Sun 12 Apr 1992 [14:36]

1 ACTION DEFINITIONS

For any n-tuple e of expressions, n-tuple v of variables, and action A:

* A(e/v) denotes the formula obtained by substituting the e for unprimed occurrences of v in A.
* A(e/v′) denotes the formula obtained by substituting the e for primed occurrences of v in A.
* A(e1/v,e2/v′) denotes the obvious (simultaneous) substitution for v and v′.

For actions A and B, we define A·B to be the action such that

$$s[[A \cdot B]]t \;\triangleq\; \exists\, r : s[[A]]r \;\wedge\; r[[B]]t$$

If v is the n-tuple of all variables occurring (primed or unprimed) in A and B and w is an n-tuple of rigid variables that do not occur free in A or B, then

$$A \cdot B = \exists\, w : A(w/v') \;\wedge\; B(w/v)$$

For an action A, integer $i > 0$

$$A^i \triangleq \text{IF } i = 1 \text{ THEN } A \text{ ELSE } A \cdot A^{i-1}$$

$$A^+ \triangleq \exists\, i > 0 : A^i$$

We would like to define A^* to equal Id $\vee$ A^+, where Id is the identity relation. Unfortunately, Id isn′t an action--it can′t be expressed by any finite formula. However, we can define Id semantically by

$$s[[Id]]t \triangleq (s = t)$$

From which we get

$$s[[A^*]]t \triangleq (s = t) \;\vee\; s[[A^+]]t$$

Although A^* by itself isn′t an action, certain expressions involving A^* are actions. In particular, for any actions A and B, and any predicate P, we can define

$$A^* \cdot B \;\triangleq\; B \;\vee\; A^+ \cdot B$$
$$B \cdot A^* \;\triangleq\; B \;\vee\; B \cdot A^+$$
$$A^* \;\wedge\; P' \;\triangleq\; P \;\vee\; (A^+ \;\wedge\; P')$$

(The semantic definition of A^* makes the left-hand sides of these definitions semantically equivalent to the right-hand sides.)

For any action A, the action A^{-1} is defined syntactically to be the action obtained by interchanging primed and unprimed variables. That is, if v is the tuple of all variables in A, then A^{-1} equals

$A(v/v', v'/v)$. For example, $(x' = x+1)^{-1} = (x = x'+1)$. Semantically,

$$s [\![A^{-1}]\!] t \triangleq t [\![A]\!] s$$

The following relations hold

$$(A \cdot B)^{-1} = (B^{-1}) \cdot (A^{-1})$$
$$(A^{+})^{-1} = (A^{-1})^{+}$$
$$(A^{*})^{-1} = (A^{-1})^{*} \quad \text{(in any action expression involving } A^{*})$$

2 THE REDUCTION THEOREM

A reduction theorem allows one to prove properties of a program Π by reasoning about a simpler "reduced" program Π_r. The conclusion of such a theorem should be something like $\Pi \Rightarrow \Pi_r$, which implies that Π satisfies any property satisfied by Π_r.

In the standard reduction theorems, starting from Lipton's classic 1972 paper, the reduced program is obtained by replacing a composite statement R;X;L with the atomic action $\langle$R;X;L$\rangle$, where X is atomic. (Angle brackets $\langle$...$\rangle$ enclose an atomic action.) To translate this into TLA, we first have to figure out how to express R;X;L and $\langle$R;X;L$\rangle$.

In TLA, all forms of traditional statement composition are represented by disjunction. If A_i is the TLA action corresponding to program statement S_i, then the TLA action corresponding to $S_1;S_2$ is $A_1 \vee A_2$. The fact that the disjunction represents $S_1;S_2$ rather than S_2;S-1 or $S_1 \| S_2$ (parallel composition) is determined by how A_1 and A_2 modify the control state.

The atomic action $\langle$R;X;L$\rangle$ means execute R, then X, then L all as a single action. Since X is atomic, the TLA counterpart of executing X is just taking an X step. Since R is nonatomic, the TLA counterpart of executing R is doing any number of R steps---and similarly for L. Therefore, executing $\langle$R;X;L$\rangle$ corresponds to taking an $R^{*} \cdot X \cdot L^{*}$ step. But, an $R^{*} \cdot X \cdot L^{*}$ step corresponds to the execution of $\langle$R;X;L$\rangle$ only if it starts in an "initial" state of R and ends in a "final" state of L. So, the TLA action corresponding to $\langle$R;X;L$\rangle$ is

$$\text{(initial state of R)} \wedge R^{*} \cdot X \cdot L^{*} \wedge \text{(final state of L)}'$$

The first conjunct is unnecessary because the reduced program doesn't take any R steps--except as part of an atomic $R^{*} \cdot X \cdot L^{*}$ step--so it can never reach an "internal" state of R. One of the hypotheses of the reduction theorem is that, once control reaches statement L, that statement can always be executed until it finishes. In other words, an "internal" state of L is one in which L is enabled. Hence, a final state of L has been reached when L is not enabled, so the final conjunct can be written as $\neg(\text{Enabled } L)'$.

Putting all this together, we get the following correspondence:

Pgming-Language Version	TLA Version
original program	next-state relation N
R;X;L	$R \lor X \lor L$
$\langle$R;X;L$\rangle$	$R^* \cdot X \cdot L^* \land \neg(\text{Enabled } L)'$
reduced program =	reduced next-state relation =
original pgm	$\lor \land N$
- R;X;L	$\land \neg(R \lor X \lor L)$
+ $\langle$R;X;L$\rangle$	$\lor R^* \cdot X \cdot L^* \land \neg(\text{Enabled } L)'$

The conclusion of the reduction theorem doesn't assert that $\Pi \Rightarrow \Pi_r$; it's more complicated. Let v be the tuple of all variables that actually occur in Π, and let w be a tuple of "pretend" variables, that are different from the variables of v. The theorem asserts that there are some pretend variables w such that Π implies Π_r with the actual varaibles v replaced by the pretend variables w. In other words, the conclusion asserts:

$$\Pi \Rightarrow \exists\, w : \Pi_r(w/v, w'/v')$$

For this to be of any use, we need to know the relations between the actual variables v and the pretend variables w. The assertion is that one of the following holds:

* $v = w$: They're equal.
* $L^+(w/v')$: Some sequence of L steps will convert the real variables to the pretend ones.
* $(R^{-1})^+(w/v')$: Some sequence of backwards R steps will convert the real variables to the pretend ones. (Equivelently, some sequence of R steps will convert the pretend variables to the real ones.)

