A Definitional Encoding of TLA in Isabelle/HOL

Gudmund Grov & Stephan Merz

September 19, 2015

Abstract

We mechanise the logic TLA* [8], an extension of Lamport’s Temporal Logic of Actions (TLA) [5] for specifying and reasoning about concurrent and reactive systems. Aiming at a framework for mechanising the verification of TLA (or TLA*) specifications, this contribution reuses some elements from a previous axiomatic encoding of TLA in Isabelle/HOL by the second author [7], which has been part of the Isabelle distribution. In contrast to that previous work, we give here a shallow, definitional embedding, with the following highlights:

- a theory of infinite sequences, including a formalisation of the concepts of stuttering invariance central to TLA and TLA*;
- a definition of the semantics of TLA*, which extends TLA by a mutually-recursive definition of formulas and pre-formulas, generalising TLA action formulas;
- a substantial set of derived proof rules, including the TLA* axioms and Lamport’s proof rules for system verification;
- a set of examples illustrating the usage of Isabelle/TLA* for reasoning about systems.

Note that this work is unrelated to the ongoing development of a proof system for the specification language TLA+, which includes an encoding of TLA+ as a new Isabelle object logic [1].

A previous version of this embedding has been used heavily in the work described in [4].

Contents

1 (Infinite) Sequences 3
1.1 Some operators on sequences . . . . . . . . . . . . . . . 3
1.1.1 Properties of first and second . . . . . . . . . . . . . . 4
1.1.2 Properties of op | . . . . . . . . . . . . . . . . . . . . . . . 4
1.1.3 Properties of op ## . . . . . . . . . . . . . . . . . . . . . . 4
1.2 Finite and Empty Sequences . . . . . . . . . . . . . . . . . 5
1.2.1 Properties of emptyseq . . . . . . . . . . . . . . . . . . 5
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.2</td>
<td>Properties of <code>Sequence.last</code> and <code>laststate</code></td>
<td>6</td>
</tr>
<tr>
<td>1.3</td>
<td>Stuttering Invariance</td>
<td>6</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Properties of <code>nonstutseq</code></td>
<td>7</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Properties of <code>nextnat</code></td>
<td>7</td>
</tr>
<tr>
<td>1.3.3</td>
<td>Properties of <code>nextsuffix</code></td>
<td>8</td>
</tr>
<tr>
<td>1.3.4</td>
<td>Properties of <code>next</code></td>
<td>8</td>
</tr>
<tr>
<td>1.3.5</td>
<td>Properties of <code>∷</code></td>
<td>9</td>
</tr>
<tr>
<td>1.4</td>
<td>Similarity of Sequences</td>
<td>9</td>
</tr>
<tr>
<td>1.4.1</td>
<td>Properties of <code>op ≈</code></td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>Representing Intensional Logic</td>
<td>11</td>
</tr>
<tr>
<td>2.1</td>
<td>Abstract Syntax</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Concrete Syntax</td>
<td>13</td>
</tr>
<tr>
<td>2.3</td>
<td>Definitions</td>
<td>16</td>
</tr>
<tr>
<td>2.4</td>
<td>Lemmas and Tactics</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Semantics</td>
<td>18</td>
</tr>
<tr>
<td>3.1</td>
<td>Types of Formulas</td>
<td>18</td>
</tr>
<tr>
<td>3.2</td>
<td>Semantics of TLA*</td>
<td>19</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Concrete Syntax</td>
<td>19</td>
</tr>
<tr>
<td>3.3</td>
<td>Abbreviations</td>
<td>20</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Concrete Syntax</td>
<td>20</td>
</tr>
<tr>
<td>3.4</td>
<td>Properties of Operators</td>
<td>21</td>
</tr>
<tr>
<td>3.5</td>
<td>Invariance Under Stuttering</td>
<td>21</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Properties of <code>-stutinv</code></td>
<td>22</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Properties of <code>-nstutinv</code></td>
<td>23</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Abbreviations</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>Reasoning about PreFormulas</td>
<td>25</td>
</tr>
<tr>
<td>4.1</td>
<td>Lemmas about <code>Unchanged</code></td>
<td>27</td>
</tr>
<tr>
<td>4.2</td>
<td>Lemmas about <code>after</code></td>
<td>27</td>
</tr>
<tr>
<td>4.3</td>
<td>Lemmas about <code>before</code></td>
<td>28</td>
</tr>
<tr>
<td>4.4</td>
<td>Some general properties</td>
<td>28</td>
</tr>
<tr>
<td>4.5</td>
<td>Unlifting attributes and methods</td>
<td>29</td>
</tr>
<tr>
<td>5</td>
<td>A Proof System for TLA*</td>
<td>29</td>
</tr>
<tr>
<td>5.1</td>
<td>The Basic Axioms</td>
<td>29</td>
</tr>
<tr>
<td>5.2</td>
<td>Derived Theorems</td>
<td>31</td>
</tr>
<tr>
<td>5.3</td>
<td>Some other useful derived theorems</td>
<td>33</td>
</tr>
<tr>
<td>5.4</td>
<td>Theorems about the eventually operator</td>
<td>36</td>
</tr>
<tr>
<td>5.5</td>
<td>Theorems about the leadsto operator</td>
<td>39</td>
</tr>
<tr>
<td>5.6</td>
<td>Lemmas about the next operator</td>
<td>43</td>
</tr>
<tr>
<td>5.7</td>
<td>Higher Level Derived Rules</td>
<td>44</td>
</tr>
</tbody>
</table>
theory Sequence
imports Main
begin

Lamport’s Temporal Logic of Actions (TLA) is a linear-time temporal logic, and its semantics is defined over infinite sequence of states, which we simply represent by the type 'a seq, defined as an abbreviation for the type nat ⇒ 'a, where 'a is the type of sequence elements.

