Proof of the TLA Reduction Theorem

Leslie Lamport

Tue 20 Jan 1998 [16:50]

Theorem 3 *Define:*

$$\begin{array}{lcl}
R & \triangleq & M \land \mathcal{R}' \\
L & \triangleq & \mathcal{L} \land M \\
X & \triangleq & (\neg\mathcal{L}) \land M \land (\neg R') \\
M^R & \triangleq & \neg(\mathcal{R} \lor \mathcal{L}) \land M^+ \land \neg(\mathcal{R} \lor \mathcal{L})' \\
N & \triangleq & M \lor E \\
N^R & \triangleq & M^R \lor E \\
S & \triangleq & \mathit{Init} \land \Box[N]_v \\
S^R & \triangleq & \mathit{Init} \land \Box[N^R]_v \\
I & \triangleq & \land\ \mathcal{R} \Rightarrow R^+(\widehat{v}/v,\ v/v') \\
 & & \land\ \mathcal{L} \Rightarrow L^+(\widehat{v}/v') \\
 & & \land\ \neg(\mathcal{R} \lor \mathcal{L}) \Rightarrow (\widehat{v} = v) \\
 & & \land\ \neg(\mathcal{R} \lor \mathcal{L})(\widehat{v}/v) \\
Q & \triangleq & \lor\ \Box\Diamond\neg\mathcal{L} \\
 & & \lor\ \Diamond\Box[\text{FALSE}]_v\ \land\ \Diamond\Box\text{ENABLED}\,(L^+ \land \neg\mathcal{L}') \\
A_i & \triangleq & B_i \lor (\Delta_i \land M) \\
A_i^R & \triangleq & B_i \lor (\Delta_i \land M^R) \\
O & \triangleq & (\exists\, i \in \mathcal{I} : \Delta_i) \land \Box\Diamond\langle R\rangle_v \ \Rightarrow\ \Box\Diamond\neg\mathcal{R}
\end{array}$$

Assume:

1. (a) $\mathit{Init} \Rightarrow \neg(\mathcal{R} \lor \mathcal{L})$
   (b) $E \Rightarrow (\mathcal{R}' \equiv \mathcal{R}) \land (\mathcal{L}' \equiv \mathcal{L})$
   (c) $\neg(\mathcal{L} \land M \land \mathcal{R}')$
   (d) $\neg(\mathcal{R} \land \mathcal{L})$
2. (a) $R \cdot E \Rightarrow E \cdot R$
   (b) $E \cdot L \Rightarrow L \cdot E$
   (c) $\forall\, i \in \mathcal{I} : R \cdot \langle E \land B_i\rangle_v \Rightarrow \langle E \land B_i\rangle_v \cdot R$
   (d) $\forall\, i \in \mathcal{I} : \langle E \land B_i\rangle_v \cdot L \Rightarrow L \cdot \langle E \land B_i\rangle_v$

Prove: $S \land Q \land O \ \Rightarrow\ \boldsymbol{\exists}\, \widehat{v} : \Box I \land \widehat{S^R} \land (\forall\, i \in \mathcal{I} : \Box\Diamond\langle A_i\rangle_v \Rightarrow \Box\Diamond\langle \widehat{A_i^R}\rangle_{\widehat{v}})$.

Proof of the Theorem

Let m, $r_1, \ldots, r_k$, p, n and $l_1, \ldots, l_k$ be variables distinct from the variables of v and $\widehat{v}$, let r equal $\langle r_1, \ldots, r_k \rangle$, and l equal $\langle l_1, \ldots, l_k \rangle$. We also let u denote a k-tuple of bound variables, distinct from all the other variables.

We first define a temporal formula H^c which asserts that b and c are history variables chosen as follows. The initial condition I^c asserts, and it will remain true forever, that c is an infinite sequence of elements of $\mathcal{I}$ in which each element appears infinitely many times. (Such a sequence exists because $\mathcal{I}$ is at most countably infinite.) The inital value of b doesn't matter; we take it to be an arbitrary element of $\mathcal{I}$. We choose b' to be the first element i in the sequence c such that the current step is a $E \wedge B_i$ step. We define c' to be the sequence obtained from c by deleting the element b'. (If there is no such i, we let $c' = c$ and let b' be an arbitrary element $\top$ not in $\mathcal{I}$.)

$$
\begin{aligned}
\top \;&\triangleq\; \text{CHOOSE } i : i \notin \mathcal{I} \\
I^c \;&\triangleq\; \wedge\; c \in [Nat \rightarrow \mathcal{I}] \\
&\quad\;\; \wedge\; \forall n \in Nat, i \in \mathcal{I} : \exists m \in Nat : (m > n) \wedge (c[m] = i) \\
&\quad\;\; \wedge\; b \in \mathcal{I} \cup \{\top\} \\
Pos(i) \;&\triangleq\; \min\{n \in Nat : c[n] = i\} \\
N^c \;&\triangleq\; \textbf{if } E \wedge (\exists i \in \mathcal{I} : \langle B_i \rangle_v) \\
&\qquad \textbf{then } \wedge\; b' = \text{CHOOSE } i : \wedge\; (i \in \mathcal{I}) \wedge \langle B_i \rangle_v \\
&\qquad\qquad\qquad\qquad\qquad\qquad\;\; \wedge\; \forall j \in \mathcal{I} : \langle B_j \rangle_v \Rightarrow (Pos(i) \leq Pos(j)) \\
&\qquad\qquad\;\; \wedge\; c' = [n \in Nat \mapsto \textbf{if } n < Pos(b') \;\textbf{then } c[n] \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\;\; \textbf{else } c[n+1]] \\
&\qquad \textbf{else } \wedge\; b' = \textbf{if } v' = v \;\textbf{then } b \;\textbf{else } \top \\
&\qquad\qquad\;\; \wedge\; c' = c \\
H^c \;&\triangleq\; I^c \wedge \Box[N^c]_{\langle v, b, c \rangle}
\end{aligned}
$$

Note that the initial predicate I^c is actually an invariant of H^c.

For convenience, we define the action D by

$$D \;\triangleq\; \textbf{if } b' = \top \textbf{ then } E \;\textbf{ else } E \wedge \langle B_{b'} \rangle_v$$

We next define a temporal formula H^r, which asserts that r is a history variable, and a predicate I^r that we will prove is an invariant of H^r. Note that $\rho(u)$ is a state predicate, if u is a k-tuple of state functions.

$$
\begin{array}{l}
\rho(u) \;\triangleq\; (\neg\mathcal{R} \wedge R^+)(u/v, v/v') \\
N^r \;\triangleq \\
\quad r' = \textbf{if } \neg\mathcal{R}' \textbf{ then } v' \\
\qquad\qquad \textbf{else if } R \textbf{ then } r \\
\qquad\qquad\qquad \textbf{else if } \langle E\rangle_v \textbf{ then } \text{CHOOSE } u : \\
\qquad\qquad\qquad\qquad\qquad (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v') \\
\qquad\qquad\qquad\qquad \textbf{else } r \\
H^r \;\triangleq\; (r = v) \wedge \Box[N^r \wedge (v' \neq v)]_{\langle v,r\rangle} \\
I^r \;\triangleq\; \wedge\, \neg\mathcal{R} \Rightarrow (r = v) \\
\qquad\;\; \wedge\, \mathcal{R} \Rightarrow \rho(r)
\end{array}
$$

Next, we define $\mathcal{R}^p$ and $\mathcal{R}^l$, which assert that p, n, and l are prophecy variables. The prophecy variable p is an "infinite prophecy" of the form $\Box(p = F)$ for a temporal formula F. For a prophecy variable like l, the invariant I^l is part of the formula that describes the variable.

$$
\begin{array}{l}
P^p \;\triangleq\; \Box(p = \wedge\, \Box\text{ENABLED}\,(L^+ \wedge \neg\mathcal{L}') \\
\qquad\qquad\quad\; \wedge\, \Box[\text{FALSE}]_v) \\
\lambda(u) \;\triangleq\; (L^+ \wedge \neg\mathcal{L}')(u/v') \\
l_{\mathit{final}} \;\triangleq\; \text{CHOOSE } u : \lambda(u) \\
I^l \;\triangleq\; \wedge\, \neg\mathcal{L} \Rightarrow (l = v) \\
\qquad\; \wedge\, \mathcal{L} \Rightarrow \lambda(l) \\
\qquad\; \wedge\, p \Rightarrow (l = l_{\mathit{final}}) \\
N^l \;\triangleq \\
\quad l = \textbf{if } p \textbf{ then } l_{\mathit{final}} \\
\qquad\quad \textbf{else if } \neg\mathcal{L} \textbf{ then } v \\
\qquad\qquad\quad \textbf{else if } L \textbf{ then } l' \\
\qquad\qquad\qquad\quad \textbf{else if } \langle E\rangle_v \\
\qquad\qquad\qquad\qquad \textbf{then } \text{CHOOSE } u : \\
\qquad\qquad\qquad\qquad\qquad \wedge\, \lambda(u) \\
\qquad\qquad\qquad\qquad\qquad \wedge\, D(u/v, l'/v') \\
\qquad\qquad\qquad\qquad \textbf{else } l' \\
P^l \;\triangleq\; \Box I^l \wedge \Box[N^l \wedge (\langle p, v\rangle' \neq \langle p, v\rangle)]_{\langle v,b,c,p,l\rangle}
\end{array}
$$

Note that the symmetric relation between the history variable r and the prophecy variable p becomes more apparent if, in the definition of N^r, we replace the expression $R^+(u/v)$ with the equivalent expression $\rho(u)'$. (The expressions are equivalent because the bound variable u in the expression CHOOSE u : ... is by definition a constant, so $u' = u$.)

We also define the action N^p and predicate I^p, which play the role of next-state relation and invariant for P^p.

$$\begin{array}{rcl} N^p & \triangleq & \wedge\ p \Rightarrow (v' = v) \\ & & \wedge\ (v' = v) \Rightarrow (p' = p) \\ I^p & \triangleq & p \Rightarrow (\exists\, u : \lambda(u)) \end{array}$$

For convenience, we combine all these next-state relations and invariants with the following definitions

$$\begin{array}{rcl} all & \triangleq & \langle v, b, c, r, p, l \rangle \\ N^{all} & \triangleq & (v' \neq v) \wedge N \wedge N^c \wedge N^r \wedge N^p \wedge N^l \\ I^{all} & \triangleq & I^c \wedge I^r \wedge I^l \end{array}$$

We also define X by

$$X \triangleq \neg\mathcal{L} \wedge M \wedge \neg\mathcal{R}'$$

Finally, we define our refinement mapping $\overline{v}$ by

$$\overline{v} \triangleq \textbf{if } \mathcal{R} \textbf{ then } r \textbf{ else if } \mathcal{L} \textbf{ then } l \textbf{ else } v$$

We use the following simple observations. If v is the tuple of all variables that appear in the actions A and B, then for any u_1 and u_2,

$$(A \cdot B)(u_1/v, u_2/v') \equiv \exists\, w : A(u_1/v, w/v') \wedge B(w/v, u_2/v') \tag{1}$$

The proof of the theorem follows.

$\langle 1 \rangle 1.$ 1. $(I^c)' \wedge N^c \wedge E \wedge \rho(r) \Rightarrow \exists\, u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$
2. $(I^c)' \wedge N^c \wedge E \wedge \lambda(l)' \Rightarrow \exists\, u : \lambda(u) \wedge D(u/v, l'/v')$
3. $\forall\, u : (R^+(u/v, v/v') \Rightarrow \neg\mathcal{L})$
4. $M \equiv R \vee X \vee L$

$\langle 2 \rangle 1.$ ASSUME: $(I^c)' \wedge N^c \wedge E \wedge \rho(r)$
PROVE: $\exists\, u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$

$\langle 3 \rangle 1.$ $R \cdot D \Rightarrow D \cdot R$
PROOF: Assumption $\langle 2 \rangle$ (which implies $b' \in \mathcal{I} \cup \{\top\}$), the definition of D, and hypotheses 2(a) (if $b' = \top$) and 2(c) (if $b' \in \mathcal{I}$).