For this to hold, it's necessary that Π imply that if control reaches L, then eventually L finishes. Since L finishing means $\neg$(Enabled L), this means that Π must imply $\Box\Diamond\neg$(Enabled L). So, in the theorem, we include $\Box\Diamond\neg$(Enabled L) as a conjunct of Π.

Now, for the hypotheses. Hypothesis 1 asserts that $R \lor X \lor L$ represents R;X;L (instead of L;R;X or (L $\|$ X);R or ...) and that L remains enabled until it's finished.

1(a) It's not possible to take an L step from an initial state or a state in which an R or X step is possible.
 (b) Only an X step can go from a state in which an L step is impossible to one in which it's possible.
 (c) Only an L step can disable L.
 (d) R and X are disjoint. (The disjointess of R and X from

L follows from hypothesis 1(a).)

(e) The statement R;X;L occurs in the original program.

Hypothesis 2 is the more interesting hypothesis, asserting commutativity conditions on the actions.

2(a) The actions of R right commute with all program actions except those of R;X;L. Action A right commutes with action B means that if it's possible to take an A step followed by a B step, then the same effect can be obtained by taking a B step followed by an A step.

(b) The actions of L left commute with all program actions except those of R;X;L.

Unfortunately, I don't have time now to go into the significance of this theorem, and how it is used. Here's the precise statement of the theorem.

REDUCTION THEOREM: Assume that N, R, X, L are actions, Init a predicate, f a state function, and v an n-tuple of variables.

LET $S \triangleq R \lor X \lor L$

$M \triangleq N \land \neg S$

$N_r \triangleq M \lor (R^* \cdot X \cdot L^* \land \neg(\text{Enabled } L)')$

$w \triangleq$ an n-tuple of variables distinct from v.

IF

0. v includes all variables occurring in N, R, X, L, Init, or f.

1. (a) $\text{Init} \lor \text{Enabled } R \lor \text{Enabled } X \Rightarrow \neg(\text{Enabled } L)$
   (b) $\neg(\text{Enabled } L) \land [N]_f \land \neg X \Rightarrow \neg(\text{Enabled } L)'$
   (c) $(\text{Enabled } L) \land [N]_f \land \neg L \Rightarrow (\text{Enabled } L)'$
   (d) $\neg(R \land X)$
   (e) $S \Rightarrow N$

2. (a) $R \cdot [M]_f \Rightarrow [M]_f \cdot R$
   (b) $[M]_f \cdot L \Rightarrow L \cdot [M]_f$

THEN

$$\begin{array}{l} \text{Init} \land \Box[N]_f \land \Box\Diamond\neg(\text{Enabled } L) \Rightarrow \\ \quad \exists\, w : \land\ \text{Init}(w/v) \land \Box[N_r(w/v,\ w'/v')]_{f(w/v)} \\ \qquad\qquad \land\ \Box((v = w) \lor L^+(w/v') \lor (R^{-1})^+(w/v')) \end{array}$$

This theorem is of the form

$$\Pi \Rightarrow \exists\, w : \Pi_r$$

To prove the theorem, one must construct a refinement mapping--a tuple of state functions $\overline{w}$ such that

$$\Pi \Rightarrow \overline{\Pi_r}$$

To define $\overline{w}$, we first construct a history variable h and prophesy variable p as follows:

* h equals v unless control is in the middle of R, in which case it

is a tuple of values such that it′s possible to get from a state in which v = h to a state in which v has its current value by doing a sequence of R steps. The variable h remembers what the value of v was before execution of R began, except it changes its memory so it can pretend that no actions of the rest of the program occurred.

* p equals v unless control is at or inside L, in which case it is a sequence of values for v that can be produced from v′s current value by finishing the execution of L. The variable p predicts what L is going to do, changing its prediction to account for actions taken by the rest of the program.

We then define $\overline{w}$ to equal h if control is in R, the last element of the sequence p if control is in L, and v otherwise.

PROOF OF REDUCTION THEOREM
NOTATION:
Assume v an n-tuple of variables.

For any n-tuple of values q and r and action A:

$$q.A.r \triangleq A(q/v, r/v')$$

$$\| f \| \triangleq \text{Choose } m : \text{dom } f = [0 \,..\, m]$$

For any action A:

$$f//A//v \triangleq \begin{array}{l} \wedge\ \| f \| \in \text{Nat} \\ \wedge\ \text{dom } f = [0 \,..\, \| f \|] \\ \wedge\ \forall\, i \in [0 \,..\, \| f \|] : f[i] \text{ an n-tuple of values} \\ \wedge\ \forall\, i \in [1 \,..\, \| f \|] : f[i-1].A.f[i] \end{array}$$

LEMMA 1: Let A and B be actions whose free variables are among the variables of v, let q be an n-tuple of values, and assume f//A//v.