This theory defines some useful notions about such sequences, and in particular concepts related to stuttering (finite repetitions of states), which are important for the semantics of TLA. We identify a finite sequence with an infinite sequence that ends in infinite stuttering. In this way, we avoid the complications of having to handle both finite and infinite sequences of states: see e.g. Devillers et al [2] who discuss several variants of representing possibly infinite sequences in HOL, Isabelle and PVS.

type-synonym 'a seq = nat ⇒ 'a

1.1 Some operators on sequences

Some general functions on sequences are provided

definition first :: 'a seq ⇒ 'a
where first s ≡ s 0

definition second :: ('a seq) ⇒ 'a
where second s ≡ s 1
definition suffix :: 'a seq ⇒ nat ⇒ 'a seq (infixl \mid\ 60)
where s \mid i ≡ \lambda n. s (n+i)

definition tail :: 'a seq ⇒ 'a seq
where tail s ≡ s \mid 1

definition app :: 'a ⇒ ('a seq) ⇒ ('a) (infixl \#\# 60)
where s \#\# \sigma ≡ \lambda n. if n=0 then s else \sigma (n - 1)

s \mid i returns the suffix of sequence s from index i. first returns the first
element of a sequence while second returns the second element. tail returns
the sequence starting at the second element. s \#\# \sigma prefixes the sequence
\sigma by element s.

1.1.1 Properties of first and second

lemma first-tail-second: first (tail s) = second s
⟨proof⟩

1.1.2 Properties of op \mid

lemma suffix-first: first (s \mid n) = s n
⟨proof⟩

lemma suffix-second: second (s \mid n) = s (Suc n)
⟨proof⟩

lemma suffix-plus: s \mid n \mid m = s \mid (m + n)
⟨proof⟩

lemma suffix-commute: ((s \mid n) \mid m) = ((s \mid m) \mid n)
⟨proof⟩

lemma suffix-plus-com: s \mid m \mid n = s \mid (m + n)
⟨proof⟩

lemma suffix-zero[simp]: s \mid 0 = s
⟨proof⟩

lemma suffix-tail: s \mid 1 = tail s
⟨proof⟩

lemma tail-suffix-suc: s \mid (Suc n) = tail (s \mid n)
⟨proof⟩

1.1.3 Properties of op \#\#

lemma seq-app-second: (s \#\# \sigma) 1 = \sigma 0
lemma seq-app-first: \( (s \#\# \sigma) \ 0 = s \)

lemma seq-app-first-tail: \( \text{first} \ s \#\# \text{tail} \ s = s \)

lemma seq-app-tail: \( \text{tail} \ (x \#\# s) = s \)

lemma seq-app-greater-than-zero: \( n > 0 \implies (s \#\# \sigma) \ n = \sigma \ (n - 1) \)

### 1.2 Finite and Empty Sequences

We identify finite and empty sequences and prove lemmas about them.

**Definition** fin :: ('a seq) ⇒ bool
where fin s ≡ ∃ i. ∀ j ≥ i. s j = s i

**Abbreviation** inf :: ('a seq) ⇒ bool
where inf s ≡ ¬(fin s)

**Definition** last :: ('a seq) ⇒ nat
where last s ≡ LEAST i. (∀ j ≥ i. s j = s i)

**Definition** laststate :: ('a seq) ⇒ 'a
where laststate s ≡ s (last s)

**Definition** emptyseq :: ('a seq) ⇒ bool
where emptyseq ≡ λ s. ∀ i. s i = s 0

**Abbreviation** notemptyseq :: ('a seq) ⇒ bool
where notemptyseq s ≡ ¬(emptyseq s)

Predicate fin holds if there is an element in the sequence such that all subsequent elements are identical, i.e. the sequence is finite. Sequence.last s returns the smallest index from which on all elements of a finite sequence s are identical. Note that if s is not finite then an arbitrary number is returned. laststate returns the last element of a finite sequence. We assume that the sequence is finite when using Sequence.last and laststate. Predicate emptyseq identifies empty sequences – i.e. all states in the sequence are identical to the initial one, while notemptyseq holds if the given sequence is not empty.

#### 1.2.1 Properties of emptyseq

**Lemma** empty-is-finite: assumes emptyseq s shows fin s
lemma empty-suffix-is-empty: assumes H: emptyseq s shows emptyseq (s |ₙ n)
⟨proof⟩

lemma suc-empty: assumes H1: emptyseq (s |ₙ m) shows emptyseq (s |ₙ (Suc m))
⟨proof⟩

lemma empty-suffix-exteq: assumes H: emptyseq s shows (s |ₙ s n) m = s m
⟨proof⟩

lemma empty-suffix-eq: assumes H: emptyseq s shows (s |ₙ s n) = s
⟨proof⟩

lemma seq-empty-all: assumes H: emptyseq s shows s i = s j
⟨proof⟩

1.2.2 Properties of Sequence.last and laststate

lemma fin-stut-after-last: assumes H: fin s shows ∀ j ≥ last s. s j = s (last s)
⟨proof⟩

1.3 Stuttering Invariance

This subsection provides functions for removing stuttering steps of sequences, i.e. we formalise Lamport’s ♦ operator. Our formal definition is close to that of Wahab in the PVS prover.

The key novelty with the Sequence theory, is the treatment of stuttering invariance, which enables verification of stuttering invariance of the operators derived using it. Such proofs require comparing sequences up to stuttering. Here, Lamport’s [5] method is used to mechanise the equality of sequences up to stuttering: he defines the ♦ operator, which collapses a sequence by removing all stuttering steps, except possibly infinite stuttering at the end of the sequence. These are left unchanged.

definition nonstutseq :: ('a seq) ⇒ bool
where nonstutseq s ≡ ∀ i. s i = s (Suc i) −→ (∀ j > i. s i = s j)

definition stutstep :: ('a seq) ⇒ nat ⇒ bool
where stutstep s n ≡ (s n = s (Suc n))

definition nextnat :: ('a seq) ⇒ nat
where nextnat s ≡ if emptyseq s then 0 else LEAST i. s i ≠ s 0

definition nextsuffix :: ('a seq) ⇒ ('a seq)
where nextsuffix s ≡ s |ₙ (nextnat s)

fun next :: nat ⇒ ('a seq) ⇒ ('a seq) where
next 0 = id
| next (Suc n) = nextsuffix o (next n)

definition collapse :: ('a seq) ⇒ ('a seq) (\)
where \ s ≡ λ n. (next n s) \n
Predicate nonstutseq identifies sequences without any stuttering steps – except possibly for infinite stuttering at the end. Further, stutstep s n is a predicate which holds if the element after s n is equal to s n, i.e. Suc n is a stuttering step. \ s formalises Lamports \ operator. It returns the first state of the result of next n s. next n s finds suffix of the n\textsuperscript{th} change. Hence the first element, which \ s returns, is the state after the n\textsuperscript{th} change. next n s is defined by primitive recursion on n using function composition of function nextsuffix. E.g. next 3 s equals nextsuffix (nextsuffix (nextsuffix s)). nextsuffix s returns the suffix of the sequence starting at the next changing state. It uses nextnat to obtain this. All the real computation is done in this function. Firstly, an empty sequence will obviously not contain any changes, and \ is therefore returned. In this case nextsuffix behaves like the identity function. If the sequence is not empty then the smallest number i such that s i is different from the initial state is returned. This is achieved by Least.