$\langle 3 \rangle 2.$ $R^+ \cdot D \Rightarrow D \cdot R^+$
PROOF: By induction from $\langle 3 \rangle 1$ and the associativity of "·".

$\langle 3 \rangle 3.$ $(\neg\mathcal{R} \wedge R^+) \cdot D \Rightarrow D \cdot (\neg\mathcal{R} \wedge R^+)$

PROOF:

$$\begin{array}{rcll} (\neg\mathcal{R} \wedge R^+) \cdot D & \equiv & \neg\mathcal{R} \wedge (R^+ \cdot D) & \text{By (1).} \\ & \Rightarrow & \neg\mathcal{R} \wedge (D \cdot R^+) & \text{By } \langle 3\rangle 2. \\ & \equiv & (\neg\mathcal{R} \wedge D) \cdot R^+ & \text{By (1).} \\ & \Rightarrow & (D \wedge \neg\mathcal{R}') \cdot R^+ & \text{By hypothesis 1(b), since } D \Rightarrow E. \\ & \equiv & D \cdot (\neg\mathcal{R} \wedge R^+) & \text{By (1).} \end{array}$$

$\langle 3\rangle 4$. Q.E.D.

PROOF: By assumption $\langle 2\rangle$, since

$$\begin{array}{lll} \rho(r) \wedge E & & \\ \quad \Rightarrow & \rho(r) \wedge D & \text{Assumption } \langle 2\rangle \text{ and def of } N^c. \\ \quad \equiv & (\neg\mathcal{R} \wedge R^+)(r/v, v/v') \wedge D & \text{Definition of } \rho. \\ \quad \Rightarrow & ((\neg\mathcal{R} \wedge R^+) \cdot D)(r/v) & \text{By (1).} \\ \quad \Rightarrow & (D \cdot (\neg\mathcal{R} \wedge R^+))(r/v) & \text{By } \langle 3\rangle 3. \\ \quad \equiv & \exists\, u : D(r/v, u/v') \wedge (\neg\mathcal{R} \wedge R^+)(u/v) & \text{By (1).} \end{array}$$

$\langle 2\rangle 2$. ASSUME: $(I^c)' \wedge N^c \wedge E \wedge \lambda(l)'$

PROVE: $\exists\, u : (\lambda(u) \wedge D)(u/v, l'/v')$

$\langle 3\rangle 1$. $D \cdot L \Rightarrow L \cdot D$

PROOF: Assumption $\langle 2\rangle$ (which implies $b' \in \mathcal{I} \cup \{\top\}$), the definition of D, and Hypotheses 2(b) (if $b' = \top$) and 2(d) (if $b' \in \mathcal{I}$).

$\langle 3\rangle 2$. $D \cdot L^+ \Rightarrow L^+ \cdot D$

PROOF: By induction from $\langle 3\rangle 1$ and the associativity of "$\cdot$".

$\langle 3\rangle 3$. $\forall\, u, w : D(u/v, w/v') \wedge \neg\mathcal{L}(w/v) \Rightarrow \neg\mathcal{L}(u/v)$

PROOF: Hypothesis 1(b) (which implies $E \wedge \mathcal{L} \Rightarrow \mathcal{L}'$), since assumption $\langle 2\rangle$ and the definition of D imply $D \Rightarrow E$.

$\langle 3\rangle 4$. Q.E.D.

PROOF: By assumption $\langle 2\rangle$, since

$$\begin{array}{lll} (\lambda(l))' \wedge E & & \\ \quad \Rightarrow & (\lambda(l))' \wedge D & \text{Assumption } \langle 2\rangle \text{ and def of } N^c. \\ \quad \equiv & L^+(v'/v, l'/v') \wedge \neg\mathcal{L}(l'/v) \wedge D & \text{By definition of } \lambda. \\ \quad \Rightarrow & (D \cdot L^+)(l'/v') \wedge \neg\mathcal{L}(l'/v) & \text{By (1).} \\ \quad \Rightarrow & (L^+ \cdot D)(l'/v') \wedge \neg\mathcal{L}(l'/v) & \text{By } \langle 3\rangle 2. \\ \quad \Rightarrow & \exists\, u : L^+(u/v') \wedge D(u/v, l'/v') \wedge \neg\mathcal{L}(l'/v) & \text{By (1).} \\ \quad \Rightarrow & \exists\, u : L^+(u/v') \wedge D(u/v, l'/v') \wedge \neg\mathcal{L}(u/v) & \text{By } \langle 3\rangle 3 \\ \quad \equiv & \exists\, u : \lambda(u) \wedge D(u/v, l'/v') & \text{By definition of } \lambda. \end{array}$$

$\langle 2\rangle 3$. ASSUME: u a $k-$tuple of constants

PROVE: $R^+(u/v, v/v') \Rightarrow \neg\mathcal{L}$

$\langle 3\rangle 1$. $R(u/v, v/v') \;\Rightarrow\; \neg\mathcal{L}$

PROOF: By definition, R implies $\mathcal{R}'$, so $R(u/v, v/v')$ implies $\mathcal{R}$, which by hypothesis 1(d) implies $\neg\mathcal{L}$.

$\langle 3\rangle 2$. Q.E.D.

PROOF: $\langle 3 \rangle 1$, by induction on k.

$\langle 2 \rangle 4.$ $M \equiv R \lor X \lor L$

PROOF:
$$\begin{aligned} M &\equiv (\neg\mathcal{L} \land M \land \mathcal{R}') \lor (\neg\mathcal{L} \land M \land \neg\mathcal{R}') \lor (\mathcal{L} \land M) \\ &\qquad \text{Propositional logic.} \\ &\equiv (M \land \mathcal{R}') \lor (\neg\mathcal{L} \land M \land \neg\mathcal{R}') \lor (\mathcal{L} \land M) \\ &\qquad \text{Hypothesis 1(c).} \\ &\equiv R \lor X \lor L \\ &\qquad \text{Definitions of } R,\ X, \text{ and } L. \end{aligned}$$

$\langle 2 \rangle 5.$ Q.E.D.

PROOF: $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, and $\langle 2 \rangle 4$.

$\langle 1 \rangle 2.$ $P^p \Rightarrow \Box[N^p]_{\langle v,p \rangle} \land \Box I^p$

$\langle 2 \rangle 1.$ $P^p \Rightarrow \Box[N^p]_{\langle v,p \rangle}$

PROOF: This is semantically obvious, since $v = v'$ implies
$$\text{ENABLED}\,(L^+ \land \neg\mathcal{L}') \equiv (\text{ENABLED}\,(L^+ \land \neg\mathcal{L}'))'$$
but I don't know how to derive it from more primitive proof rules.

$\langle 2 \rangle 2.$ $P^p \Rightarrow \Box I^p$

PROOF: Follows from the definitions of P^p and I^p by simple temporal reasoning, since ENABLED $(L^+ \land \neg\mathcal{L}')$ is equivalent to $\exists\, u : \lambda(u)$.

$\langle 2 \rangle 3.$ Q.E.D.

PROOF: $\langle 2 \rangle 1$ and $\langle 2 \rangle 2$.

$\langle 1 \rangle 3.$ $\boldsymbol{\exists}\, b, c : H^c \land \Box I^c$

$\langle 2 \rangle 1.$ $\boldsymbol{\exists}\, b, c : H^c$

PROOF: By the standard rule for adding history variables.

$\langle 2 \rangle 2.$ $H^c \Rightarrow \Box I^c$

$\langle 3 \rangle 1.$ $I^c \land [N^c]_{\langle v,c \rangle} \Rightarrow (I^c)'$

PROOF: Immediate from the definitions.

$\langle 3 \rangle 2.$ Q.E.D.

PROOF: $\langle 3 \rangle 1$ and the TLA invariance rule.

$\langle 2 \rangle 3.$ Q.E.D.

PROOF: $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, and predicate logic.

$\langle 1 \rangle 4.$ $\Box I^c \land H^c \land S \Rightarrow \boldsymbol{\exists}\, r : H^r \land \Box I^r$

$\langle 2 \rangle 1.$ $\boldsymbol{\exists}\, r : H^r$

PROOF: By the rules for history variables.

$\langle 2 \rangle 2.$ $\Box I^c \land H^c \land S \land H^r \Rightarrow \Box I^r$

$\langle 3 \rangle 1.$ ASSUME: $(I^c)' \land N^c \land N \land N^r \land (v' \neq v) \land I^r$

PROVE: $(I^r)'$

$\langle 4 \rangle 1.$ CASE: $E \land \neg R$

$\langle 5 \rangle 1.$ CASE: $\mathcal{R}$

$\langle 6 \rangle 1.$ $\mathcal{R}'$

PROOF: Assumptions $\langle 5 \rangle$ and $\langle 4 \rangle$ and hypothesis 1(b) (which implies $E \wedge \mathcal{R} \Rightarrow \mathcal{R}'$).

⟨6⟩2. $r' = \text{CHOOSE } u : (\neg\mathcal{R} \wedge R^{+})(u/v) \wedge D(r/v, u/v')$

PROOF: ⟨6⟩1, assumption ⟨4⟩ ($\neg R$), assumption ⟨3⟩ (which asserts $(v' \neq v) \wedge N^{r}$), and the definition of N^{r}.

⟨6⟩3. $\rho(r)$

PROOF: Assumptions ⟨5⟩ and ⟨3⟩ (which asserts I^{r}), and the definition of I^{r}.

⟨6⟩4. $(\neg\mathcal{R} \wedge R^{+})(r'/v)$

PROOF: ⟨6⟩2, ⟨6⟩3, assumptions ⟨3⟩ (which asserts $(I^{c})' \wedge N^{c}$) and ⟨4⟩, and ⟨1⟩1.1.

⟨6⟩5. Q.E.D.

PROOF: ⟨6⟩4 implies $\rho(r)'$, since $(\neg\mathcal{R} \wedge R^{+})(r'/v) = (\neg\mathcal{R} \wedge R^{+})(r'/v, v'/v') = (\neg\mathcal{R} \wedge R^{+})(r/v, v/v')' = \rho(r)'$. The level-⟨3⟩ goal then follows from ⟨6⟩1 and the definition of I^{r}.

⟨5⟩2. CASE: $\neg\mathcal{R}$

⟨6⟩1. $\neg\mathcal{R}'$

PROOF: Assumptions ⟨5⟩ and ⟨4⟩ and hypothesis 1(b) (which implies $E \wedge \mathcal{R}' \Rightarrow \mathcal{R}$).

⟨6⟩2. $r' = v'$

PROOF: ⟨6⟩1, assumption ⟨3⟩ (which asserts N^{r}), and the definition of N^{r}.

⟨6⟩3. Q.E.D.

PROOF: ⟨6⟩1, ⟨6⟩2, and the definition of I^{r} imply tle level-⟨3⟩ goal.

⟨5⟩3. Q.E.D.

PROOF: Immediate from ⟨5⟩1 and ⟨5⟩2.

⟨4⟩2. CASE: R

⟨5⟩1. $r' = r$

PROOF: Assumption ⟨3⟩ (which asserts N^{r}), assumption ⟨4⟩, which by definition of R implies $\mathcal{R}'$, and the definition of N^{r}.

⟨5⟩2. CASE: $\mathcal{R}$

⟨6⟩1. $\rho(r) \wedge R \Rightarrow \rho(r)'$

PROOF:

$$\begin{array}{rcll}
\rho(r) \wedge R & \equiv & (\neg\mathcal{R} \wedge R^{+})(r/v, v/v') \wedge R & \text{By definition of } \rho. \\
& \Rightarrow & ((\neg\mathcal{R} \wedge R^{+}) \cdot R)(r/v) & \text{By (1).} \\
& \equiv & (\neg\mathcal{R} \wedge (R^{+} \cdot R))(r/v) & \text{By (1).} \\
& \Rightarrow & (\neg\mathcal{R} \wedge R^{+})(r/v) & \text{By definition of } ^{+}. \\
& \equiv & (\neg\mathcal{R} \wedge R^{+})(r'/v, v'/v') & \text{By } \langle 5 \rangle 1. \\
& \equiv & (\rho(r))' & \text{By definition of } \rho.
\end{array}$$

⟨6⟩2. Q.E.D.