(a) If $A \cdot B \Rightarrow B \cdot A$ and $f[\| f \|].B.q$, then there exists g such that
   (i) $\| g \| = \| f \|$
   (ii) g//A//v
   (iii) f[0].B.g[0]
   (iv) $g[\| g \|] = q$

(b) If $B \cdot A \Rightarrow A \cdot B$ and q.B.f[0], then there exists g such that
   (i) $\| g \| = \| f \|$
   (ii) g//A//v,
   (iii) $g[\| g \|].B.f[\| f \|]$
   (iv) g[0] = q

Proof of (a): By induction on $\| f \|$.
1. Case $\| f \| = 0$.
   Pf: Trivial. Take $\| g \| = 0$ and g[0] = q.

2. Induction step:
   Assume: Lemma true for $\| f \| = m \ \wedge \ \| f \| = m+1$
   2.1. f[m].A.f[m+1] and f[m+1].B.q.

Pf: By hypothesis and assumption $m+1 = \| f \|$.

2.2. Choose n-tuple r such that f[m].B.r and r.A.q.

Pf: 2.1 and hypothesis that $AB \Rightarrow BA$.

2.3. Let $d \triangleq [i \in [0 .. m] \mapsto f[i]]$. Then $\| d \| = m$, d//A//v and $d[\| d \|]$.B.r.

Pf: Follows immediately from the definition of d, the assumption f//A//v, and the assumption 2.2.

2.4. Choose e such that e//A//v, d[0].B.e[0], and $e[\| e \|] = r$.

Pf: 2.3 and induction hypothesis.

2.5. QED

Pf: Let $g \triangleq [i \in [0 .. m+1] \mapsto \text{IF } i = m+1 \text{ THEN } q \text{ ELSE } e[i]]$

Then g//A//v follows from e//A//v, $e[m] = r$ (by 2.4) and r.A.q (by 2.2).

f[0].B.g[0] follows from d[0].B.e[0], since $d[0] = f[0]$ and $g[0] = e[0]$.

$g[\| g \|] = q$ follows from the definition of g.

Proof of (b): similar.

LEMMA 2: Let v be a tuple containing all variables in A, u, and P. Then

$$\models \Box[A]_u \wedge \Diamond P \Rightarrow \exists f : \begin{array}{l} \wedge\ f//[A]_u//v \\ \wedge\ \forall i \in [0 .. \| f \| -1] : \neg f[i].P \\ \wedge\ f[0] = v \\ \wedge\ f[\| f \|].P \end{array}$$

Assume: $\sigma \models \models \Box[A]_u \wedge \Diamond P$

Prove: $\exists f : \sigma \models \begin{array}{l} \wedge\ f//[A]_u//v \\ \wedge\ \exists i \in [0 .. \| f \| -1] : \neg f[i].P \\ \wedge\ f[0] = v \\ \wedge\ f[\| f \|].P \end{array}$

1. $\forall i \in Nat : \sigma_i [[[A]_u]] \sigma_{i+1}$

Pf: Assumption $\sigma \models \Box[A]_u$.

2. $\forall i \in Nat : \sigma_i [[v]] . [A]_u . \sigma_{i+1} [[v]]$

Pf: 1 and assumption v includes all variables free in A and u.

3. Let $n = \text{minimum } \{i : \sigma_i.P\}$. Then $n \in Nat$.

Pf: Assumption that $\sigma \models \Diamond P$.

4. QED

Pf: Choose $f = [i \in [0 .. n] \mapsto \sigma_i [[v]]]$.

Then $f//[A]_u//v$ follows from 2 and 3.

LEMMA 3: Let v include all free variables of A and B.

If (a) $f//A \vee B//v$ and (b) $\models B \cdot A \Rightarrow A \cdot B$

Then there exists g and h such that

(i) g//A//v

(ii) h//B//v

(iii) $f[0] = g[0] \wedge f[\| f \|] = h[\| h \|] \wedge g[\| g \|] = h[0]$

Proof Sketch: This is a straightforward induction argument, moving all the "A actions" in f to the left.

1. Let h be a variable distinct from the variables in v, and let

$$F^h \triangleq [i \in [0 .. 0] \mapsto v]$$

$$G^h \triangleq \text{CASE}$$

$$\begin{array}{l} R \rightarrow [i \in [0 .. \|h\|+1] \\ \qquad \mapsto \text{IF } i = \|h\|+1 \text{ THEN } v' \text{ ELSE } h[i]\ ] \\ X \rightarrow [i \in [0 .. 0] \mapsto v'] \\ \neg(R \lor X) \rightarrow \text{IF } \|h\| = 0 \\ \qquad \text{THEN } [i \in [0 .. 0] \mapsto v'] \\ \qquad \text{ELSE Choose } q : \begin{array}{l} \land\ \|q\| = \|h\| \\ \land\ q//R//v \\ \land\ h[0].[M]_f.q[0] \\ \land\ q[\|q\|] = v' \end{array} \end{array}$$

$$H \triangleq h = F^h \land \Box[h' = G^h]_{(v,h)}$$

$$I^h \triangleq \begin{array}{l} 1. \land\ h//R//v \\ 2. \land\ h[\|h\|] = v \\ 3. \land\ \|h\| > 0 \Rightarrow \neg(\text{Enabled } L) \end{array}$$

Then H defines h to be a history variable for
$\text{Init} \land \Box[N]_f \land \Box\Diamond(\text{Enabled } L)$, and
$\models \text{Init} \land \Box[N]_f \land H \Rightarrow \Box I^h$

Pf: It's obvious that H defines h to be a history variable.
We now prove $\models \text{Init} \land \Box[N]_f \land H \Rightarrow \Box I^h$.

<2>1. $(h = F^h) \Rightarrow I^h$

Pf: Immediate from def of F^h and I^h.

<2>2. $[h' = G^h]_{(v,h)} \land [N]_f \land I^h \Rightarrow I^{h\prime}$

<3>1. $(h' = G^h) \land [N]_f \land I^h \Rightarrow I^{h\prime}$

Assume: $(h' = G^h) \land [N]_f \land I^h$

Prove: $I^{h\prime}$

<4>1. Case R.