1.3.1 Properties of nonstutseq

lemma seq-empty-is-nonstut:
  assumes H: emptyseq s shows nonstutseq s
  ⟨proof⟩

lemma notempty-exist-nonstut:
  assumes H: ¬ emptyseq (s | s m) shows ∃ i. s i ≠ s m ∧ i > m
  ⟨proof⟩

1.3.2 Properties of nextnat

lemma nextnat-le-unch:
  assumes H: n < nextnat s shows s n = s \n
  ⟨proof⟩

lemma stutnempty:
  assumes H: ¬ stutstep s n shows ¬ emptyseq (s | s n)
  ⟨proof⟩

lemma notstutstep-nexnat1:
  assumes H: ¬ stutstep s n shows nextnat (s | s n) = 1

  ⟨proof⟩

lemma stutstep-notempty-notempty:
  assumes h1: emptyseq (s | s Suc n) (is emptyseq ?sn)
  and h2: stutstep s n
  shows emptyseq (s | s n) (is emptyseq ?s)
lemma proof
lemma stutstep-empty-suc:
  assumes stutstep s n
  shows emptyseq (s \langle s, Suc n \rangle) = emptyseq (s \langle s, n \rangle)

lemma proof
lemma stutstep-notempty-sucnextnat:
  assumes h1: \neg emptyseq (s \langle s, n \rangle) and h2: stutstep s n
  shows (nextnat (s \langle s, n \rangle)) = Suc (nextnat (s \langle s, (Suc n) \rangle))

lemma proof
lemma nextnat-empty-neq: assumes H: \neg emptyseq s shows s (nextnat s) \neq s 0

lemma proof
lemma nextnat-empty-gzero: assumes H: \neg emptyseq s shows nextnat s > 0

1.3.3 Properties of nextsuffix

lemma empty-nextsuffix:
  assumes H: emptyseq s shows nextsuffix s = s
  ⟨proof⟩

lemma empty-nextsuffix-id:
  assumes H: emptyseq s shows nextsuffix s = id s
  ⟨proof⟩

lemma notstutstep-nextsuffix1:
  assumes H: \neg stutstep s n shows nextsuffix (s \langle s, n \rangle) = s \langle s, (Suc n) \rangle
  ⟨proof⟩

1.3.4 Properties of next

lemma next-suc-suffix: next (Suc n) s = nextsuffix (next n s)
  ⟨proof⟩

lemma next-suffix-com: nextsuffix (next n s) = (next n (nextsuffix s))
  ⟨proof⟩

lemma next-plus: next (m+n) s = next m (next n s)
  ⟨proof⟩

lemma next-empty: assumes H: emptyseq s shows next n s = s
  ⟨proof⟩

lemma notempty-nextnotzero:
  assumes H: \neg emptyseq s shows (next (Suc 0) s) 0 \neq s 0
  ⟨proof⟩
lemma next-ex-id: \exists \ i. \ s \ i = (next m s) 0
(proof)

1.3.5 Properties of \( \natural \)

lemma emptyseq-collapse-eq: assumes A1: emptyseq s shows \( \natural \) s = s
(proof)

lemma empty-collapse-empty:
  assumes H: emptyseq s shows emptyseq (\( \natural \) s)
(proof)

lemma collapse-empty-empty:
  assumes H: emptyseq (\( \natural \) s) shows emptyseq s
(proof)

lemma collapse-empty-iff-empty [simp]: emptyseq (\( \natural \) s) = emptyseq s
(proof)

1.4 Similarity of Sequences

Since adding or removing stuttering steps does not change the validity of a stuttering-invariant formula, equality is often too strong, and the weaker equality up to stuttering is sufficient. This is often called similarity \( (\approx) \) of sequences in the literature, and is required to show that logical operators are stuttering invariant. This is mechanised as:

definition seqsimilar :: (\'a seq) \Rightarrow (\'a seq) \Rightarrow bool (infixl \approx 50)
where \( \sigma \approx \tau \equiv (\natural \sigma) = (\natural \tau) \)

1.4.1 Properties of op \( \approx \)

lemma seqsim-refl [iff]: s \approx s
(proof)

lemma seqsim-sym: assumes H: s \approx t shows t \approx s
(proof)

lemma seqeq-imp-sim: assumes H: s = t shows s \approx t
(proof)

lemma seqsim-trans [trans]: assumes h1: s \approx t and h2: t \approx z shows s \approx z
(proof)

theorem sim-first: assumes H: s \approx t shows first s = first t
(proof)

lemmas sim-first2 = sim-first[unfolded first-def]

