Case:** \( u_i \) is obtained by Rule \( R2 \) (using previous \( \vdash u_k \) and \( \vdash u_k \supset u_i \)).

1. \( \vdash (\Box w_1) \supset u_k \)  
induction hypothesis
2. \( \vdash (\Box w_1) \supset (u_k \supset u_i) \quad \text{induction hypothesis} \\
3. \vdash (\Box w_1) \supset u_i \quad \text{by 1, 2, and } PR

\text{Case: } u_i \text{ is obtained by Rule R3 (using previous } \vdash u_k, \text{ i.e., } u_i \text{ is } \Box u_k. \)

1. \( \vdash (\Box w_1) \supset u_k \quad \text{induction hypothesis} \\
2. \vdash (\Box \Box w_1) \supset \Box u_k \quad \text{by } \Box \Box \\
3. \vdash (\Box w_1) \supset (\Box \Box w_1) \quad \text{by } T12 \\
4. \vdash (\Box w_1) \supset \Box u_k \quad \text{by 2, 3, and } PR

\text{Case: } u_i \text{ is obtained by Rule R4 (using previous } \vdash u \supset v, \text{ i.e. } u_k, \text{ to get } \vdash u \supset \forall z.v, \text{ i.e. } u_i, \text{ where } z \text{ is not free in } u). \\

By our deduction rule assumption, we know also that } x \text{ is not free in } w_1.

1. \( \vdash (\Box w_1) \supset (u \supset v) \quad \text{induction hypothesis} \\
2. \vdash ((\Box w_1) \land u) \supset v \quad \text{by } PR \\
3. \vdash ((\Box w_1) \land u) \supset \forall z.v \quad \text{by } R4 \quad \text{(since } z \text{ is not free in } u \text{ or } w_1) \\
4. \vdash (\Box w_1) \supset (u \supset \forall z.v)

A different approach to coping with the application of \( \Box \) insertion rule (Rule R3) is to forbid it altogether. We then get the following restricted deduction rule:

\[
\text{Restricted Deduction Rule — } RDED \\
\frac{w_1 \vdash w_2}{\vdash w_1 \supset w_2} \\
\text{Provided } \Box I \text{ (Rule R3) is never applied and } \forall I \text{ (Rule R4) is never applied to a free variable of } w_1 \text{ in the derivation of } w_1 \vdash w_2.
\]

Here, we are not allowed to use rule \( \Box I \) or any theorem or derived rule that \( \Box I \) was used in its proof.

The proof of \( RDED \) follows exactly that of \( DED \) except that the case in which Rule R3 is applied does not arise.

**Predicate Theorems**

\( T25. \vdash (\forall z.w) \equiv (\exists x. \sim w) \)

\text{proof:}

1. \( \vdash (\sim \sim w) \equiv w \quad \text{by } PT \\
2. \vdash (\forall z. \sim \sim w) \equiv \forall z.w \quad \text{by } \forall \forall \)
3. $\vdash (\sim \exists x. \sim w) \equiv \forall x. w$
   by $D1$ and $PR$

4. $\vdash \sim \forall x. w \equiv \exists x. \sim w$
   by $PR$

**T26.** $\vdash \forall x. (w_1 \land w_2) \equiv (\forall x. w_1 \land \forall x. w_2)$

**proof:**

1. $\vdash \forall x. w_1 \supset w_1$    by $D2$
2. $\vdash \forall x. w_2 \supset w_2$    by $D2$
3. $\vdash (\forall x. w_1 \land \forall x. w_2) \supset (w_1 \land w_2)$    by 1, 2, and $PR$
4. $\vdash (\forall x. w_1 \land \forall x. w_2) \equiv \forall x. (w_1 \land w_2)$    by $\forall I$
5. $\vdash (w_1 \land w_2) \supset w_1$    by $PT$
6. $\vdash \forall x. (w_1 \land w_2) \supset \forall x. w_1$    by $\forall W$
7. $\vdash (w_1 \land w_2) \supset w_2$    by $PT$
8. $\vdash \forall x. (w_1 \land w_2) \equiv \forall x. w_2$    by $\forall W$
9. $\vdash \forall x. (w_1 \land w_2) \equiv (\forall x. w_1 \land \forall x. w_2)$    by 6, 8, and $PR$
10. $\vdash \forall x. (w_1 \land w_2) \equiv (\forall x. w_1 \land \forall x. w_2)$    by 4, 9, and $PR$

**T27.** $\vdash \exists x. (w_1 \lor w_2) \equiv (\exists x. w_1 \lor \exists x. w_2)$

**proof:**

1. $\vdash \forall x. (\sim w_1 \land \sim w_2) \equiv (\forall x. \sim w_1 \land \forall x. \sim w_2)$    by $T26$ and $\forall L$
2. $\vdash \forall x. \sim (w_1 \lor w_2) \equiv (\forall x. \sim \sim w_1 \land \forall x. \sim w_2)$    by $ER$
3. $\vdash \sim \exists x. (w_1 \lor w_2) \equiv (\sim \exists x. w_1 \land \sim \exists x. w_2)$    by $D1$ and $PR$
4. $\vdash \exists x. (w_1 \lor w_2) \equiv (\exists x. w_1 \lor \exists x. w_2)$    by $PR$

**T28.** $\vdash (\forall x. \Box w) \equiv (\Box \forall x. w)$

**proof:**

1. $\vdash (\forall x. w) \supset w$    by $D2$
2. $\vdash (\Box \forall x. w) \supset \Box w$    by $\Box\Box$
3. $\vdash (\Box \forall x. w) \equiv (\forall x. \Box w)$    by $\forall I$
4. $\vdash (\forall x. \Box w) \equiv (\Box \forall x. w)$    by $D3$
5. $\vdash (\forall x. \Box w) \equiv (\Box \forall x. w)$    by 3, 4, and $\forall R$

**alternative proof of** $\vdash (\Box \forall x. w) \equiv (\forall x. \Box w)$

1. $\vdash \forall x. w$
2. $\vdash w$    by $D2$ and $MP$
3. $\vdash \Box w$    by $\Box I$
4. $\vdash \forall x. \Box w$    by $\forall I$

Thus, $\forall x. w \vdash \forall x. \Box w$ and by the deduction rule

5. $\vdash (\Box \forall x. w) \equiv (\forall x. \Box w)$
Theorem T28 implies the commutativity of $V$ with $\Box$: Both have a universal character, with one quantifying over individuals and the other quantifying over states. Similarly, Theorem T29 implies the commutativity of $\exists$ with $\Diamond$. The last two theorems (T30 and T31) imply the commutativity of $V$ and $\exists$ with $O$.