<5>1. $I^{h\prime}.1$

Pf: Immediate from the definition of G^h, the assumption $I^h.1$, and the definition of $h'//R//v$.

<5>2. $I^{h\prime}.2$

Pf: Immediate.

<5>3. $I^{h\prime}.3$

<6>1. ¬(Enabled L)

Pf: Hypothesis 1(a) and R [Case <4>]

<6>2. ¬X

Pf: Hypotehsis 1(d) and R [Case <4>]

<6>3. QED

Pf: <6>1, <6>2, R, and Hypothesis 1(e).

<4>2. Case X

Pf: Immediate from definition of G^h, since $h'//R//v$ is vacuous when $\|h'\| = 0$.

$\langle 4\rangle 3$. Case $\neg(R \lor X) \land \|h\| = 0$.
Pf: Immediate from definition of G^h, since $h'//R//v$ is vacuous when $\|h'\| = 0$.

$\langle 4\rangle 4$. Case $\neg(R \lor X) \land \|h\| > 0$.

$\langle 5\rangle 1$. $\neg L$
Pf: $\|h\| > 0$ (Case $\langle 4\rangle$ assumption) and $I^h.3$.

$\langle 5\rangle 2$. $[M]_f$
Pf: $[N]_f \land \neg(R \lor X)$ [Case $\langle 4\rangle$] $\land \neg L$ ($\langle 5\rangle 1$)

$\langle 5\rangle 3$. $h[\|h\|].[M]_f.v'$
Pf: $\langle 5\rangle 2$ and $I^h.2$.

$\langle 5\rangle 4$. $\exists\, q : \land\ \|q\| = \|h\|$
$\quad\land\ q//R//v$
$\quad\land\ h[0].[M]_f.q[0]$
$\quad\land\ q[\|q\|] = v'$
Pf: By Part (a) of Lemma 1, using $I^h.1$, $\langle 5\rangle 3$, and Hypothesis 2(a).

$\langle 5\rangle 5$. (a) $\|h'\| = \|h\|$
(b) $h'//R//v$
(c) $h'[\|h'\|] = v'$
Pf: $\langle 5\rangle 4$ and def of G^h.

$\langle 5\rangle 6$. $\neg(\text{Enabled } L) \Rightarrow \neg(\text{Enabled } L)'$
Pf: $\neg X$ [Case $\langle 4\rangle$], $[N]_f$ [Assumption $\langle 3\rangle$], and hypothesis 1(b).

$\langle 5\rangle 7$. QED
Pf: $I^{h}{}'.1$ and $I^{h}{}'.2$ follow from $\langle 5\rangle 5$ (b) and (c), and $I^{h}{}'.3$ follows from $I^h.3$, $\langle 5\rangle 5$(c) and $\langle 5\rangle 6$.

$\langle 3\rangle 2$. $(v,h)' = (v,h) \land [N]_f \land I^h \Rightarrow I^{h}{}'$
Pf: Immediate, since hypothesis 0 implies that v and h are only variables that occur in I^h.

$\langle 3\rangle 3$. QED
Pf: $\langle 3\rangle 1$ and $\langle 3\rangle 2$.

$\langle 2\rangle 3$. QED
Pf: $\langle 2\rangle 1$, $\langle 2\rangle 2$, and TLA rule INV

2. Let p be a variable distinct from h and the variables in v, and let

$$I^p \triangleq \begin{array}{l} 1.\ \land\ p//L//v \\ 2.\ \land\ p[0] = v \\ 3.\ \land\ \neg p[\|p\|].(\text{Enabled } L) \end{array}$$

$$G^p \triangleq \begin{array}{l} \text{CASE} \\ \quad L \rightarrow [\, i \in [0 \,..\, \|p\|'+1] \\ \qquad\qquad \mapsto \text{IF } i = 0 \text{ THEN } v \text{ ELSE } p'[i-1]\,] \\ \quad \neg(\text{Enabled } L) \rightarrow [i \in [0 \,..\, 0] \mapsto v] \\ \quad \neg L \land (\text{Enabled } L) \rightarrow \\ \qquad\quad \text{Choose } q : \land\ \|q\| = \|p'\| \\ \qquad\qquad\qquad\quad \land\ q//L//v \end{array}$$

$\land\ q[\|q\|].[M]_f.p'[\|p'\|]$
$\land\ q[0] = v$

$P \ \triangleq\ \Box I^p \land \Box[p = G^p]_{(p,v)}$

Then P defines p to be a prophecy variable for
$\quad Init \land \Box[N]_f \land \Box\Diamond\neg(\text{Enabled } L) \land H$.

<2>1. p does not occur unprimed in G^p.
Pf: trivial.

<2>2. p does not occur free in
$\quad Init \land \Box[N]_f \land \Box\Diamond\neg(\text{Enabled } L) \land H$.
Pf: trivial.

<2>3. $[N]_f \land I^{p\prime} \land (p = G^p) \Rightarrow I^p$
Assume: $[N]_f \land I^{p\prime} \land (p = G^p)$
Prove: I^p
<3>1. Case L
<4>1. p//L//v
<5>1. For $i \in [2\ ..\ \|p\|] : p[i-1].L.p[i]$
Pf: By $I^{p\prime}$.1 and def of G^p.
<5>2. For $i \in p[0].L.p[1]$
Pf: By $I^{p\prime}$.2, which implies $p'[0] = v'$,
def of G^p, which implies $p[0] = v$ and $p[1] = p'[0]$,
and L [Case <3>].
<5>3. QED
Pf: Immediate from <5>1, <5>2, def of G^p and,
$I^{p\prime}$.1.
<4>2. $p[0] = v$
Pf: Immediate from the definition of G^p.
<4>3. $\neg p[\|p\|].(\text{Enabled } L)$
By $I^{p\prime}$.3, since the def of G^p implies
$p[\|p\|] = p'[\|p'\|]$.
<4>4. QED
Pf: <4>1 - <4>3.