lemma tail-sim-second: assumes H: tail s \approx tail t shows second s = second t
\begin{proof}
\textbf{lemma seqsimilarI:}
\begin{itemize}
\item \textbf{assumes} 1: \textit{first} \textit{s} = \textit{first} \textit{t} \textbf{and} 2: \textit{nextsuffix} \textit{s} \approx \textit{nextsuffix} \textit{t}
\item \textbf{shows} \textit{s} \approx \textit{t}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seqsim-empty-empty:}
\begin{itemize}
\item \textbf{assumes} \textit{H1}: \textit{s} \approx \textit{t} \textbf{and} \textit{H2}: \textit{emptyseq} \textit{s} \textbf{shows} \textit{emptyseq} \textit{t}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seqsim-empty-iff-empty:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \textit{s} \approx \textit{t} \textbf{shows} \textit{emptyseq} \textit{t} = \textit{emptyseq} \textit{s}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seq-empty-eq:}
\begin{itemize}
\item \textbf{assumes} \textit{H1}: \textit{s} 0 = \textit{t} 0 \textbf{and} \textit{H2}: \textit{emptyseq} \textit{s} \textbf{and} \textit{H3}: \textit{emptyseq} \textit{t}
\item \textbf{shows} \textit{s} = \textit{t}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seqsim-natstutstep:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \neg (\textit{stutstep} \textit{s} \textit{n}) \textbf{shows} \textit{s} |_{\textit{s}} (\textit{Suc} \textit{n}) \approx \textit{nextsuffix} \textit{s} |_{\textit{s}} \textit{n}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma stat-success-suc:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \textit{stutstep} \textit{s} \textit{n} \textbf{shows} \textit{nextsuffix} \textit{s} |_{\textit{s}} \textit{n} = \textit{nextsuffix} \textit{s} |_{\textit{s}} (\textit{Suc} \textit{n})
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seqsim-suffix-seqsim:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \textit{s} \approx \textit{t} \textbf{shows} \textit{nextsuffix} \textit{s} \approx \textit{nextsuffix} \textit{t}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma seqsim-stutstep:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \textit{stutstep} \textit{s} \textit{n} \textbf{shows} \textit{s} |_{\textit{s}} (\textit{Suc} \textit{n}) \approx \textit{nextsuffix} \textit{s} |_{\textit{s}} \textit{n} \textbf{is} \textit{?sn} \approx \textit{?s}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma addfirststut:} \textit{stutstep} (\textit{(first} \textit{t}) \# \textit{t}) 0
\end{proof}

\begin{proof}
\textbf{lemma addfirststut:} (\textit{(first} \textit{t}) \# \textit{t}) \approx \textit{t}
\end{proof}

\begin{proof}
\textbf{lemma addfirststat:}
\begin{itemize}
\item \textbf{assumes} \textit{H}: \textit{first} \textit{s} = \textit{second} \textit{s} \textbf{shows} \textit{s} \approx \textit{tail} \textit{s}
\end{itemize}
\end{proof}

\begin{proof}
\textbf{lemma app-seqsimilar:}
\begin{itemize}
\item \textbf{assumes} \textit{h1}: \textit{s} \approx \textit{t} \textbf{shows} \textit{x} \# \textit{t} \approx \textit{x} \# \textit{t}
\end{itemize}
\end{proof}
If two sequences are similar then for any suffix of one of them there exists a similar suffix of the other one. We will prove a stronger result below.

**lemma simstep-disj1**: assumes \( H : s \approx t \) shows \( \exists \, m. \, ((s \upharpoonright m) \approx (t \upharpoonright m)) \)

**lemma nextnat-le-seqsim**: assumes \( n: n < \text{nextnat} \, s \) shows \( s \approx (s \upharpoonright n) \)

**lemma seqsim-prev-nextnat**: \( s \approx (s \upharpoonright (\text{nextnat} \, s - 1)) \)

The following main result about similar sequences shows that if \( s \approx t \) holds then for any suffix \( s \upharpoonright n \) of \( s \) there exists a suffix \( t \upharpoonright m \) such that

- \( s \upharpoonright n \) and \( t \upharpoonright m \) are similar, and
- \( s \upharpoonright (n+1) \) is similar to either \( t \upharpoonright (m+1) \) or \( t \upharpoonright m \).

**theorem sim-step**: assumes \( H : s \approx t \) shows \( \exists \, m. \, (s \upharpoonright n \approx t \upharpoonright m) \land ((s \upharpoonright \text{Suc} \, n \approx t \upharpoonright \text{Suc} \, m) \lor (s \upharpoonright \text{Suc} \, n \approx t \upharpoonright m)) \)

The idea is to pick the largest \( m \) such that \( s \upharpoonright n \approx t \upharpoonright m \) (or some such \( m \) if \( s \upharpoonright n \) is empty).

**2 Representing Intensional Logic**

**theory Intensional**

**imports** Main

**begin**

In higher-order logic, every proof rule has a corresponding tautology, i.e. the deduction theorem holds. Isabelle/HOL implements this since object-level implication (\( \rightarrow \)) and meta-level entailment (\( \Rightarrow \)) commute, viz. the
proof rule \textit{impI}: $(P \implies Q) \implies P \implies Q$. However, the deduction theorem does not hold for most modal and temporal logics [6, page 95][7]. For example $A \vdash \Box A$ holds, meaning that if $A$ holds in any world, then it always holds. However, $\vdash A \rightarrow \Box A$, stating that $A$ always holds if it initially holds, is not valid.

Merz [7] overcame this problem by creating an Intensional logic. It exploits Isabelle’s axiomatic type class feature [9] by creating a type class \textit{world}, which provides Skolem constants to associate formulas with the world they hold in. The class is trivial, not requiring any axioms.

class \textit{world}

\textit{world} is a type class of possible worlds. It is a subclass of all HOL types \textit{type}. No axioms are provided, since its only purpose is to avoid silly use of the Intensional syntax.

2.1 Abstract Syntax

type-synonym $(\, w, a \,) \ expr = w \Rightarrow a$
type-synonym $w \ form = (w, \text{bool}) \ expr$

The intention is that $a$ will be used for unlifted types (class \textit{type}), while $w$ is lifted (class \textit{world}).

consts
  \begin{align*}
  \text{Valid} & :: \ (w::world) \ form \Rightarrow \text{bool} \\
  \text{const} & :: a \Rightarrow (w::world, a) \ expr \\
  \text{lift} & :: [a \Rightarrow b, (w::world, a) \ expr] \Rightarrow (w,b) \ expr \\
  \text{lift2} & :: [a \Rightarrow b \Rightarrow c, (w::world,a) \ expr, (w,b) \ expr] \Rightarrow (w,c) \ expr \\
  \text{lift3} & :: [a \Rightarrow b \Rightarrow c \Rightarrow d, (w::world,a) \ expr, (w,b) \ expr, (w,c) \ expr] \Rightarrow (w,d) \ expr \\
  \text{lift4} & :: [a \Rightarrow b \Rightarrow c \Rightarrow d \Rightarrow e, (w::world,a) \ expr, (w,b) \ expr, (w,c) \ expr, (w,d) \ expr] \Rightarrow (w,e) \ expr
  \end{align*}