PROOF: Assumptions $\langle 5 \rangle$ and $\langle 3 \rangle$ (which asserts I^r) imply $\rho(r)$. The level-$\langle 3 \rangle$ goal then follows from assumption $\langle 4 \rangle$ (which, by definition of R, implies $\mathcal{R}'$), step $\langle 6 \rangle 1$, and the definition of I^r.

$\langle 5 \rangle 3$. CASE: $\neg \mathcal{R}$

$\langle 6 \rangle 1$. $r = v$

PROOF: Assumptions $\langle 5 \rangle$ and $\langle 3 \rangle$ (which asserts I^r) and the definition of I^r.

$\langle 6 \rangle 2$. $R(r'/v, v'/v')$

PROOF: By assumption $\langle 4 \rangle$, since $\langle 6 \rangle 1$ and $\langle 5 \rangle 1$ imply $r' = v$.

$\langle 6 \rangle 3$. $\rho(r)'$

PROOF: By assumption $\langle 5 \rangle$ and $\langle 6 \rangle 2$, since R implies R^+ and $(\neg \mathcal{R} \wedge R^+)(r'/v, v'/v') = (\neg \mathcal{R} \wedge R^+)(r/v, v/v')' = \rho(r)'$.

$\langle 6 \rangle 4$. Q.E.D.

PROOF: $\langle 6 \rangle 3$, assumption $\langle 4 \rangle$ (which implies $\mathcal{R}'$), and the definition of I^r imply the level-$\langle 3 \rangle$ goal.

$\langle 5 \rangle 4$. Q.E.D.

PROOF: Immediate from $\langle 5 \rangle 2$ and $\langle 5 \rangle 3$.

$\langle 4 \rangle 3$. CASE: $\neg \mathcal{R}'$

$\langle 5 \rangle 1$. $r' = v'$

PROOF: Assumption $\langle 3 \rangle$ (which asserts N^r), assumption $\langle 4 \rangle$, and the definition of N^r.

$\langle 5 \rangle 2$. Q.E.D.

PROOF: $\langle 5 \rangle 1$, assumption $\langle 4 \rangle$, and the definition of I^r imply our level-$\langle 3 \rangle$ goal.

$\langle 4 \rangle 4$. Q.E.D.

$\langle 5 \rangle 1$. $N \equiv (E \wedge \neg R) \vee R \vee (M \wedge \neg \mathcal{R}')$

PROOF:
$$
\begin{aligned}
N &\equiv E \vee M && \text{By definition of } N.\\
&\equiv E \vee (M \wedge \mathcal{R}') \vee (M \wedge \neg \mathcal{R}') && \text{By predicate logic.}\\
&\equiv E \vee R \vee (M \wedge \neg \mathcal{R}') && \text{By definition of } R.\\
&\equiv (E \wedge \neg R) \vee R \vee (M \wedge \neg \mathcal{R}') && \text{By propositional logic.}
\end{aligned}
$$

$\langle 5 \rangle 2$. Q.E.D.

PROOF: By $\langle 5 \rangle 1$ and assumption $\langle 3 \rangle$ (which asserts N), cases $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, and $\langle 4 \rangle 3$ are exhaustive.

$\langle 3 \rangle 2$. $I^r \wedge \text{UNCHANGED } \langle v, r \rangle \Rightarrow (I^r)'$

PROOF: Immediate, since v and r are the only free variables of I^r.

$\langle 3 \rangle 3$. Q.E.D.

PROOF: By $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, the definition of H^r, and the usual TLA invariance rule.

$\langle 2 \rangle 3$. Q.E.D.

PROOF: ⟨2⟩1 and ⟨2⟩2 and predicate logic.

⟨1⟩5. $\Box I^c \land H^c \land S \land Q \Rightarrow \mathbf{\exists}\, p, l : P^p \land P^l$

⟨2⟩1. $\mathbf{\exists}\, p : P^p$

PROOF: By the following rule for adding "infinite prophecy" variables:

If p does not occur free in the temporal formula F, then $\mathbf{\exists}\, p : \Box(p = F)$.

⟨2⟩2. $\Box I^c \land H^c \land Q \land S \land P^p \Rightarrow \mathbf{\exists}\, l : P^l$

⟨3⟩1. $I^p \land p \Rightarrow I^l$

⟨4⟩1. $I^p \land p \Rightarrow \lambda(l_{final})$

PROOF: By definition of I^p and l_{final}.

⟨4⟩2. $\lambda(l_{final}) \Rightarrow \mathcal{L}$

PROOF: By definition of λ, since L^+ equals $(\mathcal{L} \land M)^+$ (by definition of L), which implies $\mathcal{L}$.

⟨4⟩3. Q.E.D.

PROOF: ⟨4⟩1, ⟨4⟩2, and the definition of I^l

⟨3⟩2. $Q \land P^p \Rightarrow \Box\Diamond(\exists\,!u : I^l(u/l))$

⟨4⟩1. $\Box I^p \land \Box\Diamond\neg\mathcal{L} \Rightarrow \Box\Diamond(\exists\,!u : I^l(u/l))$

⟨5⟩1. $I^p \land \neg\mathcal{L} \Rightarrow \neg p$

PROOF: $I^p \land p \Rightarrow (\exists\, u : \lambda(u)) \Rightarrow L^+ \Rightarrow \mathcal{L}$.

⟨5⟩2. $I^p \land \neg\mathcal{L} \Rightarrow (\exists\,!u : I^l(u/l))$

PROOF: ⟨5⟩1 and the definition of I^l imply $I^l(u/l) \equiv (u = v)$.

⟨5⟩3. Q.E.D.

PROOF: ⟨5⟩2 and temporal reasoning.

⟨4⟩2. $\Box I^p \land \Box p \Rightarrow \Box(\exists\,!u : I^l(u/l))$

⟨5⟩1. $I^l \land p \Rightarrow (l = l_{final})$

PROOF: Definition of I^l

⟨5⟩2. $I^p \land p \Rightarrow (\exists\,!u : I^l(u/l))$

PROOF: Immediate from ⟨5⟩1 and ⟨3⟩1.

⟨5⟩3. Q.E.D.

PROOF: ⟨5⟩2 and simple temporal reasoning.

⟨4⟩3. $Q \land P^p \Rightarrow (\Box\Diamond\neg\mathcal{L}) \lor \Diamond\Box p$

PROOF: By definition of Q and P^p.

⟨4⟩4. Q.E.D.

PROOF: By ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨1⟩2 (which implies $P^p \Rightarrow \Box I^p$), and simple temporal reasoning.

⟨3⟩3. $\Box I^c \land H^c \land S \land P^p \Rightarrow \Box[(I^l)' \land (v' \neq v) \Rightarrow \exists\, u : N^l(u/l) \land I(u/l)]_v$

⟨4⟩1. ASSUME: $(I^c)' \land N^c \land N \land I^p \land N^p \land (I^l)' \land (v' \neq v)$
PROVE: $\exists\, u : N^l(u/l) \land I^l(u/l)$

⟨5⟩1. $\neg p$

PROOF: Assumption ⟨4⟩, since $N^p \wedge (v' \neq v)$ implies $\neg p$.

⟨5⟩2. CASE: $\neg \mathcal{L}$

⟨6⟩1. $I^l(v/l) \wedge N^l(v/l)$

PROOF: ⟨5⟩1, assumption ⟨5⟩, and the definitions of I^l and N^l.

⟨6⟩2. Q.E.D.

PROOF: Immediate from ⟨6⟩1.

⟨5⟩3. CASE: $\mathcal{L}$

⟨6⟩1. CASE: $E \wedge \neg L$

⟨7⟩1. $\mathcal{L}'$

PROOF: Assumptions ⟨6⟩ and ⟨5⟩ and hypothesis 1(b) (which implies $E \wedge \mathcal{L} \Rightarrow \mathcal{L}'$).

⟨7⟩2. $\exists\, u : \lambda(u) \wedge D(u/v, l'/v')$

PROOF: ⟨7⟩1 and assumption ⟨4⟩ (which asserts $(I^l)'$) imply $\lambda(l)'$. The result follows from $\lambda(l)'$, assumptions ⟨6⟩ and ⟨4⟩ (which implies $(I^c)' \wedge N^c$), and ⟨1⟩1.2.

⟨7⟩3. Q.E.D.

LET: $u \triangleq$ CHOOSE $u : \lambda(u) \wedge D(u/v, l'/v')$

⟨8⟩1. $N^l \equiv (l = u)$

PROOF: ⟨5⟩1, assumption ⟨5⟩, assumption ⟨6⟩, assumption ⟨4⟩ (which implies $v' \neq v$), and the definition of N^l.

⟨8⟩2. $N^l(u/l)$

PROOF: By ⟨8⟩1.

⟨8⟩3. $\lambda(u)$

PROOF: ⟨7⟩2 and the definition of u.

⟨8⟩4. $I^l(u/l)$

PROOF: ⟨8⟩3, assumption ⟨5⟩, ⟨5⟩1, and the definition of I^l.

⟨8⟩5. Q.E.D.

PROOF: ⟨8⟩2 and ⟨8⟩4 imply the level-⟨4⟩ goal.

⟨6⟩2. CASE: L

⟨7⟩1. CASE: $\mathcal{L}'$

⟨8⟩1. $(\lambda(l))' \wedge L \Rightarrow \lambda(l')$

PROOF: $(\lambda(l))' \land L$

$$\equiv \; L^+(v'/v, l'/v') \land \neg\mathcal{L}(l'/v) \land L$$

By definition of λ

$$\Rightarrow \; (L \cdot L^+)(l'/v') \land \neg\mathcal{L}(l'/v)$$

By (1).

$$\Rightarrow \; (L^+)(l'/v') \land \neg\mathcal{L}(l'/v)$$

By definition of A^+ for an action A.

$$\equiv \; \lambda(l')$$

By definition of λ

$\langle 8\rangle 2.$ $\lambda(l')$

PROOF: Assumption $\langle 4\rangle$ implies $(I^l)'$, which by assumption $\langle 7\rangle$ implies $(\lambda(l))'$. By $\langle 8\rangle 1$, $(\lambda(l))'$ and assumption $\langle 6\rangle$ imply $\lambda(l')$.

$\langle 8\rangle 3.$ $I^l(l'/l)$

PROOF: $\langle 5\rangle 1$ and assumption $\langle 5\rangle$ imply $I^l \equiv \lambda(l)$, so $\langle 8\rangle 2$ implies $I^l(l'/l)$.

$\langle 8\rangle 4.$ $N^l(l'/l)$

PROOF: $\langle 5\rangle 1$, assumptions $\langle 5\rangle$ and $\langle 6\rangle$ imply $N^l \equiv (l = l')$, so $N^l(l'/l) \equiv (l' = l')$.

$\langle 8\rangle 5.$ Q.E.D.

PROOF: $\langle 8\rangle 3$ and $\langle 8\rangle 4$ imply the level-$\langle 4\rangle$ goal.

$\langle 7\rangle 2.$ CASE: $\neg\mathcal{L}'$

$\langle 8\rangle 1.$ $l' = v'$

PROOF: Assumption $\langle 4\rangle$ (which implies $(I^l)'$), assumption $\langle 7\rangle$, and the definition of I^l.

$\langle 8\rangle 2.$ $\lambda(v')$

PROOF: Assumption $\langle 6\rangle$ implies L^+, which with assumption $\langle 7\rangle$ implies $(L^+ \land \neg\mathcal{L}')(v'/v')$, which equals $\lambda(v')$.

$\langle 8\rangle 3.$ $I^l(v'/l)$

PROOF: $\langle 5\rangle 1$ and assumption $\langle 5\rangle$ imply $I^l \equiv \lambda(l)$, so $\langle 8\rangle 2$ implies $I^l(v'/l)$.

$\langle 8\rangle 4.$ $N^l(v'/l)$

PROOF: $\langle 5\rangle 1$, assumption $\langle 5\rangle$, and assumption $\langle 6\rangle$ imply $N^l \equiv (l = l')$. By $\langle 8\rangle 1$, this implies $N^l \equiv (l = v')$, so $N^l(v'/l) \equiv (v' = v')$.