5. EQUALITY

Equality is handled by the following axioms:

**Axioms:**

\begin{align*}
E1. & \vdash t = t \quad \text{for any term } t \\
E2. & \vdash (t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)] \quad \text{and } t_2 \text{ is any term globally free for } t_1 \text{ in } w.
\end{align*}

Axiom E1 states the reflexivity of equality. Axiom E2 states the substitutivity property of equality. We use $w(t_1, t_2)$ to indicate that $t_2$ replaces some of the occurrences of $t_1$ in $w$. 27
Recall that a term \( t_2 \) is said to be globally free for \( t_1 \) in \( w \) if substitution of \( t_2 \) for all free occurrences of \( t_1 \) in \( w \): (a) does not create new bound occurrences of (global) variables, and (b) does not create new occurrences of local variables in the scope of a modal operator.

Note that the classical axiom for substitutivity of equality \( E2 \)

\[
\vdash (t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]
\]

(where \( t_2 \) is free for \( t_1 \) in \( w \)) is not correct if \( w \) contains modal operators. We could take \( w(t_1, t_2) \) to be \( \Box(t_1 = t_2) \) and deduce from \( E2 \)

\[
\vdash (t_1 = t_2) \supset [\Box(t_1 = t_1) \equiv \Box(t_1 = t_2)],
\]

i.e.,

\[
\vdash (t_1 = t_2) \supset \Box(t_1 = t_2),
\]

which is not a valid statement (since \( t_1 = t_2 \) may contain local variables). But we have the following theorem for arbitrary formulas.

**T32. Substitutivity of Equality**

\[
\vdash \Box(t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]
\]

where \( t_2 \) is free for \( t_1 \) in \( w \).

**proof:**

By induction on the structure of \( w \).

**Case:** \( w \) contains no modal operators. Then

1. \( \vdash (t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)] \quad \text{by } E2\)
2. \( \vdash \Box(t_1 = t_2) \supset (t_1 = t_2) \quad \text{by } C3\)
3. \( \vdash \Box(t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)] \quad \text{by } MP\)

**Case:** \( w \) is of the form \( \Box u \). Then

1. \( \vdash \Box(t_1 = t_2) \supset [u(t_1, t_1) \equiv u(t_1, t_2)] \quad \text{induction hypothesis}\)
2. \( \vdash \Box(t_1 = t_2) \quad \text{assumption}\)
3. \( \vdash u(t_1, t_1) \equiv u(t_1, t_2) \quad \text{by } MP\)
4. \( \vdash \Box u(t_1, t_1) \equiv \Box u(t_1, t_2) \quad \text{by } \Box \Box\)

Thus, \( \Box(t_1 = t_2) \vdash \Box u(t_1, t_1) \equiv \Box u(t_1, t_2) \)

1. \( \vdash \Box(t_1 = t_2) \supset [\Box u(t_1, t_1) \equiv \Box u(t_1, t_2)] \quad \text{by } DED\)

28
5. \( \vdash \Box(t_1 = t_2) \supset [\Box u(t_1, t_1) \equiv \Box u(t_1, t_2)] \) by T2 and PR

The cases in which \( w \) is of the form \( 0, 0 \cdot u, 0 \cdot v, V \cdot u, 3 \cdot u \) are treated similarly, using the \( \Box \cdot \)-rule, the \( 0 \cdot 0 \)-rule, the \( \forall \forall \)-rule, and the \( \exists \exists \)-rule, respectively.

Case: \( w \) is of the form \( u \cdot u, v \cdot u, V \cdot u, 3 \cdot u \)

1. \( \vdash \Box(t_1 = t_2) \supset [u(t_1, t_1) \equiv u(t_1, t_2)] \) induction hypothesis
2. \( \vdash \Box(t_1 = t_2) \supset [v(t_1, t_1) \equiv v(t_1, t_2)] \) induction hypothesis
3. \( \vdash \Box(t_1 = t_2) \) assumption
4. \( \vdash u(t_1, t_1) \equiv u(t_1, t_2) \) by 1, 3, and MP
5. \( \vdash v(t_1, t_1) \equiv v(t_1, t_2) \) by 2, 3, and MP
6. \( \vdash [u(t_1, t_1) \cup v(t_1, t_1)] \equiv [u(t_1, t_2) \cup v(t_1, t_2)] \) by 4, 5, and ER

Thus, \( \Box(t_1 = t_2) \vdash (u(t_1, t_1) \cup v(t_1, t_1)) \equiv (u(t_1, t_2) \cup v(t_1, t_2)) \)

7. \( \vdash \Box \Box(t_1 = t_2) \supset [(u(t_1, t_1) \cup v(t_1, t_1)) \equiv (u(t_1, t_2) \cup v(t_1, t_2))] \) by DED
8. \( \vdash \Box(t_1 = t_2) \supset [(u(t_1, t_1) \cup v(t_1, t_1)) \equiv (u(t_1, t_2) \cup v(t_1, t_2))] \) by T2 and PR

T33. Commutativity of Equality

\( \vdash (t_1 = t_2) \supset (t_2 = t_1) \)

proof:

1. \( \vdash (t_1 = t_2) \supset [(t_1 = t_1) \equiv (t_2 = t_1)] \) by E2
2. \( \vdash t_1 = t_1 \) by E1
3. \( \vdash (t_1 = t_2) \supset (t_2 = t_1) \) by 1, 2, and PR

T34. Transitivity of Equality

\( \vdash [(t_1 = t_2) \land (t_2 = t_3)] \supset (t_1 = t_3) \)

proof:

1. \( \vdash (t_1 = t_2) \supset [(t_1 = t_3) \equiv (t_2 = t_3)] \) by E2
2. \( \vdash [(t_1 = t_2) \land (t_2 = t_3)] \supset (t_1 = t_3) \) by PR

T35. Term Equality

(a) \( \vdash \Box(t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \) for any term \( \tau \)
(b) \( \vdash (t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \) where \( \tau \) does not contain the next operator.
Here, \( \tau(t_2) \) is the result of replacing an occurrence of \( t_1 \) in \( \tau \) by \( t_2 \).

**proof of (a):**

1. \( \vdash \Box(t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \equiv (\tau(t_2) = \tau(t_2)) \) \hspace{1cm} by T32
2. \( \vdash \tau(t_2) = \tau(t_2) \) \hspace{1cm} by E1
3. \( \vdash \Box(t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \) \hspace{1cm} by 1, 2, and PR

**proof of (b):**

1. \( \vdash (t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \equiv (\tau(t_2) = \tau(t_2)) \) \hspace{1cm} by E2 (no \( \Box \) in \( \tau \))
2. \( \vdash \tau(t_2) = \tau(t_2) \) \hspace{1cm} by E1
3. \( \vdash (t_1 = t_2) \supset (\tau(t_1) = \tau(t_2)) \) \hspace{1cm} by 1, 2, and PR

6. **FRAME AXIOMS AND RULES**

The use of the next operator \( \Box \) applied to terms is governed by the axioms:

**Axioms:**

\[
\begin{align*}
N1. & \vdash \Box f(t_1, \ldots, t_n) = f(\Box t_1, \ldots, \Box t_n) \quad \text{for any function } f \text{ and terms } t_1, \ldots, t_n \\
N2. & \vdash \Box p(t_1, \ldots, t_n) \equiv p(\Box t_1, \ldots, \Box t_n) \quad \text{for any predicate } p \text{ and terms } t_1, \ldots, t_n \\
N3. & \vdash (t_1 = t_2) \equiv (\Box t_1 = \Box t_2)
\end{align*}
\]

Axiom \( N3 \) is a special case of \( N2 \) where \( p \) is the equality predicate.