\text{Valid} F asserts that the lifted formula $F$ holds everywhere. \text{const} allows lifting of a constant, while \text{lift} through \text{lift4} allow functions with arity 1–4 to be lifted. (Note that there is no way to define a generic lifting operator for functions of arbitrary arity.)

consts
  \begin{align*}
  \text{RAll} & :: (a \Rightarrow (w::world) \ form) \Rightarrow w \ form \quad \text{(binder Rall \ 10)} \\
  \text{REx} & :: (a \Rightarrow (w::world) \ form) \Rightarrow w \ form \quad \text{(binder Rex \ 10)} \\
  \text{REx1} & :: (a \Rightarrow (w::world) \ form) \Rightarrow w \ form \quad \text{(binder Rex! \ 10)}
  \end{align*}

\text{RAll}, \text{REx} and \text{REx1} introduces “rigid” quantification over values (of non-world types) within “intensional” formulas. \text{RAll} is universal quantification, \text{REx} is existential quantification. \text{REx1} requires unique existence.
2.2 Concrete Syntax

The non-terminal `lift` represents lifted expressions. The idea is to use Isabelle’s macro mechanism to convert between the concrete and abstract syntax.

```
syntax
  :: id ⇒ lift (-)
  :: longid ⇒ lift (-)
  :: var ⇒ lift (-)

-applC :: [lift, cargs] ⇒ lift ((1/-) [1000, 1000] 999)
  :: lift ⇒ lift ('-')

-lambda :: [idts, 'a] ⇒ lift ((%/- ) [0, 3] 3)

-constrain :: [lift, type] ⇒ lift ((::-) [4, 0] 3)

  :: lift ⇒ liftargs (-)

-liftargs :: [lift, liftargs] ⇒ liftargs (-/-)

-Valid :: lift ⇒ bool ((|- |-) 5)

-holdsAt :: ['a, lift] ⇒ bool ((| - |=) [100,10] 10)

LIFT :: lift ⇒ 'a (LIFT -)
```

```
-const :: 'a ⇒ lift ((#) [1000] 999)

-lift :: ['a, lift] ⇒ lift ((<-> ) [1000] 999)

-lift2 :: ['a, lift, lift] ⇒ lift ((<-/- />) [1000] 999)

-lift3 :: ['a, lift, lift, lift] ⇒ lift ((<-/- /> ->) [1000] 999)

-lift4 :: ['a, lift, lift, lift, lift] ⇒ lift ((<-/- /-/-/ ->) [1000] 999)
```

```
-liftEqu :: [lift, lift] ⇒ lift ((=/ ) [50,51] 50)

-liftNeq :: [lift, lift] ⇒ lift ((=/ ) [50,51] 50)

-liftNot :: lift ⇒ lift ("-" [90] 90)

-liftAnd :: [lift, lift] ⇒ lift ("&" [36,35] 35)

-liftOr :: [lift, lift] ⇒ lift ("|" [31,30] 30)


-liftIf :: [lift, lift, lift] ⇒ lift ((if ()/ then ()/ else ())/) 10)

-liftPlus :: [lift, lift] ⇒ lift ((/+ ) [66,65] 65)

-liftMinus :: [lift, lift] ⇒ lift ((/- ) [66,65] 65)

-liftTimes :: [lift, lift] ⇒ lift ((*/ ) [71,70] 70)

-liftDiv :: [lift, lift] ⇒ lift ((/- ) [71,70] 70)

-liftMod :: [lift, lift] ⇒ lift ((mod ) [71,70] 70)

-liftLess :: [lift, lift] ⇒ lift ((/- < ) [50,51] 50)

-liftLeq :: [lift, lift] ⇒ lift ((/- <= ) [50,51] 50)

-liftMem :: [lift, lift] ⇒ lift ((/- ) [50,51] 50)

-liftNeg :: [lift, lift] ⇒ lift ((/- ) [50,51] 50)

-liftFinset :: liftargs ⇒ lift (({-}) )
```
-liftPair :: [lift, liftargs] ⇒ lift
   ((1’/ - ’))

-liftCons :: [lift, lift] ⇒ lift
   ((#/) [65,66] 65)

-liftApp :: [lift, lift] ⇒ lift
   ((@/) [65,66] 65)

-liftList :: liftargs ⇒ lift
   ([[]])

-ARAll :: [idts, lift] ⇒ lift
   ((3! -/) [0, 10] 10)

-AREx :: [idts, lift] ⇒ lift
   ((3? -/) [0, 10] 10)

-AREx1 :: [idts, lift] ⇒ lift
   ((3? ! -/) [0, 10] 10)

-RAAll :: [idts, lift] ⇒ lift
   ((3ALL -/) [0, 10] 10)

-REx :: [idts, lift] ⇒ lift
   ((3EX -/) [0, 10] 10)

-REx1 :: [idts, lift] ⇒ lift
   ((3EX! -/) [0, 10] 10)

translations
-const ⇏ CONST const

translations
-lift ⇏ CONST lift
-lift2 ⇏ CONST lift2
-lift3 ⇏ CONST lift3
-lift4 ⇏ CONST lift4
-Valid ⇏ CONST Valid

translations
-RAll x A ⇏ Rall x. A
-REx x A ⇏ Rex x. A
-REx1 x A ⇏ Rex! x. A

translations
-ARAll → -RAAll
-AREx → -REx
-AREx1 → -REx1

w | A ⇒ A w
LIFT A ⇒ A::⇒ -

translations
-liftEqu ⇏ lift2 (op =)
-liftNeq u v ⇏ liftNot (-liftEqu u v)
-liftNot ⇏ lift (CONST Not)
-liftAnd ⇏ lift2 (op &)
-liftOr ⇏ lift2 (op | )
-liftImp ⇏ lift2 (op −−>)
-liftIf ⇏ lift3 (CONST If)
-liftPlus ⇏ lift2 (op +)
-liftMinus ⇏ lift2 (op −)
-liftTimes ⇏ lift2 (op *)
\begin{align*}
\text{-liftDiv} & \iff \text{-lift2 (op div)} \\
\text{-liftMod} & \iff \text{-lift2 (op mod)} \\
\text{-liftLess} & \iff \text{-lift2 (op <)} \\
\text{-liftLeq} & \iff \text{-lift2 (op <=)} \\
\text{-liftMem} & \iff \text{-lift2 (op :)} \\
\text{-liftNotMem x xs} & \iff \text{-liftNot (-liftMem x xs)}
\end{align*}