$\langle 8\rangle 5.$ Q.E.D.

PROOF: $\langle 8\rangle 3$ and $\langle 8\rangle 4$ imply the level-$\langle 4\rangle$ goal.

$\langle 7\rangle 3.$ Q.E.D.

PROOF: Immediate from $\langle 7\rangle 1$ and $\langle 7\rangle 2$.

$\langle 6\rangle 3.$ Q.E.D.

PROOF: $N \equiv E \vee M$ — By definition of N.
$\equiv E \vee (\mathcal{L} \wedge M)$ — By assumption $\langle 5 \rangle$.
$\equiv E \vee L$ — By definition of L.
$\equiv (E \wedge \neg L) \vee L$ — By propositional logic.

Therefore, cases $\langle 6 \rangle 1$ and $\langle 6 \rangle 2$ are exhaustive.

$\langle 5 \rangle 4$. Q.E.D.

PROOF: $\langle 5 \rangle 3$ and $\langle 5 \rangle 2$.

$\langle 4 \rangle 2$. $(I^c)' \wedge [N^c]_{\langle v,b,c \rangle} \wedge [N]_v \wedge I^p \wedge [N^p]_{\langle v,p \rangle} \Rightarrow$
$[(I^l)' \wedge (v' \neq v) \Rightarrow \exists\, u : N^l(u/l) \wedge I^l(u/l)]_v$

PROOF: $\langle 4 \rangle 1$, since $v' = v$ implies $[\ldots]_v$.

$\langle 4 \rangle 3$. $\Box I^c \wedge \Box[N^c]_{\langle v,b,c \rangle} \wedge \Box[N]_v \wedge \Box I^p \wedge \Box[N^p]_{\langle v,p \rangle} \Rightarrow$
$\Box[(I^l)' \wedge (v' \neq v) \Rightarrow \exists\, u : N^l(u/l) \wedge I^l(u/l)]_v$

PROOF: $\langle 4 \rangle 2$ and simple TLA reasoning.

$\langle 4 \rangle 4$. Q.E.D.

PROOF: $\langle 4 \rangle 3$ and $\langle 1 \rangle 2$.

$\langle 3 \rangle 4$. Q.E.D.

PROOF: By $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, and the following rule for adding prophecy variables.

Let w be an m-tuple of variables, let x be an n-tuple of variables distinct from the variables of w, let I be a predicate and N an action, where all the free variables of I and N are included in w and x. Then

$\wedge\ \Box\Diamond(\exists\,!a : I(a/x))$
$\wedge\ \Box[I' \wedge (w' \neq w) \Rightarrow (\exists\, a : N(a/x) \wedge I(a/x))]_w$
$\Rightarrow \boldsymbol{\exists}\, x : \Box I \wedge \Box[N \wedge (w' \neq w)]_{\langle w,x \rangle}$

where $\exists\,!a$ means there exists a unique a:

$$\exists\,!a : F(a) \ \triangleq\ \exists\, a : F(a) \wedge (\forall\, b : F(b) \Rightarrow (b = a))$$

$\langle 2 \rangle 3$. Q.E.D.

$\langle 3 \rangle 1$. $\Box I^c \wedge H^c \wedge Q \wedge S \wedge P^p \Rightarrow \boldsymbol{\exists}\, l : (P^p \wedge P^l)$

PROOF: By $\langle 2 \rangle 2$ and temporal predicate logic, since l does not occur free in P^p.

$\langle 3 \rangle 2$. $(\boldsymbol{\exists}\, p : \Box I^c \wedge H^c \wedge Q \wedge S \wedge P^p) \Rightarrow \boldsymbol{\exists}\, p, l : (P^p \wedge P^l)$

PROOF: By $\langle 3 \rangle 1$ and temporal predicate logic.

$\langle 3 \rangle 3$. $(\boldsymbol{\exists}\, p : \Box I^c \wedge H^c \wedge Q \wedge S \wedge P^p) \equiv \Box I^c \wedge H^c \wedge Q \wedge S$

PROOF: By $\langle 2 \rangle 2$ and temporal predicate logic, since p does not occur free in $\Box I^c \wedge H^c \wedge Q \wedge S$.

$\langle 3 \rangle 4$. Q.E.D.

PROOF: By $\langle 3 \rangle 2$ and $\langle 3 \rangle 3$.

$\langle 1 \rangle 6$. ASSUME: $N^{all} \wedge I^{all} \wedge (I^{all})' \wedge X$

PROVE: $\overline{M^R}$

⟨2⟩1. $(\neg\mathcal{R} \wedge (r = v)) \vee (\neg\mathcal{R} \wedge R^+)(r/v, v/v')$

PROOF: Assumption ⟨1⟩ implies I^r, and the conclusion follows from I^r and the definition of $\rho(r)$.

⟨2⟩2. $(\neg\mathcal{L}' \wedge (l' = v')) \vee (L^+ \wedge \neg\mathcal{L}')(v'/v, l'/v')$

PROOF: Assumption ⟨1⟩ implies $(I^l)'$, and the conclusion follows from $(I^l)'$ and the definition of $\lambda(l)$.

⟨2⟩3. $M^R(r/v, l'/v')$

⟨3⟩1. $(\neg(\mathcal{R} \vee \mathcal{L}) \wedge M^+)(r/v)$

⟨4⟩1. CASE: $\neg\mathcal{R} \wedge (r = v)$

PROOF: Assumption ⟨1⟩ implies $\neg\mathcal{L} \wedge M$, from which we deduce $\neg(\mathcal{R} \vee \mathcal{L}) \wedge M \wedge (r = v)$, which implies the level-⟨3⟩ goal because M implies M^+.

⟨4⟩2. CASE: $(\neg\mathcal{R} \wedge R^+)(r/v, v/v')$

⟨5⟩1. $\neg\mathcal{L}(r/v)$

PROOF: Since R equals $M \wedge \mathcal{R}'$, this follows from assumption ⟨4⟩ and hypothesis 1(c).

⟨5⟩2. $(\neg\mathcal{R} \wedge M^+)(r/v)$

PROOF: Assumption ⟨1⟩ implies M. Since R^+ implies M^+, assumption ⟨4⟩ implies $(\neg\mathcal{R} \wedge M^+)(r/v, v/v')$. From (1), we then deduce $(\neg\mathcal{R} \wedge (M^+ \cdot M))(r/v)$, which implies the desired result since $M^+ \cdot M$ implies M^+.

⟨5⟩3. Q.E.D.

PROOF: The result follows immediately from ⟨5⟩1 and ⟨5⟩2.

⟨4⟩3. Q.E.D.

PROOF: ⟨2⟩1 implies that cases ⟨4⟩1 and ⟨4⟩2 are exhaustive.

⟨3⟩2. Q.E.D.

⟨4⟩1. CASE: $\neg\mathcal{L}' \wedge (l' = v')$

PROOF: By ⟨3⟩1 and assumption ⟨1⟩, which implies $\neg\mathcal{R}'$, we have $(\neg(\mathcal{R} \vee \mathcal{L}) \wedge M^+)(r/v) \wedge \neg(\mathcal{R} \vee \mathcal{L})' \wedge (l' = v')$, which implies $(\neg(\mathcal{R} \vee \mathcal{L}) \wedge M^+ \wedge \neg(\mathcal{R} \vee \mathcal{L})')(r/v, l'/v')$, and the level-⟨2⟩ goal follows from the definition of M^R.

⟨4⟩2. CASE: $(L^+ \wedge \neg\mathcal{L}')(v'/v, l'/v')$

⟨5⟩1. $\neg\mathcal{R}'(l'/v')$

PROOF: Since L equals $\mathcal{L} \wedge M$, this follows from assumption ⟨4⟩ and hypothesis 1(c).

⟨5⟩2. $(\neg(\mathcal{R} \vee \mathcal{L}) \wedge M^+ \wedge \neg\mathcal{L}')(r/v, l'/v')$

PROOF: By (1), ⟨3⟩1 and assumption ⟨4⟩ imply

$$((\neg(\mathcal{R} \vee \mathcal{L}) \wedge M^+) \cdot (L^+ \wedge \neg\mathcal{L}'))(r/v, l'/v')$$

which by (1) equals

$$(\neg(\mathcal{R} \vee \mathcal{L}) \wedge (M^+ \cdot L^+) \wedge \neg\mathcal{L}')(r/v, l'/v')$$

The result then follows because $M^+ \cdot L^+$ implies $M^+ \cdot M^+$, which implies M^+.

⟨5⟩3. Q.E.D.

PROOF: The level-⟨2⟩ goal follows immediately from ⟨5⟩1, ⟨5⟩2, and the definition of M^R.

⟨4⟩3. Q.E.D.

PROOF: ⟨2⟩2 implies that cases ⟨4⟩1 and ⟨4⟩2 are exhaustive.

⟨2⟩4. $\overline{v} = r$

⟨3⟩1. CASE: $\mathcal{R}$

PROOF: Immediate from the definition of $\overline{v}$.

⟨3⟩2. CASE: $\neg\mathcal{R}$

PROOF: Assumption ⟨1⟩ implies $\neg\mathcal{L}$ and I^r. From $\neg\mathcal{R}$, $\neg\mathcal{L}$, and the definition of $\overline{v}$ we deduce $\overline{v} = v$. From $\neg\mathcal{R} \wedge I^r$ we deduce $r = v$.

⟨3⟩3. Q.E.D.

PROOF: Immediate from ⟨3⟩1 and ⟨3⟩2.

⟨2⟩5. $\overline{v}' = l'$

⟨3⟩1. CASE: $\mathcal{L}'$

PROOF: Assumption ⟨1⟩ implies $\mathcal{L} \wedge M$, which by hypothesis 1(c) implies $\neg\mathcal{R}'$. From $\neg\mathcal{R}'$, $\mathcal{L}'$, and definition of $\overline{v}$, we deduce $\overline{v}' = l'$.

⟨3⟩2. CASE: $\neg\mathcal{L}'$

PROOF: Assumption ⟨1⟩ implies $\neg\mathcal{R}$' and $(I^r)'$. From $\neg\mathcal{R}'$ and $\neg\mathcal{L}'$ we deduce $\overline{v}' = v'$, and from $\neg\mathcal{L}' \wedge (I^r)'$ we deduce $l' = v'$.

⟨2⟩6. Q.E.D.

PROOF: ⟨2⟩3, ⟨2⟩4, and ⟨2⟩5.

⟨1⟩7. $\mathit{Init} \wedge \Box[N^{all}]_{all} \wedge \Box I^{all} \Rightarrow \overline{\mathit{Init}} \wedge \Box[\overline{N^R}]_{\overline{v}}$

⟨2⟩1. $\mathit{Init} \wedge I^{all} \Rightarrow \overline{\mathit{Init}}$

PROOF: Assumption ⟨1⟩ implies $I^r \wedge I^l$. By hypothesis 1(a), *Init* implies $\neg(\mathcal{R} \vee \mathcal{L})$, which by $I^r \wedge I^l$ implies $(l = v) \wedge (r = v)$, which by definition of $\overline{v}$ implies $\overline{v} = v$, so $\overline{\mathit{Init}} = \mathit{Init}$.

⟨2⟩2. ASSUME: $N^{all} \wedge I^{all} \wedge (I^{all})'$

PROVE: $[\overline{N^R}]_{\overline{v}}$

⟨3⟩1. $\neg p$

PROOF: Assumption ⟨2⟩ implies N^{all}, which implies $(v' \neq v) \wedge N^p$, which implies $\neg p$.

⟨3⟩2. CASE: $E \wedge \neg R \wedge \neg L$

⟨4⟩1. CASE: $\neg\mathcal{R} \wedge \neg\mathcal{L}$

⟨5⟩1. $\neg\mathcal{R}' \wedge \neg\mathcal{L}'$

PROOF: Assumptions ⟨3⟩ and ⟨4⟩ and hypothesis 1(b) (which implies $E \wedge \mathcal{L}' \Rightarrow \mathcal{L}$ and $E \wedge \mathcal{R}' \Rightarrow \mathcal{R}$).