These axioms are consistent with the evaluation rules that we gave which stated that to evaluate an expression \( \Box \xi(t_1, \ldots, t_n) \), we can evaluate \( \xi(\Box t_1, \ldots, \Box t_n) \) regardless of whether \( \xi \) is a term or a logical expression.

Recall that we split the set of our symbols into two subsets: global and local symbols. The logical consequence of this convention is the following frame axiom:

\[
\text{FA. Frame Axiom}
\]

\( \vdash z = \Box z \) for every global variable \( z \)

We can therefore prove by induction on the structure of the term \( t \) and the formula \( \psi \) the following frame theorems:
T36. For a term \( t \) and formula \( w \)

(a) \( \vdash t = \Box t \) provided \( t \) does not contain local symbols

(b) \( \vdash w \equiv \Box w \) provided \( w \) does not contain local symbols

(c) \( \vdash w(\Box y_1, \ldots, \Box y_n) \equiv \Box w(y_1, \ldots, y_n) \)

provided \( y_1, \ldots, y_n \) are all the local variables in \( w \).

A derived frame rule that we will be using is

\[
\begin{array}{c}
\text{Frame Rule: FR} \\
\frac{\vdash w_1 \supset \Diamond w_2}{\vdash (w \land w_1) \supset \Diamond (w \land w_2)}
\end{array}
\]

provided \( w \) does not contain local symbols.

proof:

1. \( \vdash w \supset \Box w \) by T36
2. \( \vdash w_1 \supset \Diamond w_2 \) given
3. \( \vdash (w \land w_1) \supset (\Box w \land \Diamond w_2) \) by 1, 2, and \( \text{PR} \)
4. \( \vdash (\Box w \land \Diamond w_2) \supset \Diamond (w \land w_2) \) by T10
5. \( \vdash (w \land w_1) \supset \Diamond (w \land w_2) \) by 3, 4, and \( \text{PR} \)

7. DOMAIN PART

The next part of the system contains domain axioms that specify the necessary properties of the domain of interest. Thus, to reason about programs manipulating natural numbers, we need the set of Peano Axioms, and to reason about trees we need a set of axioms giving the basic properties of trees and the basic operations defined on them.

An essential axiom schema for many domains is the induction axiom schema. This (and all other schemas) should be formulated to admit modal instances as subformulas. Thus the induction principle for natural numbers can be stated as follows:

\[
\begin{array}{c}
\text{Induction Axiom} \\
\frac{\vdash [R(0) \land \forall n(R(n) \supset R(n + 1))] \supset R(k)}{\text{for any statement } R}
\end{array}
\]

One instance of this principle, which will be used later, is obtained by taking \( R(n) \) to be \( \Box (Q(n) \supset \Diamond \psi) \):
Similar induction theorems exist for other domains and depend on well-founded orderings existing in those domains.

Using this induction theorem we can derive the following useful induction rule:

**Induction Rule – IND**

\[ \begin{align*}
\vdash Q(0) \supset \Diamond \psi \\
\vdash Q(n+1) \supset (\Diamond \psi \lor \Diamond Q(n)) \\
\vdash Q(k) \supset \Diamond \psi
\end{align*} \]

*IND* is useful for proving convergence of a loop: Show that \( Q(0) \) guarantees \( \Diamond \psi \) and that for each \( n \), either \( Q(n+1) \) implies \( Q(n) \) across the loop or it already establishes \( \Diamond \psi \) and no further execution is necessary. Then \( Q(k) \) ensures that the loop is executed at most \( k \) times and that \( \Diamond \psi \) is established on the last iteration or earlier.

**proof:**

1. \[ \vdash Q(0) \supset \Diamond \psi \] \hspace{1cm} given
2. \[ \vdash \Box(Q(0) \supset \Diamond \psi) \] \hspace{1cm} by \( \Box I \)
3. \[ \vdash Q(n+1) \supset (\Diamond \psi \lor \Diamond Q(n)) \] \hspace{1cm} given
4. \[ \vdash \Box(Q(n) \supset \Diamond \psi) \supset (\Box Q(n) \supset \Diamond \psi) \] \hspace{1cm} by \( T5, T3 \) and \( PR \)
5. \[ \vdash [(\Box Q(n) \supset \Diamond \psi) \land (\Diamond \psi \lor \Diamond Q(n))] \supset \Diamond \psi \] \hspace{1cm} by \( PT \)
6. \[ \vdash [Q(n+1) \land \Box(Q(n) \supset \Diamond \psi)] \supset \Diamond \psi \] \hspace{1cm} by 3, 4, 5 and \( PR \)
7. \[ \vdash \Box(Q(n) \supset \Diamond \psi) \supset (Q(n+1) \supset \Diamond \psi) \] \hspace{1cm} by \( PR \)
8. \[ \vdash \Box \Box(Q(n) \supset \Diamond \psi) \supset \Box(Q(n+1) \supset \Diamond \psi) \] \hspace{1cm} by \( \Box \Box \)
9. \[ \vdash \Box(Q(n) \supset \Diamond \psi) \supset \Box(Q(n+1) \supset \Diamond \psi) \] \hspace{1cm} by \( T2 \) and \( PR \)
10. \[ \forall n[\Box(Q(n) \supset \Diamond \psi) \supset \Box(Q(n+1) \supset \Diamond \psi)] \] \hspace{1cm} by \( \forall I \)
11. \[ \vdash \Box(Q(k) \supset \Diamond \psi) \] \hspace{1cm} by 2, 10, and Induction Theorem
12. \[ \vdash Q(k) \supset \Diamond \psi \] \hspace{1cm} by \( C3 \) and \( MP \)

32
8. PROGRAM PART

Our proof system must be augmented by additional axioms that reflect the structure of the program under consideration. These additional axioms constrain the state sequences to be exactly the set of execution sequences of the program under study. This releases us from the need to express program text syntactically in the system; all necessary information is captured by constraints on the accessibility relation that are expressed by the additional axioms.

For simplicity, we assume that the program is represented by a directed graph whose nodes are the program locations or labels and whose edges represent transitions between the labels. A transition is an instruction of the general form

\[
\begin{array}{c}
\mathcal{L} \\
\tau(\bar{y}) \rightarrow [\bar{y} := f(\bar{y})] \\
\mathcal{L}'
\end{array}
\]

Here, \(\tau(\bar{y})\) is a condition (possibly the trivial condition true) under which the transition replacing \(\bar{y}\) by \(f(\bar{y})\) should be taken, where \(\bar{y} = (y_1, \ldots, y_n)\) is the vector of program variables.