<3>2. Case $\neg(\text{Enabled } L)$
Pf: Immediate from def of G^p and I^p.

<3>3. Case $\neg L \land (\text{Enabled } L)$
<4>1. $\neg(X \lor R)$
Pf: Enabled L [Case <3>] and Hypothesis 1(a).
<4>2. $[M]_f$
Pf: $\land\ [N]_f$ [Assumption <2>]
$\land\ \neg L$ [Case <3>]
$\land\ \neg(X \lor R)$ [<4>1.]
<4>3. $v.[M]_f.p'[0]$
Pf: <4>2 and $I^{p\prime}$.3
<4>4. $\exists\, q : \land\ \|q\| = \|p'\|$
$\land\ q//L//v$
$\land\ q[\|q\|].[M]_f.p'[\|p'\|]$
$\land\ q[0] = v$
Pf: <4>3, Hypothesis 2(b), and part (b) of Lemma 1.

<4>5. (a) $p//L//v$
(b) $p[\|p\|].[M]_f.p'[\|p'\|]$
(c) $p[0] = v$
Pf: <4>4 and def of G^p.
<4>6. $\neg(\text{Enabled } L)' \land [M]_f \Rightarrow \neg(\text{Enabled } L)$
Pf: Hypothesis 1(c), since $[M]_f \Rightarrow [N]_f \land \neg L$.
<4>7. $\neg p[\|p\|].(\text{Enabled } L)$.
Pf: <4>5(b) and <4>6.
<4>8. QED
Pf: <4>5(a), <4>5(c), and <4>7.

<2>4. $\text{Init} \land \Box[N]_f \land \Box\Diamond\neg(\text{Enabled } L) \Rightarrow \Box(\exists\, p : I^p)$
<3>1. $\models \Box[N]_f \land \Diamond\neg(\text{Enabled } L) \Rightarrow \exists\, p : I^p$
<4>1. $\models \Box[N]_f \land \Diamond\neg(\text{Enabled } L) \Rightarrow$
$\exists\, g : \land\ g//[N]_f//v$
$\land\ \forall\, i \in [0 \,..\, \|g\|-1] : g[i].(\text{Enabled } L)$
$\land\ g[0] = v$
$\land\ \neg g[\|g\|].(\text{Enabled } L)$
Pf: Lemma 2.
<4>2. $\models \Box[N]_f \land \Diamond\neg(\text{Enabled } L) \Rightarrow$
$\exists\, g : \land\ g//[M]_f \lor L//v$
$\land\ \forall\, i \in [0 \,..\, \|g\|-1] : g[i].(\text{Enabled } L)$
$\land\ g[0] = v$
$\land\ \neg g[\|g\|].(\text{Enabled } L)$
Pf: <4>1 and Hypothesis 1(a), since
$[N]_f \land \neg R \land \neg X = [M]_f \lor L$.
<4>3. $\models \Box[N]_f \land \Diamond\neg(\text{Enabled } L) \Rightarrow$
$\exists\, q, t : \land\ q//L//v \land t//[M]_f//v$
$\land\ q[0] = v \land q[\|q\|]=t[0]$
$\land\ \neg t[\|t\|].(\text{Enabled } L)$
Pf: <4>2 and Lemma 3.
<4>4. $\models \Box[N]_f \land \Diamond\neg(\text{Enabled } L) \Rightarrow$
$\exists\, q, t : \land\ q//L//v \land t//[M]_f//v$
$\land\ q[0] = v \land q[\|q\|]=t[0]$
$\land\ \neg q[\|q\|].(\text{Enabled } L)$
Pf: <4>3, since Hypothesis 1(c) implies
$t//[M]_f//v \land \neg t[\|t\|].(\text{Enabled } L)$
$\Rightarrow \neg t[0].(\text{Enabled } L)$.
<4>5. QED
Pf: Immediate, from <4>4.

<3>2. QED
Pf: <3>1 and simple temporal logic reasoning.
<2>5. $\text{Init} \land \Box[N]_f \land \Box\Diamond\neg(\text{Enabled } L)$
$\Rightarrow \Box\Diamond(\{p : I^p\} \text{ is finite})$
<3>1. $\neg(\text{Enabled } L) \Rightarrow (I^p = (p = [i \in [0 \,..\, 0] \mapsto v]))$
Pf: Def of $p//L//v$ and I^p.
<3>2. QED
Pf: By <3>1, $\neg(\text{Enabled } L) \Rightarrow \text{Cardinality}(\{p : I^p\}) = 1$.

<2>6. QED

Pf: <2>1-<2>5.

LET $\overline{w} \triangleq$ IF Enabled L THEN $p[\,\|\,p\,\|\,]$
ELSE $h[0]$

$\overline{F} \triangleq F(\overline{w}/v)$, for any formula F.

3. $\models \text{Init} \ \wedge \ \Box[N]_f \ \wedge \ H \ \wedge \ P \ \Rightarrow \ \overline{\text{Init}} \ \wedge \ \overline{[N_r]_f}$

<2>1. $\text{Init} \ \wedge \ h = F^h \ \Rightarrow \ \overline{\text{Init}}$

Pf: Hypothesis 1(a) and definitions of $\overline{w}$ and F^h.

<2>2. $\wedge \ I^h \ \wedge \ I^{h\prime} \ \wedge \ I^p \ \wedge \ I^{p\prime}$
$\wedge \ [N]_f \ \wedge \ [h' = G^h]_{(v,h)} \ \wedge \ [p = G^p]_{(v,p)}$
$\Rightarrow \ \overline{[N_r]_f}$

Assume: 1. $I^h \ \wedge \ I^{h\prime} \ \wedge \ I^p \ \wedge \ I^{p\prime}$
2. $[N]_f$
3. $[h' = G^h]_{(v,h)}$
4. $[p = G^p]_{(v,p)}$

Prove: $\overline{[N_r]_f}$

<3>1. Case R

<4>1. $\neg$(Enabled L)

Pf: Hypothesis 1(a).