⟨5⟩2. $(\overline{v} = v) \wedge (\overline{v}' = v')$

PROOF: ⟨5⟩1, assumption ⟨4⟩, and the definition of $\overline{v}$.

⟨5⟩3. Q.E.D.

PROOF: ⟨5⟩2 and case assumption ⟨3⟩ imply $\overline{E}$, which in turn implies $\overline{N^R}$.

⟨4⟩2. CASE: $\mathcal{R}$

⟨5⟩1. $\exists\, u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$

PROOF: Assumption ⟨2⟩ implies $I^r \wedge (I^c)' \wedge N^c$. Assumption ⟨4⟩ and I^r implies $\rho(r)$. The result follows from assumption ⟨3⟩, $(I^c)' \wedge N^c$, $\rho(r)$, and ⟨1⟩1.1.

⟨5⟩2. $\mathcal{R}'$

PROOF: Assumptions ⟨3⟩ and ⟨4⟩ and hypothesis 1(b).

⟨5⟩3. $r' = \text{CHOOSE } u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$

PROOF: Assumption ⟨2⟩ (which implies N^r and $v' \neq v$), ⟨5⟩2, assumption ⟨3⟩, and the definition of N^r.

⟨5⟩4. $D(r/v, r'/v')$

PROOF: ⟨5⟩1 and ⟨5⟩3.

⟨5⟩5. $(\overline{v} = r) \wedge (\overline{v}' = r')$

PROOF: ⟨5⟩2, assumption ⟨4⟩, and the definition of $\overline{v}$.

⟨5⟩6. Q.E.D.

PROOF: ⟨5⟩4 and ⟨5⟩5 imply $\overline{D}$, which implies $\overline{E}$ (since D implies E), which in turn implies $\overline{N^R}$.

⟨4⟩3. CASE: $\mathcal{L}$

⟨5⟩1. $\mathcal{L}'$

PROOF: Assumptions ⟨3⟩ and ⟨4⟩ and hypothesis 1(b).

⟨5⟩2. $\lambda(l)'$

PROOF: ⟨5⟩1, assumption ⟨2⟩ (which implies $(I^l)'$), and the definition of I^l.

⟨5⟩3. $\exists\, u : \lambda(u) \wedge D(u/v, l'/v')$

PROOF: Assumption ⟨2⟩ (which implies $(I^c)' \wedge N^c$), ⟨5⟩2, assumption ⟨3⟩, and ⟨1⟩1.2.

⟨5⟩4. $l = \text{CHOOSE } u : \lambda(u) \wedge D(u/v, l'/v')$

PROOF: ⟨3⟩1, assumption ⟨4⟩, assumption ⟨3⟩, assumption ⟨2⟩ (which implies $v \neq v'$ and N^l), and the definition of N^l.

⟨5⟩5. $D(l/v, l'/v')$

PROOF: ⟨5⟩3 and ⟨5⟩4.

⟨5⟩6. $\neg\mathcal{R} \wedge \neg\mathcal{R}'$

PROOF: Assumption ⟨4⟩, ⟨5⟩1, and hypothesis 1(d).

⟨5⟩7. $(\overline{v} = l) \wedge (\overline{v}' = l')$

PROOF: Assumption ⟨4⟩, ⟨5⟩1, ⟨5⟩6, and the definition of $\overline{v}$.

⟨5⟩8. Q.E.D.

PROOF: ⟨5⟩5 and ⟨5⟩7 imply $\overline{D}$, which implies $\overline{E}$ (since D implies E), which in turn implies $\overline{N^R}$.

⟨4⟩4. Q.E.D.

PROOF: Immediate from ⟨4⟩1, ⟨4⟩2, and ⟨4⟩3.

⟨3⟩3. CASE: R

⟨4⟩1. $r' = r$

PROOF: Assumption ⟨2⟩ implies N^r, which by assumption ⟨3⟩ (which implies $\mathcal{R}'$) implies $r' = r$.

⟨4⟩2. $\overline{v}' = r'$

PROOF: Assumption ⟨3⟩ (which implies $\mathcal{R}'$) and the definition of $\overline{v}$.

⟨4⟩3. $\neg\mathcal{L}$

PROOF: Assumption ⟨3⟩ (which implies $\mathcal{R}'$) and hypothesis 1(c).

⟨4⟩4. $\overline{v} = r$

⟨5⟩1. CASE: $\mathcal{R}$

PROOF: The definition of $\overline{v}$ implies $\overline{v} = r$.

⟨5⟩2. CASE: $\neg\mathcal{R}$

PROOF: By ⟨4⟩3, the definition of $\overline{v}$ implies $\overline{v} = v$. Assumption ⟨2⟩ implies I^r, which implies $v = r$.

⟨5⟩3. Q.E.D.

PROOF: Immediate from ⟨5⟩1 and ⟨5⟩2.

⟨4⟩5. Q.E.D.

PROOF: ⟨4⟩1, ⟨4⟩2, and ⟨4⟩4 imply $\overline{v}' = \overline{v}$, which implies the level-⟨2⟩ goal.

⟨3⟩4. CASE: L

⟨4⟩1. $\neg\mathcal{R}$

PROOF: Assumption ⟨3⟩ (which implies $\mathcal{L}$) and hypothesis 1(d).

⟨4⟩2. $l' = l$

PROOF: Assumption ⟨2⟩ implies N^l, which by ⟨3⟩1 and assumption ⟨3⟩ (which implies $\mathcal{L}$) implies $l = l'$.

⟨4⟩3. $\overline{v} = l$

PROOF: ⟨4⟩1, assumption ⟨3⟩ (which implies $\mathcal{L}$), and the definition of $\overline{v}$.

⟨4⟩4. $\overline{v}' = l'$

⟨5⟩1. $\neg\mathcal{R}'$

PROOF: Assumption ⟨3⟩ (which implies $\mathcal{L}$) and hypothesis 1(c).

⟨5⟩2. CASE: $\mathcal{L}'$

PROOF: ⟨5⟩1 and the definition of $\overline{v}$ imply $\overline{v}' = l'$.

⟨5⟩3. CASE: $\neg\mathcal{L}'$

PROOF: ⟨5⟩1 and the definition of $\overline{v}$ imply $\overline{v}' = v'$. Assumption ⟨2⟩ implies $(I^l)'$, which implies $l' = v'$, proving $\overline{v}' = l'$.

⟨5⟩4. Q.E.D.

PROOF: Immediate from ⟨5⟩2 and ⟨5⟩3.

⟨4⟩5. Q.E.D.

PROOF: ⟨4⟩2, ⟨4⟩3, and ⟨4⟩4 imply $\overline{v}' = \overline{v}$, which implies the level-⟨2⟩ goal.

⟨3⟩5. CASE: X

PROOF: Assumption ⟨2⟩ and ⟨1⟩6 imply $\overline{M^R}$, which implies the level-⟨2⟩ goal.

⟨3⟩6. Q.E.D.

PROOF: Assumption ⟨2⟩ implies N, which equals $E \vee M$, so ⟨1⟩1.4 implies that cases ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, and ⟨3⟩5 are exhuastive.

⟨2⟩3. $[N^{all} \wedge I^{all} \wedge (I^{all})']_{all} \Rightarrow [\overline{N^R}]_{\overline{v}}$

PROOF: ⟨2⟩2, since the definition of $\overline{v}$ implies $(\overline{all}' = \overline{all}) \Rightarrow (\overline{v}' = \overline{v})$.

⟨2⟩4. Q.E.D.

PROOF: ⟨2⟩1, ⟨2⟩3, and the usual TLA step-simulation rule.

⟨1⟩8. $\Box I^{all} \Rightarrow \Box I(\overline{v}/\widehat{v})$

⟨2⟩1. $I^r \wedge I^l \Rightarrow I(\overline{v}/\widehat{v})$

⟨3⟩1. $I^r \wedge \mathcal{R} \Rightarrow R^+(\overline{v}/v, v/v') \wedge \neg(\mathcal{R} \vee \mathcal{L})(\overline{v}/v)$

PROOF:
$$
\begin{aligned}
I^r \wedge \mathcal{R} \;&\Rightarrow\; \rho(r) \wedge \mathcal{R} && \text{By definition of } I^r.\\
&=\; R^+(r/v, v/v') \wedge \mathcal{R} \wedge \neg\mathcal{R}(r/v) && \text{By definition of } \rho.\\
&\Rightarrow\; R^+(r/v, v/v') \wedge \neg\mathcal{L}(r/v) \wedge \neg\mathcal{R}(r/v) && \text{Since } R = M \wedge \mathcal{R}'\text{, hypothesis 1(c) implies } \neg(\mathcal{L} \wedge R^+).\\
&=\; R^+(r/v, v/v') \wedge \neg(\mathcal{R} \vee \mathcal{L})(r/v) && \text{By propositional logic.}
\end{aligned}
$$

and $\mathcal{R}$ implies $\overline{v} = r$ by definition of $\overline{v}$.

⟨3⟩2. $I^l \wedge \mathcal{L} \Rightarrow L^+(\overline{v}/v') \wedge \neg(\mathcal{R} \vee \mathcal{L})(\overline{v}/v)$

PROOF:
$$
\begin{aligned}
I^l \wedge \mathcal{L} \;&\Rightarrow\; \lambda(l) && \text{By definition of } I^l.\\
&=\; L^+(l/v') \wedge \neg\mathcal{L}'(l/v') && \text{By definition of } \lambda.\\
&\Rightarrow\; L^+(l/v') \wedge \neg\mathcal{R}'(l/v') \wedge \neg\mathcal{L}'(l/v') && \text{Since } L = \mathcal{L} \wedge M\text{, hypothesis 1(c) implies } \neg(L^+ \wedge \mathcal{R}').\\
&\Rightarrow\; L^+(l/v') \wedge \neg(\mathcal{R}' \vee \mathcal{L}')(l/v') && \text{By propositional logic.}\\
&=\; L^+(l/v') \wedge \neg(\mathcal{R} \vee \mathcal{L})(l/v)
\end{aligned}
$$

and, by hypothesis 1(d), $\mathcal{L}$ implies $\neg\mathcal{R}$, so $\mathcal{L}$ implies $\overline{v} = l$ by definition of $\overline{v}$.

$\langle 3 \rangle 3.$ $\neg(\mathcal{R} \vee \mathcal{L}) \Rightarrow (\overline{v} = v)$

PROOF: By definition of $\overline{v}$.

$\langle 3 \rangle 4.$ Q.E.D.

PROOF: Immediate from $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, and the definition of I.

$\langle 2 \rangle 2.$ Q.E.D.

PROOF: By simple temporal reasoning from $\langle 2 \rangle 1$.

$\langle 1 \rangle 9.$ $\forall\, i \in \mathcal{I} : Q \wedge O \wedge \Box[N^{all}]_{all} \wedge \Box I^{all} \wedge \Box\Diamond\langle A_i \rangle_v \Rightarrow \Box\Diamond\langle \overline{A_i^R} \rangle_{\overline{v}}$

LET: $T \triangleq Q \wedge O \wedge \Box[N^{all}]_{all} \wedge \Box I^{all}$

$\langle 2 \rangle 1.$ $\forall\, i \in \mathcal{I} : T \wedge \Box\Diamond\langle B_i \rangle_v \Rightarrow \Box\Diamond\langle \overline{B_i} \rangle_{\overline{v}}$

$\langle 3 \rangle 1.$ ASSUME: $(b' \in \mathcal{I}) \wedge \langle N^{all} \wedge I^{all} \wedge (I^{all})' \wedge B_{b'} \rangle_v$

PROVE: $\langle \overline{B_{b'}} \rangle_{\overline{v}}$

$\langle 4 \rangle 1.$ $\neg M$

PROOF: Assumption $\langle 3 \rangle$ and hypothesis 1(e).

$\langle 4 \rangle 2.$ $\neg p$

PROOF: Assumption $\langle 3 \rangle$, since N^{all} implies $(v' \neq v) \wedge N^p$ which implies $\neg p$.