We assume that the programs are sequential and deterministic; in other words, all the conditions \(c_1, \ldots, c_k\) on transitions departing from any node are exhaustive, i.e., \(\bigvee_{i=1}^{k} c_i(\bar{y}) = \text{true}\), and mutually exclusive. In order to uniformly satisfy this requirement we add \(\text{"true} \rightarrow [\_]\) self-transitions to all the exit nodes.

A first generic axiom states that in every state \(s\), \(\forall \ell\) is true for exactly one label \(\ell\). Let \(L\) denote the set of all labels in the program; we have

\[
\text{Location Axiom - LA} \\
\sum_{\ell \in L} \forall \ell = 1.
\]

We use here the abbreviation \(\sum_{i} p_i = 1\) or \(p_1 + \cdots + p_n = 1\) to mean that exactly one of the \(p_i\)'s is true; \(p_i = 1\) if \(p_i\) is true and \(p_i = 0\) if \(p_i\) is false.

The role of the other axioms, called the transition axioms, is to introduce our knowledge about the program into the system. Since the system does not provide direct tools for speaking about programs (such as mentioning program text in Hoare's formalism or Dynamic Logic), the transition axioms represent the program by characterizing the possible state transitions under the execution of the program. For any transition:

\[
\begin{array}{c}
\mathcal{L} \\
\tau(\bar{y}) \rightarrow [\bar{y} := f(\bar{y})] \\
\mathcal{L}'
\end{array}
\]

we generate a transition axiom \(F_\alpha\). This axiom corresponds to a "forward" propagation (symbolic execution) across the transition \(\alpha\):
Forward transition axiom

\[ F_{\alpha} : \vdash \text{at}\, \ell \land c(y) \land y = u \supset \circ\text{at}\, \ell' \land y = f(u), \]

where \( u \) are auxiliary global variables.

This axiom states: If at any state, execution is at \( \ell \), \( c(y) \) holds, and the current values of \( y \) are \( u \), then at the next state we will be at \( \ell' \) with \( y = f(u) \).

A different approach that suggests an alternative axiom schema is obtained by "backward" substitution (derivation of the weakest precondition)

Backward transition axiom

\[ B_{\alpha} : \vdash \text{at}\, \ell \land c(y) \land P(f(y))] \supset \circ\text{at}\, \ell' \land P(y), \]

where \( P \) is any state predicate (i.e., without modalities).

Here \( P(f(y)) \) denotes the substitution of \( f(y) \) for all free occurrences of \( y \) in \( P(y) \). This form of the axiom expresses the effect of the transition on an arbitrary "state" predicate \( P \); i.e., a predicate \( P \) that does not contain any modal operators. It says that if \( \text{at}\, \ell \land c(y) \land P(f(y)) \) hold, then we are guaranteed to reach \( \ell' \) with \( P(y) \) on the next step.

The predicate \( P \) may not contain modalities. As a counterexample, consider the program segment

\[ t \xrightarrow{\alpha} \text{true} \rightarrow [y := 1] \xrightarrow{\alpha} \ell' \triangleleft \text{true} \rightarrow [y := 0] \]

with

\[ P'(y) : \Box (y = 1). \]

The appropriate instance of the backward axiom for \( \alpha \) is

\[ B_{\alpha} : \vdash \text{at}\, \ell \land \text{true} \land \Box (1 = 1) \supset \circ\text{at}\, \ell' \land \Box (y = 1), \]

which clearly does not correctly reflect the computation of the program.

\( F_{\alpha} \) and \( B_{\alpha} \) are equivalent and can be derived from each other. That is

For every transition \( \alpha \):

\[ B_{\alpha} \] holds for every \( P \) if and only if \( F_{\alpha} \) holds

\[ \text{proof: } B_{\alpha} \text{ for every } P \Rightarrow F_{\alpha}. \]

1. \[ \vdash \text{at}\, \ell \land c(y) \land P'(f(y))] \supset \circ\text{at}\, \ell' \land P(y) \]

by \( B_{\alpha} \), given
2. ⊢ [at\ell ∧ c(\bar{y}) ∧ f(\bar{y}) = f(\bar{u})] ⊃ □[at\ell' ∧ \bar{y} = f(\bar{u})]
   taking P(\bar{y}) to be \bar{y} = f(\bar{u}),
   where \bar{u} are auxiliary global variables

3. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u}] ⊃ [at\ell ∧ c(\bar{y}) ∧ f(\bar{y}) = f(\bar{u})]
   by T35(b) and PR

4. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u}] ⊃ □[at\ell' ∧ \bar{y} = f(\bar{u})]
   by 2, 3 and PR

which is the desired \( F_\alpha \). \( \blacksquare \)

proof: \( F_\alpha \Rightarrow B_\alpha \) for every \( P \).

Let \( P \) be an arbitrary state predicate and \( \bar{u} \) auxiliary global variables not in \( P \). Then

1. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u}] ⊃ □[at\ell' ∧ \bar{y} = f(\bar{u})]
   \( F_\alpha \), given

2. ⊢ □[at\ell ∧ \bar{y} = f(\bar{u})] ⊃ [□ at\ell' ∧ □(\bar{y} = f(\bar{u}))]
   by T13

3. ⊢ □(\bar{y} = f(\bar{u})) ⊃ ((□\bar{y}) = f(□\bar{u}))
   by N3 and N1

4. ⊢ \bar{u} = □\bar{u}
   by FA, since \( \bar{u} \) is global

5. ⊢ f(\bar{u}) = f(□\bar{u})
   by T35(b)

6. ⊢ □(\bar{y} = f(\bar{u})) ⊃ ((□\bar{y}) = f(□\bar{u}))
   by 3, 5, E2, and PR

7. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u}] ⊃ [□ at\ell' ∧ (□\bar{y}) = f(□\bar{u})]
   by 1, 2, 6, and PR

8. ⊢ [\bar{y} = \bar{u} ∧ P(f(\bar{y}))] ⊃ P(f(\bar{u}))
   by E2 (no modal operators in \( P \)) and PR

9. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u} ∧ P(f(\bar{y}))]
   ⊃ [□ at\ell' ∧ (□\bar{y}) = f(□\bar{u}) ∧ P(f(□\bar{u}))]
   by 7, 8, and PR

10. ⊢ ((□\bar{y}) = f(□\bar{u})) ⊃ (P(□\bar{y}) ≡ P(f(\bar{u})))
    by E2 and PR

11. ⊢ P(□\bar{y}) ≡ □P(\bar{y})
    by T36(c)

12. ⊢ [(□\bar{y}) = f(\bar{u}) ∧ P(f(\bar{u}))] ⊃ □ P(\bar{y})
    by 10, 11, and PR

13. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u} ∧ P(f(\bar{y}))] ⊃ [□ at\ell' ∧ □P(\bar{y})]
    by 9, 12, and PR

14. ⊢ [at\ell ∧ c(\bar{y}) ∧ \bar{y} = \bar{u} ∧ P(f(\bar{y}))] ⊃ [□ at\ell' ∧ □P(\bar{y})]
    by INST

15. ⊢ [at\ell ∧ c(\bar{y}) ∧ P(f(\bar{y}))] ⊃ [□ at\ell' ∧ □P(\bar{y})]
    by R1 and PR

16. ⊢ [at\ell ∧ c(\bar{y}) ∧ P(f(\bar{y}))] ⊃ □[at\ell' ∧ P(\bar{y})]
    by T13 and PR

which is the desired \( B_\alpha \). \( \blacksquare \)

35
We often use a weaker form of the transition axioms:

\[ P'_\alpha: \vdash [at\ell \land c(y) \land y = \bar{u}] \supset [at\ell' \land y = f(\bar{u})] \]

and

\[ B'_\alpha: \vdash [at\ell \land c(y) \land f'(\bar{y})] \supset [at\ell' \land P(\bar{y})] \]

obtained from \( P_\alpha \) and \( B_\alpha \), respectively, by replacing \( \Box \) with \( \Diamond \). The weaker forms follow by T11, i.e., \( \vdash \Box w \supset \Diamond w \).

9. THE INVARIANCE PRINCIPLE

We now present a general method for proving invariance properties of programs, i.e., properties that hold continuously throughout the execution. Such properties are expressible by formulas of form

\[ \vdash [at\ell_0 \land \phi(x)] \supset \Box Q(y). \]

That is, \( Q(y) \) is invariantly true for every computation starting at \( \ell_0 \) with input \( \bar{x} \) satisfying the precondition \( \phi(x) \).

Let \( \ell \) be any label in the program under consideration and let its outgoing transitions be of the form

\[ c_1(y) \rightarrow [y := f_1(y)] \]

\[ c_k(y) \rightarrow [y := f_k(y)] \]

\( \ell \)

\( \ell_1 \)

\( \ell_2 \)

\( \ell_k \)

\( \alpha_1 \)

\( \alpha_k \)

Recall that we assume that \( c_1(y), \ldots, c_k(y) \) are exhaustive, i.e., \( \bigvee_{i=1}^k c_i(y) = \text{true} \), and mutually exclusive. We denote by \( \mathcal{L} \) the set of all labels in \( P \). We have
Invariance Principle:

Let \( Q(y) \) be a state predicate (with no modalities) and labels describing a property of program \( P \) with input condition \( \phi(x) \).

If

(a) \( Q \) is true initially, i.e.,
\[
\vdash [\text{att}_0 \land \phi(x)] \supset Q(y)
\]

(b) \( Q \) is maintained along any transition \( \alpha \) in \( P \), i.e.,
\[
\vdash [\text{att} \land c_\alpha(y) \land Q(y)] \supset Q(f_\alpha(y)),
\]
then \( Q \) is invariantly true, i.e.,
\[
\vdash [\text{att}_0 \land \phi(x)] \supset \Box Q(y).
\]

proof:

Consider an arbitrary label \( \ell \) and an arbitrary transition \( \alpha_i \), \( 1 \leq i \leq k \), from \( \ell \) to \( \ell_i \).

1. \( \vdash [\text{att} \land c_i(y) \land Q(y)] \supset [\text{att} \land c_i(y) \land Q(f_i(y))] \) by (b) and PR
2. \( \vdash [\text{att} \land c_i(y) \land Q(f_i(y))] \supset \Diamond [\text{att} \land Q(y)] \) by \( R_\alpha \)
3. \( \vdash [\text{att} \land c_i(y) \land Q(y)] \supset \Diamond [\text{att} \land Q(y)] \) by 1, 2 and PR
4. \( \vdash [\text{att} \land c_i(y) \land Q(y)] \supset \Box Q(y) \) by \( T13 \) and PR

5. \( \vdash \forall_{i=1}^k [\text{att} \land c_i(y) \land Q(y)] \supset \Box Q(y) \) (taking the disjunction over all transitions from \( \ell \) by PR
6. \( \vdash [\text{att} \land \forall_{i=1}^k c_i(y) \land Q(y)] \supset \Box Q(y) \) by PR
7. \( \forall_{i=1}^k c_i(y) = \text{true} \) assumption
8. \( \vdash [\text{att} \land Q(y)] \supset \Box Q(y) \) by PR

9. \( \vdash \forall_{\ell \in L} [\text{att} \land Q(y)] \supset \Box Q(y) \) (taking the disjunction over all labels of \( P \)) by PR
10. \( \vdash [\forall_{\ell \in L} \text{att}] \land Q(y)] \supset \Box Q(y) \) by PR
11. \( \vdash \forall_{\ell \in L} \text{att} = \text{true} \) by Location Axiom and PR
12. \( \vdash Q(y) \supset \Box Q(y) \) by 10, 11 and PR
13. \( \vdash Q(y) \supset \Box Q(y) \) by CI
14. \( \vdash [a t \ell_0 \land \phi(z)] \supset Q(y) \) \hspace{1cm} \text{by (a)}

15. \( \vdash [a t \ell_0 \land \phi(z)] \supset \Box Q(y) \) \hspace{1cm} \text{by 13, 14 and PR}

10. EXAMPLE: INTEGER EXPONENTIATION PROGRAM

Consider for example the following program IE over the integers, which raises a real number \( x_1 \) to an integer \( x_2 \), i.e. \( x_1^{x_2} \), where \( x_2 \geq 0 \). We assume that \( 0^0 = 1 \).

**Program IE: (Integer Exponentiation):**

Let

\( \phi: a t \ell_0 \land x_2 \geq 0 \)

\( \psi: a t \ell_2 \land y_3 = x_1^{x_2} \).

We would like to use our proof system to establish the total correctness of program IE with respect to \( \phi \) and \( \psi \); we will show

\( \vdash \phi \supset \Box \psi. \)

In the proof we ignore type considerations such as \( \text{real}(x_1) \) and \( \text{integer}(x_2) \). (See [BUR], [MW]).