\textbf{translations}
\begin{align*}
\text{-liftFinset (-liftargs x xs)} & \iff \text{-lift2 (CONST insert) x (-liftFinset xs)} \\
\text{-liftFinset x} & \iff \text{-lift2 (CONST insert) x (-const (CONST Set.empty))} \\
\text{-liftPair x (-liftargs y z)} & \iff \text{-liftPair x (-liftPair y z)} \\
\text{-liftPair} & \iff \text{-lift2 (CONST Pair)} \\
\text{-liftCons} & \iff \text{-lift2 (CONST Cons)} \\
\text{-liftApp} & \iff \text{-lift2 (op @)} \\
\text{-liftList (-liftargs x xs)} & \iff \text{-liftCons x (-liftList xs)} \\
\text{-liftList x} & \iff \text{-liftCons x (-const [])}
\end{align*}

\begin{align*}
\text{w} & \iff \sim A \iff \text{-liftNot A w} \\
\text{w} & \iff A \land B \iff \text{-liftAnd A B w} \\
\text{w} & \iff A \lor B \iff \text{-liftOr A B w} \\
\text{w} & \iff A \implies B \iff \text{-liftImp A B w} \\
\text{w} & \iff u = v \iff \text{-liftEq u v w} \\
\text{w} & \iff \text{ALL} \ x. A \iff \text{-RAll x A w} \\
\text{w} & \iff \text{EX} \ x. A \iff \text{-REx x A w} \\
\text{w} & \iff \text{EX!} \ x. A \iff \text{-REx1 x A w}
\end{align*}

\textbf{syntax (xsymbols)}
\begin{align*}
\text{-Valid} & :: \text{lift} \Rightarrow \text{bool} \\
\text{-holdsAt} & :: \text{[a, lift]} \Rightarrow \text{bool} \\
\text{-liftEq} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftOr} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftAnd} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftImp} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-RAll} & :: \text{[ids, lift]} \Rightarrow \text{lift} \\
\text{-REx} & :: \text{[ids, lift]} \Rightarrow \text{lift} \\
\text{-REx1} & :: \text{[ids, lift]} \Rightarrow \text{lift} \\
\text{-liftLeq} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftMem} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftNotMem} & :: \text{[lift, lift]} \Rightarrow \text{lift}
\end{align*}

\textbf{syntax (HTML output)}
\begin{align*}
\text{-liftEq} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftOr} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-liftAnd} & :: \text{[lift, lift]} \Rightarrow \text{lift} \\
\text{-RAll} & :: \text{[ids, lift]} \Rightarrow \text{lift} \\
\text{-REx} & :: \text{[ids, lift]} \Rightarrow \text{lift} \\
\text{-REx1} & :: \text{[ids, lift]} \Rightarrow \text{lift}
\end{align*}
-\text{liftLeq} :: [\text{lift}, \text{lift}] \Rightarrow \text{lift} \\
((-/ \leq -) [50, 51] 50) \\
-\text{liftMem} :: [\text{lift}, \text{lift}] \Rightarrow \text{lift} \\
((-/ \in -) [50, 51] 50) \\
-\text{liftNotMem} :: [\text{lift}, \text{lift}] \Rightarrow \text{lift} \\
((-/ \notin -) [50, 51] 50)

\section*{2.3 Definitions}

\text{defs} \\
\text{Valid-def:} \quad \vdash A \equiv \forall w. w \models A \\
\text{unl-con:} \quad \text{LIFT } #c \ w \equiv c \\
\text{unl-lift:} \quad (\text{LIFT } f<x>) \ w \equiv f (x \ w) \\
\text{unl-lift2:} \quad \text{LIFT } f<x, y> \ w \equiv f (x \ w) (y \ w) \\
\text{unl-lift3:} \quad \text{LIFT } f<x, y, z> \ w \equiv f (x \ w) (y \ w) (z \ w) \\
\text{unl-lift4:} \quad \text{LIFT } f<x, y, z, zz> \ w \equiv f (x \ w) (y \ w) (z \ w) (zz \ w)

\text{defs} \\
\text{unl-Rall:} \quad w \models \forall x. A \ x \equiv \forall x. (w \models A \ x) \\
\text{unl-Rex:} \quad w \models \exists x. A \ x \equiv \exists x. (w \models A \ x) \\
\text{unl-Rex1:} \quad w \models \exists! x. A \ x \equiv \exists! x. (w \models A \ x)

We declare the “unlifting rules” as rewrite rules that will be applied automatically.

\text{lemmas} \text{ intensional-rews[simp]} = \\
\quad \text{unl-con \ unh-lift unh-lift2 unh-lift3 unh-lift4} \\
\quad \text{unl-Rall unh-Rex unh-Rex1}

\section*{2.4 Lemmas and Tactics}

\text{lemma} \text{ intD[dest]}: \quad \vdash A \Rightarrow w \models A \\
\langle \text{proof} \rangle \\

\text{lemma} \text{ intI [intro!]:} \quad \text{assumes } P1:(\forall w. w \models A) \text{ shows } \vdash A \\
\langle \text{proof} \rangle \\

Basic unlifting introduces a parameter \( w \) and applies basic rewrites, e.g \( \vdash F = G \) becomes \( F \ w = G \ w \) and \( \vdash F \rightarrow G \) becomes \( F \ w \rightarrow G \ w \).
\langle \text{ML} \rangle \\

\text{lemma} \text{ inteq-reflection:} \quad \text{assumes } P1: \vdash x=y \text{ shows } (x \equiv y) \\
\langle \text{proof} \rangle \\