$\langle 4 \rangle 3.$ D

$\langle 5 \rangle 1.$ E

PROOF: $\langle 4 \rangle 1$, assumption $\langle 3 \rangle$ (which implies N), and the definition of N.

$\langle 5 \rangle 2.$ Q.E.D.

PROOF: $\langle 5 \rangle 1$, assumption $\langle 3 \rangle$ (which implies $B_{b'}$), and the definition of D.

$\langle 4 \rangle 4.$ CASE: $\mathcal{R}$

$\langle 5 \rangle 1.$ $\mathcal{R}'$

PROOF: $\langle 4 \rangle 3$, assumption $\langle 4 \rangle$ and hypothesis 1(b) (since $D \Rightarrow E$).

$\langle 5 \rangle 2.$ $r' = \text{CHOOSE } u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$

PROOF: $\langle 4 \rangle 1$ (which implies $\neg R$), $\langle 5 \rangle 1$, $\langle 4 \rangle 3$ (which with assumption $\langle 3 \rangle$ implies $\langle E \rangle_v$), assumption $\langle 3 \rangle$ (which implies N^r), and the definition of N^r.

$\langle 5 \rangle 3.$ $\exists\, u : (\neg\mathcal{R} \wedge R^+)(u/v) \wedge D(r/v, u/v')$

PROOF: Assumption $\langle 3 \rangle$ (which implies $(I^c)' \wedge N^c \wedge I^r$), $\langle 4 \rangle 3$ (which implies E), assumption $\langle 4 \rangle$ (which with I^r implies $\rho(r)$), and $\langle 1 \rangle 1.1$.

$\langle 5 \rangle 4.$ $D(r/v, r'/v')$

PROOF: $\langle 5 \rangle 2$ and $\langle 5 \rangle 3$.

⟨5⟩5. $\langle B_{b'}(r/v, r'/v')\rangle_r$

By assumption ⟨3⟩ ($b' \in \mathcal{I}$) and the definition of D, ⟨5⟩4 implies $(\langle B_{b'}\rangle_v)(r/v, r'/v')$.

⟨5⟩6. $(\overline{v} = r) \wedge (\overline{v}' = r')$

PROOF: Assumption ⟨4⟩, ⟨5⟩1, and the definition of $\overline{v}$.

⟨5⟩7. Q.E.D.

PROOF: The level-⟨3⟩ goal follows immediately from ⟨5⟩5 and ⟨5⟩6.

⟨4⟩5. CASE: $\mathcal{L}$

⟨5⟩1. $\mathcal{L}'$

PROOF: Assumption ⟨4⟩, ⟨4⟩3 (which implies E), and hypothesis 1(b).

⟨5⟩2. $l = \text{CHOOSE } u : \lambda(u) \wedge D(u/v, l'/v')$

PROOF: Assumption ⟨3⟩ implies N^l. The result then follows from ⟨4⟩2, ⟨4⟩5, ⟨4⟩1 (which implies $\neg L$), ⟨4⟩3 (which by assumption ⟨3⟩ implies $\langle E\rangle_v$), and the definition of N^l.

⟨5⟩3. $\exists\, u : \lambda(u) \wedge D(u/v, l'/v')$

PROOF: Assumption ⟨3⟩ implies $(I^c)' \wedge (I^l)'$. By ⟨5⟩1, $(I^l)'$ implies $\lambda(l)'$. The result then follows from ⟨4⟩3 and ⟨1⟩1.2.

⟨5⟩4. $D(l/v, l'/v')$

PROOF: ⟨5⟩2 and ⟨5⟩3.

⟨5⟩5. $\langle B_{b'}(l/v, l'/v')\rangle_l$

PROOF: ⟨5⟩4, assumption ⟨3⟩ (which asserts $b' \in \mathcal{I}$), and the definition of D imply $(\langle B_{b'}\rangle_v)(l/v, l'/v')$.

⟨5⟩6. $(\overline{v} = l) \wedge (\overline{v}' = l')$

PROOF: Case assumption ⟨4⟩, ⟨5⟩1, hypothesis 1(d), and the definition of $\overline{v}$.

⟨5⟩7. Q.E.D.

PROOF: The level-⟨3⟩ goal follows immediately from ⟨5⟩5 and ⟨5⟩6.

⟨4⟩6. CASE: $\neg(\mathcal{R} \vee \mathcal{L})$

⟨5⟩1. $\neg(\mathcal{R}' \vee \mathcal{L}')$

PROOF: Assumption ⟨4⟩, ⟨4⟩3 (which implies E), and hypothesis 1(b).

⟨5⟩2. $(\overline{v} = v) \wedge (\overline{v}' = v')$

PROOF: Case assumption ⟨4⟩, ⟨5⟩1, and the definition of $\overline{v}$.

⟨5⟩3. Q.E.D.

PROOF: Assumption ⟨3⟩, which implies $\langle B_{b'}\rangle_v$, and ⟨5⟩2 imply the level-⟨3⟩ goal.

⟨4⟩7. Q.E.D.

PROOF: Immediate from $\langle 4\rangle 4$, $\langle 4\rangle 5$, and $\langle 4\rangle 6$.

$\langle 3\rangle 2$. ASSUME: $i \in \mathcal{I}$

PROVE: $T \wedge \Box\Diamond\langle (i = b') \wedge B_{b'} \rangle_v \Rightarrow \Box\Diamond\langle \overline{B_i} \rangle_{\overline{v}}$

$\langle 4\rangle 1$. $\Box[N^{all}]_{all} \wedge \Box I^{all} \wedge \Box\Diamond\langle (i = b') \wedge B_{b'} \rangle_v$
$\quad \Rightarrow \Box\Diamond\langle N^{all} \wedge I^{all} \wedge (I^{all})' \wedge (i = b') \wedge B_{b'} \rangle_v$

PROOF: Since $(all' = all)$ implies $(v' = v)$, this follows easily from the following three TLA proof rules:

1. $\dfrac{[A]_f \Rightarrow [B]_g}{\Box[A]_f \Rightarrow \Box[B]_g}$
2. $\Box[A]_f \wedge \Box\mathcal{R} \Rightarrow \Box[A \wedge \mathcal{R} \wedge \mathcal{R}']_f$
3. $\Box[A]_f \wedge \Box\Diamond\langle B \rangle_f \Rightarrow \Box\Diamond\langle A \wedge B \rangle_f$

$\langle 4\rangle 2$. Q.E.D.

PROOF: By $\langle 4\rangle 1$, assumption $\langle 3\rangle$, and $\langle 3\rangle 1$, using the TLA rule

$$\frac{A \Rightarrow B}{\Box\Diamond\langle A \rangle_f \Rightarrow \Box\Diamond\langle B \rangle_f}$$

$\langle 3\rangle 3$. ASSUME: $i \in \mathcal{I}$

PROVE: $T \wedge \Box\Diamond\langle B_i \rangle_v \Rightarrow \Box\Diamond\langle (i = b') \wedge B_{b'} \rangle_v$

$\langle 4\rangle 1$. $T \wedge \Box\Diamond\langle B_i \rangle_v \Rightarrow \Box\Diamond\langle E \wedge B_i \rangle_v$

PROOF:

$$\begin{array}{lll} & T \wedge \Box\Diamond\langle B_i \rangle_v & \\ \Rightarrow & \Box[N]_v \wedge \Box\Diamond\langle B_i \rangle_v & \text{Definition of } T \\ \Rightarrow & \Box\Diamond\langle N \wedge B_i \rangle_v & \text{TLA reasoning.} \\ \Rightarrow & \Box\Diamond\langle E \wedge B_i \rangle_v & \end{array}$$

the last step following from hypothesis 1(e) and assumption $\langle 3\rangle$, which imply $N \wedge B_i \equiv E \wedge B_i$.

$\langle 4\rangle 2$. $T \wedge \Box\Diamond\langle E \wedge B_i \rangle_v \Rightarrow \vee\ \Box\Diamond\langle (i = b') \wedge E \wedge B_{b'} \rangle_v$
$\qquad \vee\ \wedge\ \Box\Diamond\langle E \wedge B_i \wedge (i \neq b') \rangle_{\langle v,b,c \rangle}$
$\qquad\quad \wedge\ \Diamond\Box[E \wedge B_i \Rightarrow (i \neq b')]_{\langle v,b,c \rangle}$

$\langle 5\rangle 1$. $\Box\Diamond\langle E \wedge B_i \rangle_v \Rightarrow \vee\ \Box\Diamond\langle (i = b') \wedge E \wedge B_{b'} \rangle_v$
$\qquad \vee\ \wedge\ \Box\Diamond\langle E \wedge B_i \wedge (i \neq b') \rangle_v$
$\qquad\quad \wedge\ \Diamond\Box[E \wedge B_i \Rightarrow (i \neq b')]_v$

PROOF: For any action A and predicate q, we have

$$\begin{array}{lll} & \Box\Diamond\langle A \rangle_v & \\ \equiv & \wedge\ \Box\Diamond\langle A \rangle_v & \Box\Diamond F \vee \Diamond\Box\neg F, \text{ for any } F \\ & \wedge\ \Box\Diamond\langle A \wedge q \rangle_v \vee \Diamond\Box[\neg A \vee \neg q]_v & \\ \Rightarrow & \vee\ \Box\Diamond\langle A \wedge q \rangle_v & \text{Propositional logic.} \\ & \vee\ \Diamond\Box[\neg A \vee \neg q]_v \wedge \Box\Diamond\langle A \rangle_v & \\ \Rightarrow & \vee\ \Box\Diamond\langle A \wedge q \rangle_v & \Diamond\Box[B]_v \wedge \Box\Diamond\langle C \rangle_v \Rightarrow \\ & \vee\ \Diamond\Box[\neg A \vee \neg q]_v \wedge \Box\Diamond\langle A \wedge \neg q \rangle_v & \quad \Box\Diamond\langle B \wedge C \rangle_v \text{ for any } B,\ C. \end{array}$$

⟨5⟩2. $T \Rightarrow$

$$\begin{array}{l}\wedge\ \Box\Diamond\langle (i = b') \wedge E \wedge B_{b'} \rangle_v \equiv \Box\Diamond\langle (i = b') \wedge E \wedge B_{b'} \rangle_{\langle v,b,c \rangle} \\ \wedge\ \Diamond\Box[E \wedge B_i \Rightarrow (i \neq b')]_v \equiv \Diamond\Box[E \wedge B_i \Rightarrow (i \neq b')]_{\langle v,b,c \rangle}\end{array}$$

⟨6⟩1. $N^c \wedge (v' = v) \Rightarrow (\langle v, b, c \rangle' = \langle v, b, c \rangle)$

PROOF: By definition of N^c.

⟨6⟩2. For any action A,

$$\Box[N^c]_{\langle v,b,c \rangle} \Rightarrow \begin{array}{l}\wedge\ \Diamond\Box[A]_v \equiv \Diamond\Box[A]_{\langle v,b,c \rangle} \\ \wedge\ \Box\Diamond[A]_v \equiv \Box\Diamond[A]_{\langle v,b,c \rangle}\end{array}$$

PROOF: By ⟨6⟩1, using the follow rules, among others

$$\frac{[A]_f \wedge [B]_g \Rightarrow [C]_h}{\Box[A]_f \wedge \Box[B]_g \Rightarrow \Box[C]_h} \quad \frac{[A]_f \wedge \langle B \rangle_g \Rightarrow \langle C \rangle_h}{\Box[A]_f \wedge \Diamond[B]_g \Rightarrow \Diamond\langle C \rangle_h)}$$

⟨6⟩3. Q.E.D.

PROOF: By ⟨6⟩2, since T implies $\Box[N^c]_{\langle v,b,c \rangle}$

⟨5⟩3. Q.E.D.