**PROOF 1: Using Backward Transition Axioms**

The backward transition axiom schemata corresponding to this program (taking the weaker form, with \( \Box \) rather than \( \bigcirc \)) are:

\( B'_a: \vdash [a t \ell_0 \land P(z_1, x_2, 1)] \supset \Box [a t \ell_1 \land P(y_1, y_2, y_3)] \)
\[ B^I_p : \vdash [\text{att} \ell_1 \land y_2 = 0 \land P(y_1, y_2, y_3)] \supset \Diamond [\text{att} \ell_2 \land P(y_1, y_2, y_3)] \]
\[ B^I_q : \vdash [\text{att} \ell_1 \land y_2 > 0 \land \text{odd}(y_2) \land P(y_1, y_2 - 1, y_1 \cdot y_3)] \supset \Diamond [\text{att} \ell_1 \land P(y_1, y_2, y_3)] \]
\[ B^I_s : \vdash [\text{att} \ell_1 \land y_2 > 0 \land \text{even}(y_2) \land P(y_1^2, y_2 \div 2, y_3)] \supset \Diamond [\text{att} \ell_1 \land P(y_1, y_2, y_3)]. \]

We prove

(a) \( \vdash \phi \supset \exists k.Q(k, \bar{y}) \)

(b) \( \vdash (\exists k.Q(k, \bar{y})) \supset \Diamond \psi \), or equivalently \( \vdash Q(k, \bar{y}) \supset \Diamond \psi \),

where

\[ Q(n, \bar{y}) : \text{att} \ell_1 \land (0 \leq y_2 \leq n) \land y_3 \cdot y_1 y_2 = z_1 x_2. \]

Here, \( 0 \leq y_2 \leq n \) is used to establish the termination, and \( y_3 \cdot y_1 y_2 = z_1 x_2 \) is the invariant used to establish the correctness.

Clearly, by rule \( \Diamond C \), parts (a) and (b) imply the desired result \( \vdash \phi \supset \Diamond \psi \).

**Proof of (a):**

1. \( \vdash 1 \cdot z_1 x_2 = z_1 x_2 \) by domain

2. \( \vdash \phi \supset [\text{att} \ell_0 \land x_2 \geq 0 \land 1 \cdot z_1 x_2 = z_1 x_2] \) by PR

3. \( \vdash [\text{att} \ell_0 \land x_2 \geq 0 \land 1 \cdot z_1 x_2 = z_1 x_2] \supset \Diamond [\text{att} \ell_1 \land y_2 \geq 0 \land y_3 \cdot y_1 y_2 = z_1 x_2] \) by \( B^I_p \)

   \( \text{where } P \text{ is } y_2 \geq 0 \land y_3 \cdot y_1 y_2 = z_1 x_2 \)

4. \( \vdash (y_2 \geq 0) \supset (0 \leq y_2 \leq y_2) \) by domain

5. \( \vdash [\text{att} \ell_1 \land y_2 \geq 0 \land y_3 \cdot y_1 y_2 = z_1 x_2] \supset [\text{att} \ell_1 \land (0 \leq y_2 \leq y_2) \land y_3 \cdot y_1 y_2 = z_1 x_2] \) by 4 and \( P' \)

6. \( \vdash [\text{att} \ell_1 \land y_2 \geq 0 \land y_3 \cdot y_1 y_2 = z_1 x_2] \supset \exists k[\text{att} \ell_1 \land (0 \leq y_2 \leq k) \land y_3 \cdot y_1 y_2 = z_1 x_2] \) by \( T24 \)

7. \( \vdash \phi \supset \exists k.Q(k, \bar{y}) \) by 2, 3, 6 and \( \Diamond Q \)

**Proof of (b):** We use the induction rule \( IND \):

\( (b_1) \vdash Q(0, \bar{y}) \supset \Diamond \psi \)
\( (b_2) \vdash Q(n + 1, \bar{y}) \supset [\Diamond \psi \lor \Diamond Q(n, \bar{y})] \)

\( \vdash Q(k, \bar{y}) \supset \Diamond \psi \)
proof of \((b_1)\):

8. \(\vdash \left(0 \leq y_2 \leq 0 \right) \land y_3 \cdot y_1^{y_2} = x_1^{y_2} \) \(\cup\) \(y_2 = 0 \land y_3 = x_1^{y_2}\) \hspace{2cm} \text{by domain}

9. \(\vdash Q(0,y) \supset \left[\forall \ell \land y_2 = 0 \land y_3 = x_1^{y_2}\right] \)

10. \(\vdash \left[\forall \ell \land y_2 = 0 \land y_3 = x_1^{y_2}\right] \supset \diamond \left[\forall \ell \land y_3 = x_1^{y_2}\right] \)

by \(PR\)

by \(H_\alpha\), where \(P\) is \(y_3 = x_1^{y_2}\)

11. \(\vdash Q(0,y) \supset \diamond \psi \)

by 9, 10 and \(PR\)

proof of \((b_2)\):

\begin{enumerate}
\item[] case 1: \(y_2 = 0\).

12. \(\vdash \left[0 \leq y_2 \leq 0 \right) \land y_3 \cdot y_1^{y_2} = x_1^{y_2} \cup y_2 = 0 \land y_3 = x_1^{y_2}\) 

by domain

13. \(\vdash \left[Q(n + 1,y) \land y_2 = 0\right] \cup \left[\forall \ell \land y_2 = 0 \land y_3 = x_1^{y_2}\right]\)

by \(PR\)

14. \(\vdash \left[\forall \ell \land y_2 = 0 \land y_3 = x_1^{y_2}\right] \supset \diamond \left[\forall \ell \land y_3 = x_1^{y_2}\right] \)

by \(H_\alpha\), where \(P\) is \(y_3 = x_1^{y_2}\)

15. \(\vdash \left[Q(n + 1,y) \land y_2 = 0\right] \supset \diamond \psi \)

by 13, 14 and \(PR\)

\item[] case 2: \(y_2 > 0 \land \text{odd}(y_2)\).

16. \(\vdash \left[y_2 > 0 \land \left(0 \leq y_2 \leq n + 1\right) \land y_3 \cdot y_1^{y_2} = x_1^{y_2}\right] \\
\supset \left[\left(0 \leq y_2 - 1 \leq n\right) \land (y_1 \cdot y_3) \cdot y_1^{y_2-1} = x_1^{y_2}\right] \)

by domain

17. \(\vdash \left[Q(n + 1,y) \land y_2 > 0 \land \text{odd}(y_2)\right] \supset \left[\forall \ell \land y_2 > 0 \land \text{odd}(y_2)\right] \\
\land \left(0 \leq y_2 - 1 \leq n\right) \land (y_1 \cdot y_3) \cdot y_1^{y_2-1} = x_1^{y_2}\)

by \(PR\)

18. \(\vdash \left[\forall \ell \land y_2 > 0 \land \text{odd}(y_2)\right] \supset \left[\left(0 \leq y_2 - 1 \leq n\right) \land (y_1 \cdot y_3) \cdot y_1^{y_2-1} = x_1^{y_2}\right] \\

by \(H_\alpha\), where \(P\) is \(0 \leq y_2 \leq n\) \land \(y_3 \cdot y_1^{y_2} = x_1^{y_2}\)

19. \(\vdash \left[Q(n + 1,y) \land y_2 > 0 \land \text{odd}(y_2)\right] \supset \diamond Q(n,y) \)

by 17, 18, and \(PR\)

\item[] case 3: \(y_2 > 0 \land \text{even}(y_2)\).