<4>2. $\neg$(Enabled L)$'$

Pf: <4>1, Hypothesis 1(d) and Hypothesis 1(b).

<4>3. $\overline{w}' = \overline{w}$

Pf: Assumption <2>.3, def of G^h, def of $\overline{w}$, and <4>1 and <4>2.

<4>4. QED

Pf: <4>3 and hypothesis 0 imply $\overline{f}' = \overline{f}$.

<3>2. Case X

<4>1. $\overline{w} = h[0]$

Pf: Hypothesis 1(a) and def of $\overline{w}$.

<4>2. $\overline{w}.R^*.v$

Pf: I^h [Assumption <2>.1] and <6>1.

<4>3. $v'.L^*.\overline{w}' \ \wedge \ \neg(\text{Enabled L})'.\overline{w}'$

<5>1. Case (Enabled L)$'$

<6>1. $\overline{w}' = p'[\,\|\,p'\,\|\,]$

Pf: (Enabled L)$'$ [Case <5>] and def of $\overline{w}$.

<6>2. QED

Pf: $I^{p\prime}$ [Assumption <2>.1 and <2>.3] and <6>1.

<5>2. Case $\neg$(Enabled L)$'$

<6>1. $\overline{w}' = v'$

Pf: Case <5> and def of $\overline{w}$.

<6>2. QED

Pf: <6>1, since $q.L^*.q$ holds for any q.

<5>3. QED

Pf: <5>1 and <5>2.

<4>4. $v.X.v'$

Pf: Case <3>.

<4>5. $\overline{w}.(R^* \cdot X \cdot L^* \ \wedge \ \neg(\text{Enabled L})'.\overline{w}'$

Pf: <4>2 - <4>4.

<4>6. QED

Pf: By <4>5, since $R^* \cdot X \cdot L^* \Rightarrow N_r$.

<3>3. Case L

<4>1. $\overline{w} = p[\,\|p\|\,]$

Pf: Def of $\overline{w}$, Case <3>.

<4>2. $p[\,\|p\|\,] = p'[\,\|p'\|\,]$

Pf: $p = G^p$ and def of G^p.

<4>3. $\overline{w}' = \overline{w}$

<5>1. Case (Enabled L)$'$

<6>1. $\overline{w}' = p'[\,\|p'\|\,]$

Pf: Case <5> and def of $\overline{w}$.

<6>2. QED

Pf: <6>1, <4>2, and <4>1.

<5>2. Case $\neg$(Enabled L)$'$

<6>1. $\|h\| = 0$

Pf: I^h.3 and Case <3>.

<6>2. $h'[0] = v'$

Pf: <6>1, L [Case <3>], hypothesis 1(a), $h' = G^h$, and def of G^h.

<6>3. $\overline{w}' = v'$

Pf: <6>2, Case <5>, and def of $\overline{w}$.

<6>4. $\|p'\| = 0$

Pf: $I^{p'}$.1, $I^{p'}$.2, and $\neg$(Enabled L)$'$ [case <5>].

<6>5. $p'[\,\|p'\|\,] = v'$

Pf: $I^{p'}$.2 and <6>4.

<6>6. QED

Pf: <6>3, <6>5, <4>2, and <4>1.

<5>3. QED

Pf: <5>1 - <5>2.

<4>4. QED

Pf: <4>3, since $\overline{w}' = \overline{w} \Rightarrow \overline{f' = f}$ by hypothesis 0.

<3>4. Case $[N]_f \wedge \neg S$

<4>1. Case $\neg$(Enabled L)

<5>1. $\neg$(Enabled L)$'$

Pf: Hypothesis 1(b) and Case <4>

<5>2. $\overline{w} = h[0] \wedge \overline{w}' = h'[0]$.

Pf: <5>1, Case <4>, and def of $\overline{w}$.

<5>3. QED

<6>1. Case $\|h\| = 0$

<7>1. $\|h'\| = 0 \wedge h'[0] = v'$

Pf: Case <6>, $\neg S$ [Case <3>], $h' = G^h$, and def of G^h.

<7>2. $v = h[0]$

Pf: Case <6> and I^h.2.

<7>3. $\overline{w} = v \wedge \overline{w}' = v'$

Pf: <5>2, <7>1, and <7>2.

<7>4. $\overline{w}.[N \land \neg S]_f.\overline{w}'$

Pf: <7>3 and Case <3>.

<7>5. QED

Pf: <7>4, since $[N \land \neg S]_f \Rightarrow [N_r]_f$.

<6>2. Case $\| h \| > 0$

<7>1. $h[0].[M]_f.h'[0]$

Pf: $h' = G^h$, def of G^h, $\neg S$ [Case <3>] and Case <6>.

<7>2. $\overline{w}.[M]_f.\overline{w}'$

Pf: <7>1 and <5>2.

<7>3. QED

Pf: <7>2, since $[M]_f \Rightarrow [N_r]_f$.

<6>3. QED

Pf: <6>1 and <6>2.

<4>2. Case (Enabled L)

<5>1. (Enabled L)$'$

Pf: Hypothesis 1(c) and Case <4>.

<5>2. $\overline{w} = p[\| p \|] \land \overline{w}' = p'[\| p' \|]$

Pf: <5>1, Case <4>, and def of $\overline{w}$

<5>3. $p[\| p \|].[M]_f.p'[\| p' \|]$

Pf: $p = G^p$, def of G^p, $\neg S$ [Case <3>] and Enabled L [Case <4>].

<5>5. $\overline{w}.[M]_f.\overline{w}'$

Pf: <5>2 and <5>3.

<5>6. QED

Pf: <5>5, since $[M]_f \Rightarrow [N_r]_f$.