\text{lemma} \text{ int-simps:} \\
\quad \vdash (x=x) = \# \text{True} \\
\quad \vdash (\neg \ # \text{True}) = \# \text{False} \\
\quad \vdash (\neg \ # \text{False}) = \# \text{True} \\
\quad \vdash (\neg \ P) = P \\
\quad \vdash ((\neg \ P) = P) = \# \text{False} \\
\quad \vdash (P \neq Q) = (P = (\neg \ Q)) \\
\quad \vdash (\# \text{True}=P) = P
⊢ (P = # True) = P
⊢ (# True → P) = P
⊢ (# False → P) = # True
⊢ (P → # True) = # True
⊢ (P → P) = # True
⊢ (P → # False) = (¬P)
⊢ (P → ¬P) = (¬P)
⊢ (P ∧ # True) = P
⊢ (# True ∧ P) = P
⊢ (P ∧ # False) = # False
⊢ (# False ∧ P) = # False
⊢ (P ∧ P) = P
⊢ (P ∧ ¬P) = # False
⊢ (¬P ∧ P) = # False
⊢ (P ∨ # True) = # True
⊢ (# True ∨ P) = # True
⊢ (P ∨ # False) = P
⊢ (# False ∨ P) = P
⊢ (P ∨ P) = P
⊢ (P ∨ ¬P) = # True
⊢ (¬P ∨ P) = # True
⊢ (∀ x. P) = P
⊢ (∃ x. P) = P
⟨ proof ⟩

lemmas intensional-simps[simp] = int-simps[THEN inteq-reflection]
⟨ ML ⟩

lemma Not-Rall: ⊢ (¬(∀ x. F x)) = (∃ x. ¬F x)
⟨ proof ⟩

lemma Not-Rex: ⊢ (¬(∃ x. F x)) = (∀ x. ¬F x)
⟨ proof ⟩

lemma TrueW [simp]: ⊢ # True
⟨ proof ⟩

lemma int-eq: ⊢ X = Y ⊢ X = Y
⟨ proof ⟩

lemma int-iffI:
  assumes ⊢ F → G and ⊢ G → F
  shows ⊢ F = G
⟨ proof ⟩

lemma int-iffD1: assumes h: ⊢ F = G shows ⊢ F → G
⟨ proof ⟩
lemma \textit{int-iffD2}: \textbf{assumes} \ h: \vdash F = G \textbf{ shows} \vdash G \rightarrow F \\
\langle \text{proof} \rangle

lemma \textit{lift-imp-trans}: \\
\textbf{assumes} \vdash A \rightarrow B \textbf{ and} \vdash B \rightarrow C \\
\textbf{ shows} \vdash A \rightarrow C \\
\langle \text{proof} \rangle

lemma \textit{lift-imp-neg}: \textbf{assumes} \vdash A \rightarrow B \textbf{ shows} \vdash \neg B \rightarrow \neg A \\
\langle \text{proof} \rangle

lemma \textit{lift-and-com}: \vdash (A \land B) = (B \land A) \\
\langle \text{proof} \rangle

end

3 \ Semantics

theory \textit{Semantics}\\nimports \textit{Sequence Intensional}\\nbegin

This theory mechanises a \textit{shallow} embedding of TLA* using the \textit{Sequence} and \textit{Intensional} theories. A shallow embedding represents TLA* using Isabelle/HOL predicates, while a \textit{deep} embedding would represent TLA* formulas and pre-formulas as mutually inductive datatypes\(^1\). The choice of a shallow over a deep embedding is motivated by the following factors: a shallow embedding is usually less involved, and existing Isabelle theories and tools can be applied more directly to enhance automation; due to the lifting in the \textit{Intensional} theory, a shallow embedding can reuse standard logical operators, whilst a deep embedding requires a different set of operators for both formulas and pre-formulas. Finally, since our target is system verification rather than proving meta-properties of TLA*, which requires a deep embedding, a shallow embedding is more fit for purpose.

3.1 \ Types of Formulas

To mechanise the TLA* semantics, the following type abbreviations are used:

type-synonym ('a,'b) \textit{formfun} = 'a seq \Rightarrow 'b \\
type-synonym 'a \textit{formula} = ('a,\textit{bool}) \textit{formfun} \\
type-synonym ('a,'b) \textit{stfun} = 'a \Rightarrow 'b \\
type-synonym 'a \textit{stpred} = ('a,\textit{bool}) \textit{stfun}

instance \\
\textit{fun} :: (type,type) world \langle \text{proof} \rangle

\(^1\)See e.g. [10] for a discussion about deep vs. shallow embeddings in Isabelle/HOL.
instance

prod :: (type,type) world ⟨proof⟩

Pair and function are instantiated to be of type class world. This allows use of the lifted intensional logic for formulas, and standard logical connectives can therefore be used.

3.2 Semantics of TLA*

The semantics of TLA* is defined.

definition always :: ('a::world) formula ⇒ 'a formula
where always F ≡ λ s. ∀ n. (s |ₙ n) ⊨ F

definition nexts :: ('a::world) formula ⇒ 'a formula
where nexts F ≡ λ s. (tail s) |ₙ = F

definition before :: ('a::world,'b) stfun ⇒ ('a,'b) formfun
where before f ≡ λ s. (first s) |ₙ = f

definition after :: ('a::world,'b) stfun ⇒ ('a,'b) formfun
where after f ≡ λ s. (second s) |ₙ = f

definition unch :: ('a::world,'b) stfun ⇒ 'a formula
where unch v ≡ λ s. s |ₙ = (after v) = (before v)

definition action :: ('a::world) formula ⇒ ('a,'b) stfun ⇒ 'a formula
where action P v ≡ λ s. ∀ i. ((s |ₙ i) ⊨ P) ∨ ((s |ₙ i) ⊨ unch v)

3.2.1 Concrete Syntax

This is the concrete syntax for the (abstract) operators above.

syntax

-always :: lift ⇒ lift (([ ] [90] 90))
-nexts :: lift ⇒ lift ((Next -) [90] 90)
-action :: [lift,lift] ⇒ lift ((([ ]'(-)) [20,1000] 90)
-before :: lift ⇒ lift ((-$) [100] 99)
-after :: lift ⇒ lift ((+$) [100] 99)
-prime :: lift ⇒ lift ((-' [100] 99)
-unch :: lift ⇒ lift (((Unchanged -) [100] 99)
TEMP :: lift ⇒ 'b ((TEMP -))

translations

-always ⇔ CONST always
-nexts ⇔ CONST nexts
-action ⇔ CONST action
-before ⇔ CONST before
-after ⇔ CONST after
3.3 Abbreviations

Some standard temporal abbreviations, with their concrete syntax.