20. \(\vdash \left[\text{even}(y_2) \land \left(0 \leq y_2 \leq n + 1\right) \land y_3 \cdot y_1^{y_2} = x_1^{y_2}\right] \\
\supset \left[\left(0 \leq y_2 \leq n + 1\right) \land y_3 \cdot (y_1^{y_2})^{y_2+2} = x_1^{y_2}\right] \)

by domain
21. $\vdash [Q(n+1, \bar{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset [\text{atom} \land y_2 > 0 \land \text{even}(y_2) \land (0 \leq y_2 \leq 2 \leq n) \land y_3 \cdot (y_1^2)^{y_2 = z_1} = x_1 \cdot z_1]$

by PR

22. $\vdash [\text{atom} \land y_2 > 0 \land \text{even}(y_2) \land (0 \leq y_2 \leq 2 \leq n) \land y_3 \cdot (y_1^2)^{y_2 = z_1}]$

$\supset \Diamond [\text{atom} \land (0 \leq y_2 \leq n) \land y_3 \cdot y_1 \cdot y_2 = x_1 \cdot z_1]\$

by $H'_6$, where $P$ is $(0 \leq y_2 \leq n) \land (y_3 \cdot y_1 \cdot y_2 = x_1 \cdot z_1)$

23. $\vdash [Q(n+1, \bar{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset \Diamond Q(n, \bar{y})$

by 21, 22, and PR

To summarize, we showed

15. $\vdash [Q(n+1, \bar{y}) \land y_2 = 0] \supset \Diamond \psi$

case 1

19. $\vdash [Q(n+1, \bar{y}) \land y_2 > 0 \land \text{odd}(y_2)] \supset \Diamond Q(n, \bar{y})$

case 2

23. $\vdash [Q(n+1, \bar{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset \Diamond Q(n, \bar{y})$

case 3

Then since

24. $\vdash Q(n+1, \bar{y}) \supset [y_2 = 0 \lor (y_2 > 0 \land \text{odd}(y_2)) \lor (y_2 > 0 \land \text{even}(y_2))]$

by domain

it follows that

25. $\vdash Q(n+1, \bar{y}) \supset [\Diamond \psi \lor \Diamond Q(n, \bar{y})]$

by 15, 19, 23, 24 and PR

This concludes the first proof of the total correctness of our example.

PROOF 2: Using Forward Transition Axioms

For comparison, let us now prove the total correctness of program $\tilde{P}$ using the forward transition axioms. The proof turns out to be longer than the previous one using the backward axioms.

The forward transition axiom schemas corresponding to the program (taking again the weaker form, with $\Diamond$ rather than $\Box$) are:

$F'_\alpha : \vdash \text{atom} \supset \Diamond [\text{atom} \land y = (z_1, z_2, 1)]$

$F'_\beta : \vdash [\text{atom} \land y_2 = 0 \land y = \bar{y}] \supset \Diamond [\text{atom} \land y = \bar{y}]$

$F'_0 : \vdash [\text{atom} \land y_2 > 0 \land \text{odd}(y_2) \land y = \bar{y}] \supset \Diamond [\text{atom} \land y = (u_1, u_1 - 1, u_1 \cdot u_3)]$

$F'_\delta : \vdash [\text{atom} \land y_2 > 0 \land \text{even}(y_2) \land y = \bar{y}] \supset \Diamond [\text{atom} \land y = (u_1^2, u_2 + 2, u_3)]$

41
Again, let
\[ \phi : \text{att}_0 \land x_2 \geq 0 \]
\[ \psi : \text{att}_2 \land y_3 = z_1^{x_2}. \]
we would like to establish the total correctness of the program, i.e.,
\[ \vdash \phi \supset \Diamond \psi. \]

As before, we prove
\[ (a) \quad \vdash \phi \supset \Diamond \exists k.Q(k, \bar{y}) \]
\[ (b) \quad \vdash (\exists k.Q(k, \bar{y})) \supset \Diamond \psi, \quad \text{or equivalently,} \quad \vdash Q(k, \bar{y}) \supset \Diamond \psi, \]
where
\[ Q(n, \bar{y}) : \text{att}_1 \land (0 \leq y_2 \leq n) \land y_3 \cdot y_1^{y_2} = z_1^{x_2}. \]

Parts (a) and (b) implies the desired result \[ \vdash \phi \supset \Diamond \psi \] by rule \( \Diamond C \). We proceed to prove (a) and (b).

\textbf{proof of (a):}

1. \[ \vdash \text{att}_0 \supset \Diamond (\text{att}_1 \land \bar{y} = (x_1, x_2, 1)) \quad \text{by } P'_a \]
2. \[ \vdash [\text{att}_0 \land x_2 \geq 0] \supset \Diamond (\text{att}_1 \land \bar{y} = (x_1, x_2, 1) \land x_2 \geq 0) \quad \text{by } P'R \]
3. \[ \vdash x_2 \geq 0 \supset [1 \cdot x_1^{x_2} = x_1^{x_2} \land (0 \leq x_2 \leq x_2)] \quad \text{by domain} \]
4. \[ \vdash [\bar{y} = (x_1, x_2, 1) \land 1 \cdot x_1^{x_2} = x_1^{x_2} \land (0 \leq x_2 \leq x_2)] \supset [y_3 \cdot y_1^{y_2} = x_1^{x_2} \land (0 \leq y_2 \leq y_2)] \quad \text{by } E^{2} \text{ and } PR \]
5. \[ \vdash [\text{att}_1 \land \bar{y} = (x_1, x_2, 1) \land x_2 \geq 0] \supset [\text{att}_1 \land y_3 \cdot y_1^{y_2} = x_1^{x_2} \land (0 \leq y_2 \leq y_2)] \quad \text{by } 3, 4, \text{ and } PR \]
6. \[ \vdash [\text{att}_1 \land y_3 \cdot y_1^{y_2} = x_1^{x_2} \land (0 \leq y_2 \leq y_2)] \supset \exists k[\text{att}_1 \land y_3 \cdot y_1^{y_2} = x_1^{x_2} \land (0 \leq y_2 \leq k)] \quad \text{by } T^{24} \]
7. \[ \vdash [\text{att}_0 \land x_2 \geq 0] \supset \Diamond \exists k[\text{att}_1 \land y_3 \cdot y_1^{y_2} = x_1^{x_2} \land (0 \leq y_2 \leq k)] \quad \text{by } 2, 5, 6, \Diamond Q \text{ and } PR \]
\[ \text{i.e.,} \quad 7'. \quad \vdash \phi \supset \Diamond \exists k.Q(k, \bar{y}). \]

\textbf{proof of (b):} We use the induction rule \( IND: \)

42
(b₁) ⊢ Q(0, y) ⊆ ◇ψ

(b₂) ⊢ Q(n+1, y) ⊆ [◇ψ ∨ ◇Q(n, y)]

⊢ Q(k, y) ⊆ ◇ψ

In our proof we use the special consequence rule

**Consequence ◇ rule - ◇ Q**

| ⊢ w₁ ⊆ ∃u.w₂  
| ⊢ w₂ ⊆ ◇w₃  
| ⊢ ∃u.w₂ ⊆ ∃u. ◇w₃  
| ⊢ ∃u.w₂ ⊆ ◇∃u.w₃  
| ⊢ w₃ ⊆ w₄  
| ⊢ ∃u.w₃ ⊆ w₄  
| ⊢ w₁ ⊆ ◇w₄  |

where u is not free in w₄.