PROOF: Immediate from ⟨5⟩1 and ⟨5⟩2

⟨4⟩3. $T \Rightarrow \neg(\wedge\ \Box\Diamond\langle E \wedge B_i \wedge (i \neq b') \rangle_{\langle v,b,c \rangle}$
$\qquad \wedge\ \Diamond\Box[(E \wedge B_i) \Rightarrow (i \neq b')]_{\langle v,b,c \rangle})$

⟨5⟩1. $I^c \wedge N^c \wedge E \wedge B_i \wedge (i \neq b') \Rightarrow Pos(i)' < Pos(i)$

PROOF: $I^c \wedge N^c \wedge E \wedge B_i$ imply $b' \in \mathcal{I}$. From $b' \in \mathcal{I}$, $i \in \mathcal{I}$ (assumption ⟨3⟩), $E \wedge B_i$, and N^c, we deduce $Pos(b') < Pos(i)$, which by N^c implies $c'[Pos(i) - 1] = i$. By definition of Pos, this implies $Pos(i)' < Pos(i)$.

⟨5⟩2. $\Box I^c \wedge \Box[N^c]_{\langle v,b,c \rangle} \wedge \Box[(E \wedge B_i) \Rightarrow (i \neq b')]_{\langle v,b,c \rangle}$
$\qquad \Rightarrow \Box[Pos(i)' \leq Pos(i)]_{\langle v,b,c \rangle}$

⟨6⟩1. $I^c \wedge N^c \wedge \neg(E \wedge B_i) \Rightarrow Pos(i)' \leq Pos(i)$

⟨7⟩1. CASE: $E \wedge \exists j \in \mathcal{I} : B_j$

PROOF: In this case, I^c and N^c imply $c'[Pos(i)] = i$ or $c'[Pos(i) - 1] = i$, either case implying $Pos(i)' \leq Pos(i)$.

⟨7⟩2. CASE: $\neg(E \wedge \exists j \in \mathcal{I} : B_j)$

PROOF: In this case, $c' = c$, so $Pos(i)' = Pos(i)$.

⟨7⟩3. Q.E.D.

PROOF: Immediate from ⟨7⟩1 and ⟨7⟩2.

⟨6⟩2. $I^c \wedge [N^c]_{\langle v,b,c \rangle} \wedge [(E \wedge B_i) \Rightarrow (i \neq b')]_{\langle v,b,c \rangle}$
$\qquad \Rightarrow [Pos(i)' \leq Pos(i)]_{\langle v,b,c \rangle}$

PROOF: ⟨5⟩1, ⟨6⟩1, and propositional logic.

⟨6⟩3. Q.E.D.

PROOF: By ⟨6⟩2 and the TLA rules

$$\frac{I \wedge I' \wedge [A]_f \Rightarrow [B]_g}{\Box I \wedge \Box[A]_f \Rightarrow \Box[B]_g} \quad \frac{[A]_f \wedge [B]_g \equiv [C]_h}{\Box[A]_f \wedge \Box[B]_g \equiv \Box[C]_h}$$

$\langle 5 \rangle 3.$ $\Box I^c \wedge \Box[N^c]_{\langle v,b,c \rangle} \wedge \Box\Diamond\langle E \wedge B_i \wedge (i \neq b') \rangle_{\langle v,b,c \rangle}$
$\Rightarrow \Box\Diamond\langle Pos(i)' < Pos(i) \rangle_{\langle v,b,c \rangle}$

PROOF: By $\langle 5 \rangle 1$, the TLA rules

$$\frac{I \wedge [A]_f \wedge \langle B \rangle_g \Rightarrow \langle C \rangle_h}{\Box I \wedge \Box[A]_f \wedge \Diamond\langle B \rangle_g \Rightarrow \Diamond\langle C \rangle_h} \qquad \frac{F \Rightarrow G}{\Box F \Rightarrow \Box G}$$

and the rule that $\Box$ distributes over $\wedge$.

$\langle 5 \rangle 4.$ Q.E.D.

$\langle 6 \rangle 1.$ $\wedge\ T$
$\wedge\ \Box\Diamond\langle E \wedge B_i \wedge (i \neq b') \rangle_{\langle v,b,c \rangle}$
$\wedge\ \Diamond\Box[(E \wedge B_i) \Rightarrow (i \neq b')]_{\langle v,b,c \rangle})$
$\Rightarrow \wedge\ \Box[Pos(i)' \leq Pos(i)]_{\langle v,b,c \rangle}$
$\wedge\ \Box\Diamond\langle Pos(i)' < Pos(i) \rangle_{\langle v,b,c \rangle}$

PROOF: $\langle 5 \rangle 2$ and $\langle 5 \rangle 3$

$\langle 6 \rangle 2.$ Q.E.D.

PROOF: the formula

$$\begin{aligned} &\wedge\ \Box(Pos(i) \in Nat) \\ &\wedge\ \Box[Pos(i)' \leq Pos(i)]_{\langle v,b,c \rangle} \\ &\wedge\ \Box\Diamond\langle Pos(i)' < Pos(i) \rangle_{\langle v,b,c \rangle} \end{aligned}$$

asserts that $Pos(i)$ is decremented infinitely many times and remains a natural number, which is impossible. Since T implies I^c, which implies $\Box(Pos(i) \in Nat)$, $\langle 6 \rangle 1$ implies the level-$\langle 4 \rangle$ goal.

$\langle 4 \rangle 4.$ Q.E.D.

PROOF: By propositional logic from $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, and $\langle 4 \rangle 3$.

$\langle 3 \rangle 4.$ Q.E.D.

PROOF: By $\langle 3 \rangle 2$ and $\langle 3 \rangle 3$.

$\langle 2 \rangle 2.$ $(\exists\, i \in \mathcal{I} : \Delta_i) \wedge T \wedge \Box\Diamond\langle M \rangle_v \Rightarrow \Box\Diamond\langle \overline{M^R} \rangle_{\overline{v}}$

$\langle 3 \rangle 1.$ $T \wedge \Box\Diamond\langle X \rangle_v \Rightarrow \Box\Diamond\langle \overline{M^R} \rangle_{\overline{v}}$

PROOF: From the general rule

$$\Box I \wedge \Box[A]_v \wedge \Box\Diamond\langle B \rangle_v \Rightarrow \Box\Diamond\langle I \wedge I' \wedge A \wedge B \rangle_v$$

and $\Box[N^{all}]_{all} \Rightarrow \Box[N^{all}]_v$ (which follows from $[N^{all}]_{all} \Rightarrow [N^{all}]_v$), we deduce that $T \wedge \Box\Diamond\langle X \rangle_v$ implies $\Box\Diamond\langle N^{all} \wedge I^{all} \wedge (I^{all})' \wedge X \rangle_v$. The result then follows from $\langle 1 \rangle 6$.

$\langle 3 \rangle 2.$ $(\exists\, i \in \mathcal{I} : \Delta_i) \wedge T \wedge \Box\Diamond\langle R \rangle_v \Rightarrow \Box\Diamond\langle \overline{M^R} \rangle_{\overline{v}}$

$\langle 4 \rangle 1.$ $(\exists\, i \in \mathcal{I} : \Delta_i) \wedge T \wedge \Box\Diamond\langle R \rangle_v \Rightarrow \Box\Diamond\neg\mathcal{R}$

PROOF: By definition of O (which is implied by T).

$\langle 4 \rangle 2.$ $\Box[N]_v \wedge \Box\Diamond\langle R \rangle_v \wedge \Box\Diamond\neg\mathcal{R} \Rightarrow \Box\Diamond\langle X \rangle_v$

$\langle 5 \rangle 1.$ $\Box\Diamond\langle R \rangle_v \wedge \Box\Diamond\neg\mathcal{R} \Rightarrow \Box\Diamond\langle \mathcal{R} \wedge \neg\mathcal{R}' \rangle_v$

PROOF: Since R implies $\mathcal{R}'$, we infer that $\Box\Diamond\langle R \rangle_v$ implies $\Box\Diamond\mathcal{R}$, and the result follows from the general rule

$$\Box\Diamond P \land \Box\Diamond\neg P \Rightarrow \Box\Diamond\langle P \land \neg P' \rangle_P$$

plus the observation that $\Box\Diamond\langle \mathcal{R} \land \neg\mathcal{R}' \rangle_{\mathcal{R}}$ implies $\Box\Diamond\langle \mathcal{R} \land \neg\mathcal{R}' \rangle_v$ because $\mathcal{R}' \neq \mathcal{R}$ implies $v' \neq v$ (because v contains all the variables that occur free in $\mathcal{R}$).

⟨5⟩2. $\Box[N]_v \land \Box\Diamond\langle \mathcal{R} \land \neg\mathcal{R}' \rangle_v \Rightarrow \Box\Diamond\langle X \rangle_v$

⟨6⟩1. $N \land \mathcal{R} \land \neg\mathcal{R}' \Rightarrow X$

PROOF:
$$\begin{array}{rcll} N \land \mathcal{R} \land \neg\mathcal{R}' & \equiv & (M \lor E) \land \mathcal{R} \land \neg\mathcal{R}' & \text{Definition of } N. \\ & \equiv & M \land \mathcal{R} \land \neg\mathcal{R}' & \text{Hypothesis 1(b).} \\ & \Rightarrow & M \land \neg\mathcal{L} \land \neg\mathcal{R}' & \text{Hypothesis 1(d).} \\ & = & X & \text{Definition of } X \end{array}$$

⟨6⟩2. Q.E.D.

PROOF: From ⟨6⟩1 by the general rule

$$\frac{[N]_v \land \langle A \rangle_v \Rightarrow \langle B \rangle_v}{\Box[N]_v \land \Box\Diamond\langle A \rangle_v \Rightarrow \Box\Diamond\langle B \rangle_v}$$

⟨5⟩3. Q.E.D.

PROOF: By propositional logic from ⟨5⟩1 and ⟨5⟩2.

⟨4⟩3. Q.E.D.

PROOF: By propositional logic from ⟨4⟩1, ⟨4⟩2, and ⟨3⟩1, since T implies $\Box[N^{all}]_{all}$ which implies $\Box[N]_v$.

⟨3⟩3. $T \land \Box\Diamond\langle L \rangle_v \Rightarrow \Box\Diamond\langle \overline{M^R} \rangle_{\overline{v}}$

⟨4⟩1. $T \land \Box\Diamond\langle L \rangle_v \Rightarrow \Box\Diamond(\neg\mathcal{L})$

PROOF: By definition of Q (which is implied by T), since $\Box\Diamond\langle L \rangle_v \Rightarrow \Box\Diamond\langle \text{TRUE} \rangle_v = \Box\neg\Box[\text{FALSE}]_v = \neg\Diamond\Box[\text{FALSE}]_v$.

⟨4⟩2. $(\neg\mathcal{L}) \land \Box[N \land \neg X]_v \Rightarrow \Box(\neg\mathcal{L})$

⟨5⟩1. $\neg\mathcal{L} \land [N \land \neg X]_v \Rightarrow \neg\mathcal{L}'$

⟨6⟩1. $\neg\mathcal{L} \land E \Rightarrow \neg\mathcal{L}'$

PROOF: Hypothesis 1(b).

⟨6⟩2. $\neg\mathcal{L} \land R \Rightarrow \neg\mathcal{L}'$

PROOF: By definition of R (which implies $\mathcal{R}'$) and hypothesis 1(d).

⟨6⟩3. $\neg\mathcal{L} \land L \Rightarrow \neg\mathcal{L}'$

PROOF: By definition of L (which implies $\mathcal{L}$).

⟨6⟩4. $\neg\mathcal{L} \land (v' = v) \Rightarrow \neg\mathcal{L}'$

PROOF: By the hypothesis that the tuple v contains all the free variables of $\mathcal{L}$.

⟨6⟩5. Q.E.D.

PROOF: By ⟨6⟩1, ⟨6⟩2, ⟨6⟩3, ⟨6⟩4, since ⟨1⟩1.4 and the definition of N imply that $N \land \neg X$ equals $E \lor R \lor L$.

$\langle 5\rangle 2.$ Q.E.D.

PROOF: By $\langle 5\rangle 1$ and the standard TLA invariance rule.

$\langle 4\rangle 3.$ $\Box\Diamond\langle L\rangle_v \wedge \Box\Diamond\neg\mathcal{L} \Rightarrow \Box\Diamond\langle \neg N \vee X\rangle_v$

$\langle 5\rangle 1.$ $\Diamond\mathcal{L} \Rightarrow \Diamond\langle \neg N \vee X\rangle_v \vee \mathcal{L}$

PROOF: By $\langle 4\rangle 2$, since $\neg\Box[N\wedge\neg X]_v$ is equivalent to $\Diamond\langle\neg N\vee X\rangle_v$.