<4>3. QED

Pf: <4>1 and <4>2.

<3>5. QED

Pf: <3>1 - <3>-4

<2>3. QED

Pf: <2>1, <2>2, 1, 2, and simple TLA reasoning.

4. $\models \text{Init} \land \Box[N]_f \land H \land P \Rightarrow \Box \lor \overline{w} = v$
$\qquad\qquad\qquad\qquad\qquad\qquad \lor \overline{w}.R^+.v$
$\qquad\qquad\qquad\qquad\qquad\qquad \lor v.L^+.\overline{w})$

<2>1. $I^p \land (\text{Enabled } L) \Rightarrow v.L^+.\overline{w}$

Assume: $I^p \land (\text{Enabled } L)$

Prove: $v.L^+.\overline{w}$

<3>1. $\overline{w} = p[\| p \|]$

Pf: Def of $\overline{w}$ and Assumption <2>.

<3>2. $v = p[0]$

Pf: I^p.2.

<3>3. $p[0].L^+.p[\| p \|]$

Pf: I^p.1.

<3>4. QED

Pf: <3>1 - <3>3.

<2>2. $I^h \wedge \neg(\text{Enabled } L) \wedge \|h\| > 0 \Rightarrow \overline{w}.R^+.v$
Assume: $I^h \wedge \neg(\text{Enabled } L) \wedge \|h\| > 0$
Prove: $\overline{w}.R^+.v$
<3>1. $\overline{w} = h[0]$
Pf: Def of $\overline{w}$ and Assumption <2>.
<3>2. $v = h[\,\|h\|\,]$
Pf: $I^h.2$.
<3>3. $h[0].R^+.h[\,\|h\|\,]$
Pf: $I^h.1$ and assumption $\|h\| > 0$
<3>4. QED
Pf: <3>1 - <3>3.

<2>3. $I^h \wedge \neg(\text{Enabled } L) \wedge \|h\| = 0 \Rightarrow \overline{w} = v$
Assume: $I^h \wedge \neg(\text{Enabled } L) \wedge \|h\| = 0$
Prove: $\overline{w} = v$
<3>1. $\overline{w} = h[0]$
Pf: Def of $\overline{w}$ and Assumption <2>.
<3>2. $v = h[\,\|h\|\,]$
Pf: $I^h.2$.
<3>3. QED
Pf: <3>1, <3>2, and assumption $\|h\| = 0$.

<2>4. QED
Pf: <2>1 - <2>3, since $I^h \Rightarrow \|h\| \in \text{Nat}$.

5. $\models \text{Init} \wedge \Box[N]_f \wedge H \wedge P \Rightarrow$
$\exists\, w : \wedge\ \text{Init}(w/v) \wedge \Box[N_r(w/v, w'/v')]_{f(w/v)}$
$\wedge\ \Box(v = w \vee w.R^+.v \vee v.L^+.w)$
Pf: 4 and simple logic.

6. $\models \exists\, p : \exists\, h : \text{Init} \wedge \Box[N]_f \wedge H \wedge P \Rightarrow$
$\exists\, w : \wedge\ \text{Init}(w/v) \wedge \Box[N_r(w/v, w'/v')]_{f(w/v)}$
$\wedge\ \Box(v = w \vee w.R^+.v \vee v.L^+.w)$
Pf: 5 and simple logic.

7. $\models \text{Init} \wedge \Box[N]_f \wedge \Box\Diamond\neg(\text{Enabled } L) \Rightarrow$
$\exists\, w : \wedge\ \text{Init}(w/v) \wedge \Box[N_r(w/v, w'/v')]_{f(w/v)}$
$\wedge\ \Box(v = w \vee w.R^+.v \vee v.L^+.w)$
Pf: 7, 1, 2, and Theorems about history and prophecy variables.

8. QED
Pf: Immediate from 7, since
$w.R^+.v = v.(R^{-1})^+.w = (R^{-1})^+(w/v')$
$v.L^+.w = L^+(w/v')$

The following corollary asserts that the conjunct $\Box\Diamond\neg(\text{Enabled } L)$ isn't needed for proving safety properties, if L satisfies the extra hypothesis

3. From any state in which L is enabled, it's possible to perform a terminating execution of L--i.e., to reach a final state of L by taking L steps.

The precise statement is:

COROLLARY: With the hypotheses of the Reduction Theorem, assume that

3. $\mathrm{Init} \wedge \Box[N]_f \Rightarrow \Box(\mathrm{Enabled}\ (L^* \wedge \neg(\mathrm{Enabled}\ L)')$

and let Π be any safety property. If

$$\begin{array}{l} \models \exists\, w : \wedge\ \mathrm{Init}(w/v) \wedge \Box[N_r(w/v, w'/v')]_{f(w/v)} \\ \qquad\quad\ \wedge\ \Box((v = w) \vee L^+(w/v') \vee (R^{-1})^+(w/v')) \\ \quad \Rightarrow \Pi \end{array}$$

then

$$\models \mathrm{Init} \wedge \Box[N]_f \Rightarrow \Pi$$

Proof of Corollary: The corollary follows easily from:

LEMMA. If $\mathrm{Init} \wedge \Box[N]_f \Rightarrow \Box(\mathrm{Enabled}\ (N^* \wedge P'))$, then $(\mathrm{Init} \wedge \Box[N]_f,\ \Box\Diamond P)$ is machine closed.