**proof of rule:**

(1) ⊢ w₁ ⊆ ∃u.w₂  
(2) ⊢ w₂ ⊆ ◇w₃  
(3) ⊢ ∃u.w₂ ⊆ ∃u. ◇w₃  
(4) ⊢ ∃u.w₂ ⊆ ◇∃u.w₃  
(5) ⊢ w₃ ⊆ w₄  
(6) ⊢ ∃u.w₃ ⊆ w₄  
(7) ⊢ w₁ ⊆ ◇w₄  
(8) by T29 and PR  
(9) by 3I, since u not free in w₄  
(10) by (1), (4), (6), and ◇ Q  

**proof of (b₁):**

8. ⊢ (0 ≤ y₂ ≤ 0) ⊆ (y₂ = 0)  
9. ⊢ Q(0, y) ⊆ [at l₁ ∧ y = y ∧ y₂ = 0 ∧ y₃ · y₄y₅ = z₁z₂]  
10. ⊢ Q(0, y) ⊆ ∃u.[at l₁ ∧ y = u ∧ u₂ = 0 ∧ u₃ · u₄w₅ = z₁z₂]  
11. ⊢ [at l₁ ∧ u₂ = 0 ∧ y = u] ⊆ ◇[at l₂ ∧ y = u]  
12. ⊢ [at l₁ ∧ y = u ∧ u₂ = 0 ∧ u₃ · u₄w₅ = z₁z₂]  
13. ⊢ [u₂ = 0 ∧ u₃ · u₄w₅ = z₁z₂] ⊆ u₃ = z₁z₂  
14. ⊢ [at l₂ ∧ u₂ = 0 ∧ u₃ · u₄w₅ = z₁z₂] ⊆ [at l₂ ∧ u₂ = z₁z₂]  
15. ⊢ [at l₂ ∧ y = u ∧ u₂ = 0 ∧ u₃ · u₄w₅ = z₁z₂]  

by domain  
by E₂ and PR  
by F₂, E₂, and PR  
by FR  
by domain  
by PR  
by E₂ and PR  

43
16. \( Q(0, \overline{y}) \supset \diamond \psi \)

\textit{proof of (b2):} We have to consider three cases: \( y_2 = 0 \), \( y_2 > 0 \land \text{odd}(y_2) \), and \( y_2 > 0 \land \text{even}(y_2) \).

\textit{Case 3:} \( y_2 > 0 \land \text{even}(y_2) \).

17. \( \vdash [Q(n+1, \overline{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset [\text{at} \ell_1 \land \overline{y} = \overline{y} \land y_2 > 0 \land \text{even}(y_2) \land (0 \leq y_2 \leq n + 1) \land y_3 \cdot y_1^{y_2} = x_1^{y_2}] \)

by E1 and PR

18. \( \vdash [Q(n+1, \overline{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset \exists \overline{u}. [\text{at} \ell_1 \land \overline{y} = \overline{u} \land y_2 > 0 \land \text{even}(u_2) \land (0 \leq u_2 \leq n + 1) \land u_3 \cdot u_1^{u_2} = x_1^{u_2}] \)

by T24 and PR

19. \( \vdash [\text{at} \ell_1 \land \overline{y} = \overline{u} \land y_2 > 0 \land \text{even}(u_2)] \supset \diamond [\text{at} \ell_1 \land \overline{y} = \{u_1^2, u_2 \div 2, u_3\}] \)

by F14, F2, and PR

20. \( \vdash [\text{at} \ell_1 \land \overline{y} = \overline{u} \land y_2 > 0 \land \text{even}(u_2)] \supset [\text{at} \ell_1 \land \overline{y} = \{u_1^2, u_2 \div 2, u_3\} \land \text{even}(u_2) \land (0 \leq u_2 \leq n + 1) \land u_3 \cdot u_1^{u_2} = x_1^{u_2}] \)

by P1R

21. \( \vdash [\text{even}(u_2) \land (0 \leq u_2 \leq n + 1) \land u_3 \cdot u_1^{u_2} = x_1^{u_2}] \supset [(0 \leq u_2 \leq n + 1) \land u_3 \cdot u_1^{u_2} = x_1^{u_2}] \)

by domain

22. \( \vdash [\text{at} \ell_1 \land \overline{y} = \{u_1^2, u_2 \div 2, u_3\} \land \text{even}(u_2) \land (0 \leq u_2 \leq n + 1) \land u_3 \cdot u_1^{u_2} = x_1^{u_2}] \supset [\text{at} \ell_1 \land (0 \leq y_2 \leq n) \land y_3 \cdot y_1^{y_2} = x_1^{y_2}] \)

by E2 and P1R

23. \( \vdash [Q(n+1, \overline{y}) \land y_2 > 0 \land \text{even}(y_2)] \supset \diamond Q(n, \overline{y}) \)

by 18, 20, 22, and \( \exists \diamond Q \)

To summarize, we can show

\begin{align*}
\vdash [Q(n+1, \overline{y}) \land y_2 = 0] & \supset \diamond \psi \quad \text{case 1} \\
\vdash [Q(n+1, \overline{y}) \land y_2 > 0 \land \text{odd}(y_2)] & \supset \diamond Q(n, \overline{y}) \quad \text{case 2} \\
\vdash [Q(n+1, \overline{y}) \land y_2 > 0 \land \text{even}(y_2)] & \supset \diamond Q(n, \overline{y}) \quad \text{case 3}
\end{align*}

Then since

\[ \vdash Q(n+1, \overline{y}) \supset [y_2 = 0 \lor (y_2 > 0 \land \text{odd}(y_2)) \land (y_2 > 0 \land \text{even}(y_2))] \]

by domain

it follows that

\[ \vdash Q(n+1, \overline{y}) \supset [\diamond \psi \lor \diamond Q(n, \overline{y})] \]

by P1R

This concludes the alternative proof of the total correctness of our example.
Acknowledgement

This exposition of temporal axiomatization and its application to the verification of deterministic, sequential programs emerged from work done in collaboration with Amir Pnueli on the temporal verification of concurrent programs. I wish to thank Amir for a most stimulating and enjoyable collaboration.

I am indebted to Jacques Hagelstein, Yoni Malachi, Ben Moszkowski, Pierre Wolper and Frank Yellin for their careful reading of the manuscript and for providing insightful comments. Special thanks are due to Evelyn Eldridge-Diaz for TEXing the manuscript.

REFERENCES