$\langle 5\rangle 2.$ $\Box\Diamond\mathcal{L} \Rightarrow \Box\Diamond\langle \neg N \vee X\rangle_v \vee \Diamond\Box\mathcal{L}$

PROOF: By $\langle 5\rangle 1$ and the proof rules

$$\frac{F \Rightarrow G}{\Box F \Rightarrow \Box G} \qquad \Box(\Diamond F \vee G) \Rightarrow \Box\Diamond F \vee \Diamond\Box G$$

$\langle 5\rangle 3.$ Q.E.D.

PROOF:

$\Box\Diamond\langle L\rangle_v \wedge \Box\Diamond\neg\mathcal{L}$

$\Rightarrow$ $\Box\Diamond\mathcal{L} \wedge \Box\Diamond\neg\mathcal{L}$ — Since $L \Rightarrow \mathcal{L}$.

$\Rightarrow$ $(\Box\Diamond\langle\neg N \vee X\rangle_v \vee \Diamond\Box\mathcal{L}) \wedge \Box\Diamond\neg\mathcal{L}$ — By $\langle 5\rangle 2$.

$\Rightarrow$ $\Box\Diamond\langle\neg N \vee X\rangle_v$ — Since $\Box\Diamond\neg\mathcal{L} \equiv \neg\Diamond\Box\mathcal{L}$.

$\langle 4\rangle 4.$ $T \wedge \Box\Diamond\langle L\rangle_v \Rightarrow \Box\Diamond\langle X\rangle_v$

$\langle 5\rangle 1.$ $T \wedge \Box\Diamond\langle L\rangle_v \Rightarrow \Box\Diamond\langle\neg N \vee X\rangle_v$

PROOF: $\langle 4\rangle 1$ and $\langle 4\rangle 3$.

$\langle 5\rangle 2.$ $\Box[N]_v \wedge \Box\Diamond\langle\neg N \vee X\rangle_v \Rightarrow \Box\Diamond\langle X\rangle_v$

PROOF: By the TLA rule $\Box[A]_v \wedge \Diamond\langle B\rangle_v \Rightarrow \Diamond\langle A \wedge B\rangle_v$.

$\langle 5\rangle 3.$ Q.E.D.

PROOF: $\langle 5\rangle 1$ and $\langle 5\rangle 2$, since T implies $\Box[N]_v$.

$\langle 4\rangle 5.$ Q.E.D.

PROOF: $\langle 4\rangle 4$ and $\langle 3\rangle 1$.

$\langle 3\rangle 4.$ Q.E.D.

PROOF: $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, and $\langle 1\rangle 1.4$, since $\Box\Diamond$ distributes over disjunction.

$\langle 2\rangle 3.$ Q.E.D.

PROOF: $\langle 2\rangle 1$ and $\langle 2\rangle 2$ and definition of A_i, since $\Delta_i \wedge \Box\Diamond\langle M\rangle_v$ equals $\Box\Diamond\langle\Delta_i \wedge M\rangle_v$ (because Δ_i is a constant), and $\Box\Diamond(F \vee G)$ is equivalent to $(\Box\Diamond F) \vee (\Box\Diamond G)$ for any temporal formulas F and G.

$\langle 1\rangle 10.$ Q.E.D.

$\langle 2\rangle 1.$ $S \wedge H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l \Rightarrow \Box I^{all} \wedge \Box[N^{all}]_{all}$

$\langle 3\rangle 1.$ $(v' = v) \wedge I^r \wedge I^l \wedge (I^l)' \wedge N^c \wedge N^r \wedge N^p \wedge N^l \Rightarrow (all' = all)$

$\langle 4\rangle 1.$ $(v' = v) \wedge N^c \Rightarrow \langle b, c\rangle' = \langle b, c\rangle$

PROOF: By definition of N^c.

$\langle 4\rangle 2.$ $I^r \wedge (v' = v) \wedge N^r \Rightarrow (r' = r)$

PROOF: Follows from the definitions of I^r and N^r, and the hypothesis that the free variables of $\mathcal{R}$ are included in the tuple of variables v, which implies $(v' = v) \Rightarrow (\mathcal{R}' = \mathcal{R})$.

$\langle 4 \rangle 3.$ $(v' = v) \wedge N^p \Rightarrow (p' = p)$

PROOF: Immedate from the definition of N^p.

$\langle 4 \rangle 4.$ $(v' = v) \wedge N^p \wedge I^l \wedge (I^l)' \wedge N^l \Rightarrow (l' = l)$

$\langle 5 \rangle 1.$ CASE: p

$\langle 6 \rangle 1.$ $I^l \Rightarrow (l = l_{\mathit{final}})$

PROOF: Assumption $\langle 5 \rangle$ and definition of I^l.

$\langle 6 \rangle 2.$ $(v' = v) \wedge N^p \Rightarrow p'$

PROOF: Assumption $\langle 5 \rangle$ and definition of N^p.

$\langle 6 \rangle 3.$ $(I^l)' \wedge p' \Rightarrow (l' = l'_{\mathit{final}})$

PROOF: By definition of I^l.

$\langle 6 \rangle 4.$ $(v = v') \Rightarrow (l'_{\mathit{final}} = l_{\mathit{final}})$

PROOF: By definition of l_{final}, since, for any constant tuple u, v are the only free variables of $\lambda(u)$.

$\langle 6 \rangle 5.$ Q.E.D.

PROOF: The level-$\langle 4 \rangle$ goal follows from $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, and $\langle 6 \rangle 4$.

$\langle 5 \rangle 2.$ CASE: $\neg p$

$\langle 6 \rangle 1.$ $N^p \Rightarrow \neg p'$

PROOF: Assumption $\langle 5 \rangle$ and the definition of N^p.

$\langle 6 \rangle 2.$ CASE: $\neg \mathcal{L}$

PROOF: In this case, $(v' = v)$ implies $\neg \mathcal{L}'$, so by $\langle 6 \rangle 1$, $I^l \wedge (I^l)' \wedge N^p \wedge (v' = v)$ implies $l = v = v' = l'$.

$\langle 6 \rangle 3.$ CASE: $\mathcal{L}$

PROOF: In this case, assumption $\langle 5 \rangle$ implies $(v' = v) \wedge N^l \Rightarrow (l = l')$.

$\langle 6 \rangle 4.$ Q.E.D.

PROOF: Cases $\langle 6 \rangle 2$ and $\langle 6 \rangle 3$ are exhaustive.

$\langle 5 \rangle 3.$ Q.E.D.

PROOF: By $\langle 5 \rangle 1$ and $\langle 5 \rangle 2$.

$\langle 4 \rangle 5.$ Q.E.D.

PROOF: By $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$, $\langle 4 \rangle 4$, and the definition of *all*.

$\langle 3 \rangle 2.$ $\Box[N]_v \wedge \Box I^r \wedge \Box I^l \wedge \Box[N^c]_{\langle v,b,c \rangle} \wedge \Box[N^r \wedge (v' \neq v)]_{\langle v,r \rangle}$
$\wedge \Box[N^p]_{\langle v,p \rangle} \wedge \Box[N^l \wedge (\langle p, v \rangle' \neq \langle p, v \rangle]_{\langle v,b,c,p,l \rangle} \Rightarrow \Box[N^{all}]_{all}$

PROOF: By the definition of N^{all}, $\langle 3 \rangle 1$, repeated application of the rule

$$\frac{\begin{array}{l} \wedge\ (g = g') \wedge A \Rightarrow (f = f') \\ \wedge\ (f = f') \wedge B \Rightarrow (g = g') \end{array}}{[A]_f \wedge [B]_g \equiv [A \wedge B]_{\langle f,g \rangle}}$$

and the usual TLA rules

$$\Box I \wedge \Box[A]_f \Rightarrow \Box[I \wedge I' \wedge A]_f \qquad \frac{[A]_f \wedge [B]_g \Rightarrow [C]_h}{\Box[A]_f \wedge \Box[B]_g \Rightarrow \Box[C]_h}$$

$\langle 3\rangle 3$. Q.E.D.

PROOF: Follows easily from $\langle 3\rangle 2$, $\langle 1\rangle 2$, the definitions, and the rule that $\Box$ distributes over $\wedge$.

$\langle 2\rangle 2$. $S \wedge Q \wedge O \wedge H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l$

$\Rightarrow \overline{S^R} \wedge \Box I(\overline{v}/\widehat{v}) \wedge (\forall i \in \mathcal{I} : \Box\Diamond\langle A_i\rangle_v \Rightarrow \Box\Diamond\langle\overline{A_i^R}\rangle_{\overline{v}})$

PROOF: $\langle 2\rangle 1$, $\langle 1\rangle 7$, $\langle 1\rangle 8$, $\langle 1\rangle 9$, and the definition of S^R.

$\langle 2\rangle 3$. $S \wedge Q \wedge O \wedge H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l$

$\Rightarrow \exists\, \widehat{v} : \widehat{S^R} \wedge \Box I \wedge (\forall i \in \mathcal{I} : \Box\Diamond\langle A_i\rangle_v \Rightarrow \Box\Diamond\langle\widehat{A_i^R}\rangle_{\widehat{v}})$

PROOF: $\langle 2\rangle 2$ and (temporal) predicate logic.

$\langle 2\rangle 4$. $S \wedge Q \wedge O \wedge (\exists\, b, c, r, p, l : H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l)$

$\Rightarrow (\exists\, \widehat{v} : \widehat{S^R} \wedge \Box I \wedge (\forall i \in \mathcal{I} : \Box\Diamond\langle A_i\rangle_v \Rightarrow \Box\Diamond\langle\widehat{A_i^R}\rangle_{\widehat{v}}))$

PROOF: $\langle 2\rangle 3$ and (temporal) predicate logic, since b, c, r, p, and l do not occur free in S, Q, O, or

$$\exists\, \widehat{v} : \widehat{S^R} \wedge \Box I \wedge (\forall i \in \mathcal{I} : \Box\Diamond\langle A_i\rangle_v \Rightarrow \Box\Diamond\langle\widehat{A_i^R}\rangle_{\widehat{v}})$$

$\langle 2\rangle 5$. $S \wedge Q \;\Rightarrow\; (\exists\, b, c, r, p, l : H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l)$

$\langle 3\rangle 1$. $H^c \wedge \Box I^c \wedge S \Rightarrow \exists\, r : H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r$

PROOF: By $\langle 1\rangle 4$, since r does not occur free in H^c and I^c.

$\langle 3\rangle 2$. $H^c \wedge \Box I^c \wedge S \wedge Q \Rightarrow \exists\, p, l : P^p \wedge P^l$

PROOF: $\langle 1\rangle 5$.

$\langle 3\rangle 3$. $H^c \wedge \Box I^c \wedge S \wedge Q \Rightarrow \exists\, r, p, l : H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l$

PROOF: $\langle 3\rangle 1$ and $\langle 3\rangle 2$, since r does not occur free in P^p or P^l, and p and l do not occur free in H^c, $\Box I^c$, H^r, or $\Box I^r$. (We are using the rule that if x does not occur free in F, then $(\exists\, x : F \wedge G) \equiv F \wedge (\exists\, x : G)$.)

$\langle 3\rangle 4$. $S \wedge Q \wedge (\exists\, b, c : H^c \wedge \Box I^c) \Rightarrow \exists\, b, c, r, p, l : H^c \wedge \Box I^c \wedge H^r \wedge \Box I^r \wedge P^p \wedge P^l$

PROOF: By $\langle 3\rangle 3$, since b and c do not occur free in S or Q. (We are using the rule that if x does not occur free in F, then $(\exists\, x : F \wedge G) \equiv F \wedge (\exists\, x : G)$.)

$\langle 3\rangle 5$. Q.E.D.

PROOF: By $\langle 3\rangle 4$ and $\langle 1\rangle 5$.

$\langle 2\rangle 6$. Q.E.D.

PROOF: $\langle 2\rangle 4$ and $\langle 2\rangle 5$.