3 WIN AND SIN

The relation between the actual and pretend variables in the Reduction Theorem can be stated in terms of the predicate transformers win (weakest invariant) and sin (strongest invariant). These predicate transformers can be defined in the following equivalent ways, where A is an action, f a state function, and P a predicate, and a predicate I is an invariant of an action N iff $N \wedge I \Rightarrow I'$ holds.

win:

* win(A, P) is the weakest invariant of A that implies P. (That is, win(A, P) is an invariant of A, and for any invariant I of A, if $I \Rightarrow P$ then $I \Rightarrow$ win(A, P).)
* $s[\![\mathrm{win}(A, P)]\!] = \forall\, t : s[\![A^*]\!]t \Rightarrow t[\![P]\!]$
* $\mathrm{win}(A, P) = \neg\mathrm{Enabled}\ (A^* \wedge \neg P')$

sin:

* sin(A, P) is the strongest invariant of A implied by P. (That is, sin(A, P) is an invariant of A and for any invariant I of A, if $P \Rightarrow I$ then sin(A, P) $\Rightarrow$ I.)
* $s[\![\mathrm{sin}(A, P)]\!] = \exists\, t : t[\![P]\!] \wedge t[\![A^*]\!]s$
* $\mathrm{sin}(A, P) = \mathrm{Enabled}\ ((A^{-1})^* \wedge P')$
* $\mathrm{sin}(A, P) = \neg\mathrm{win}(A^{-1}, \neg P)$

PROPOSITION: If the A is an action, v an n-tuple of variables that includes all free variables of A, and w an n-tuple of variables distinct from the ones in v, then

(a) $\mathrm{sin}(A \wedge (w' = w),\ v = w) = (w = v) \vee (A^{-1})^+(w/v')$

(b) $\mathrm{win}(A \wedge (w' = w),\ v = w) = (w = v) \vee A^+(w/v')$

Proof: Let

$$\mathtt{r.[[B]].t} \;\triangleq\; \mathtt{B(r/v,t/v')}$$

$$\mathtt{(r,s).[[B]].(t,u)} \;\triangleq\; \mathtt{B(r/v,s/w,t/v',u/w')}$$

Proof of (a):

$$
\begin{array}{l}
\mathtt{(v,w).sin(A} \wedge \mathtt{w'{=}w,\ v{=}w)} \\
\quad = \mathtt{(v,w).Enabled((A} \wedge \mathtt{w'{=}w)^{-1*}} \wedge \mathtt{v'{=}w)} \\
\quad = \mathtt{(v,w).(}\exists\ \mathtt{(u,r) : [[(A} \wedge \mathtt{w'{=}w)^{-1*}} \wedge \mathtt{v'{=}w]].(u,r)} \\
\quad = \exists\ \mathtt{(u,r) : (v,w).[[(A} \wedge \mathtt{w'{=}w)^{-1*}} \wedge \mathtt{v'{=}w]].(u,r)} \\
\quad = \exists\ \mathtt{(u,r) :} \wedge \mathtt{(v,w).[[(A} \wedge \mathtt{w'{=}w)^{-1*}]].(u,r)} \\
\qquad\qquad\qquad \wedge \mathtt{(v,w).[[v'{=}w]].(u,r)} \\
\quad = \exists\ \mathtt{(u,r) : (v,w).[[(A} \wedge \mathtt{w'{=}w)^{-1*}]].(u,r)} \wedge \mathtt{u = w} \\
\quad = \exists\ \mathtt{r : (v,w).[[(A} \wedge \mathtt{w'{=}w)^{-1*}]].(w,r)} \\
\quad = \exists\ \mathtt{r : (w,r).[[(A} \wedge \mathtt{w'{=}w)^{*}]].(v,w)} \\
\quad = \exists\ \mathtt{r :} \vee \mathtt{(w,r).[[(v,w)'{=}(v,w)]].(v,w)} \\
\qquad\qquad \vee \mathtt{(w,r).[[(A} \wedge \mathtt{w'{=}w)^{+}]].(v,w)} \\
\qquad\quad \mathtt{[def\ of\ A^{*}]} \\
\quad = \exists\ \mathtt{r : (w = v} \wedge \mathtt{r = w)} \vee \mathtt{(w,r).[[A^{+}} \wedge \mathtt{(w'{=}w)^{+}]].(v,w)} \\
\qquad\quad \mathtt{[w\ not\ free\ in\ A} \Rightarrow \mathtt{(A} \wedge \mathtt{(w'{=}w))^{+} = A^{+}} \wedge \mathtt{(w'{=}w)^{+}]} \\
\quad = \exists\ \mathtt{r :} \vee \mathtt{w = v} \wedge \mathtt{r = w} \\
\qquad\qquad \vee \mathtt{(w,r).[[A^{+}]](v,w)} \wedge \mathtt{(w,r).[[(w'{=}w)^{+}]].(v,w)} \\
\quad = \exists\ \mathtt{r :} \vee \mathtt{w = v} \wedge \mathtt{r = w} \\
\qquad\qquad \vee \mathtt{w.[[A^{+}]].v} \wedge \mathtt{r = w} \\
\quad = \mathtt{(w = v)} \vee \mathtt{w.[[A^{+}]].v} \\
\quad = \mathtt{(w = v)} \vee \mathtt{v.[[(A^{-1})^{+}]].w} \\
\quad = \mathtt{(w = v)} \vee \mathtt{(A^{-1})^{+}(w/v')}
\end{array}
$$

Proof of (b) is analogous.

It follows from the proposition that the conclusion of the Reduction Theorem can be written as:

$$
\begin{array}{l}
\models \mathtt{Init} \wedge \Box\mathtt{[N]_{f}} \wedge \Box\Diamond\neg\mathtt{(Enabled\ L)} \Rightarrow \\
\qquad \exists\ \mathtt{w :} \wedge \mathtt{Init(w/v)} \wedge \Box\mathtt{[N_{r}(w/v,w'/v')]_{f(w/v)}} \\
\qquad\qquad \wedge \Box \vee \mathtt{sin(R} \wedge \mathtt{(w' = w),\ v = w)} \\
\qquad\qquad\qquad \vee \mathtt{win(L} \wedge \mathtt{(w' = w),\ v = w)}
\end{array}
$$