**definition** actrans :: (′a::world) formula ⇒ (′a,′b) stfun ⇒ 'a formula
**where** actrans P v ≡ TEMP(P ∨ unch v)

**definition** eventually :: (′a::world) formula ⇒ 'a formula
**where** eventually F ≡ LIFT(¬□(¬F))

**definition** angle-action :: (′a::world) formula ⇒ (′a,′b) stfun ⇒ 'a formula
**where** angle-action P v ≡ LIFT(¬□[¬P]-v)

**definition** angle-actrans :: (′a::world) formula ⇒ (′a,′b) stfun ⇒ 'a formula
**where** angle-actrans P v ≡ TEMP(¬ actrans (LIFT(¬P)) v)

**definition** leadsto :: (′a::world) formula ⇒ 'a formula ⇒ 'a formula
**where** leadsto P Q ≡ LIFT □(P → eventually Q)

3.3.1 Concrete Syntax

**syntax**
-actrans :: [lift,lift] ⇒ lift (([·]-(-)) [20,1000] 90)
-eventually :: lift ⇒ lift ((<>) [90] 90)
-angle-action :: [lift,lift] ⇒ lift ((<><>')(-)) [20,1000] 90)
-angle-actrans :: [lift,lift] ⇒ lift ((<>')-(-)) [20,1000] 90)

**translations**
-actrans ⇔ CONST actrans
-eventually ⇔ CONST eventually
-angle-action ⇔ CONST angle-action
-angle-actrans ⇔ CONST angle-actrans
-leadsto ⇔ CONST leadsto

**syntax** (xsymbols)
-eventually :: lift ⇒ lift ((⋅-) [90] 90)
-angle-action :: [lift,lift] ⇒ lift ((⋅')(-)) [20,1000] 90)
-angle-actrans :: [lift,lift] ⇒ lift (((⋅')(-)) [20,1000] 90)
3.4 Properties of Operators

The following lemmas show that these operators have the expected semantics.

**lemma eventually-defs:** 
\[(\mathcal{w} \models \Diamond F) = (\exists n. (\mathcal{w} \upharpoonright n) \models F)\]

**proof**

**lemma angle-action-defs:** 
\[(\mathcal{w} \models \Diamond \langle P \rangle -v) = (\exists i. (\mathcal{w} \upharpoonright i) \models P) \land ((\mathcal{w} \upharpoonright i) \models v \neq \$v))\]

**proof**

**lemma unch-defs:** 
\[(\mathcal{w} \models Unchanged v) = ((second \mathcal{w}) \models v) = (\mathcal{w} \models v)\]

**proof**

**lemma linaw:**

assumes h1: \(a \leq b\) and h2: \((\mathcal{w} \upharpoonright a) \models \Box A\)

shows \((\mathcal{w} \upharpoonright b) \models \Box A\)

**proof**

3.5 Invariance Under Stuttering

A key feature of TLA* is that specification at different abstraction levels can be compared. The soundness of this relies on the stuttering invariance of formulas. Since the embedding is shallow, it cannot be shown that a generic TLA* formula is stuttering invariant. However, this section will show that each operator is stuttering invariant or preserves stuttering invariance in an appropriate sense, which can be used to show stuttering invariance for given specifications.

Formula \(F\) is stuttering invariant if for any two similar behaviours (i.e., sequences of states), \(F\) holds in one iff it holds in the other. The definition is generalised to arbitrary expressions, and not just predicates.

**definition stutinv:** \(\langle a, b \rangle \text{ formfun } \Rightarrow \text{ bool}\)

**where stutinv F \equiv \forall \sigma \tau. \sigma \preceq \tau \rightarrow (\sigma \models F) = (\tau \models F)\)

The requirement for stuttering invariance is too strong for pre-formulas. For example, an action formula specifies a relation between the first two states of a behaviour, and will rarely be satisfied by a stuttering step. This is why pre-formulas are “protected” by (square or angle) brackets in TLA*:

the only place a pre-formula \(P\) can be used is inside an action: \(\Box [P] -v\). To show that \(\Box [P] -v\) is stuttering invariant, is must be shown that a slightly weaker predicate holds for \(P\). For example, if \(P\) contains a term of the form \(\text{oo } Q\), then it is not a well-formed pre-formula, thus \(\Box [P] -v\) is not stuttering invariant. This weaker version of stuttering invariance has been named near stuttering invariance.

**definition nstutinv:** \(\langle a, b \rangle \text{ formfun } \Rightarrow \text{ bool}\)
where \( nsstutinv \) \( P \equiv \forall \sigma \tau. (\text{first} \sigma = \text{first} \tau) \land (\text{tail} \sigma) \approx (\text{tail} \tau) \rightarrow (\sigma \models P) = (\tau \models P) \)

**Syntax**

- \textit{-stutinv} :: lift \( \Rightarrow \) bool ((\textit{STUTINV -}) [40] 40)
- \textit{-nstutinv} :: lift \( \Rightarrow \) bool ((\textit{NSTUTINV -}) [40] 40)

**Translations**

- \textit{-stutinv} \( \rightleftharpoons \) \textit{CONST stutinv}
- \textit{-nstutinv} \( \rightleftharpoons \) \textit{CONST nstutinv}

Predicate \( \textit{STUTINV} \) \( F \) formalises stuttering invariance for formula \( F \). That is if two sequences are similar \( s \approx t \) (equal up to stuttering) then the validity of \( F \) under both \( s \) and \( t \) are equivalent. Predicate \( \textit{NSTUTINV} \) \( P \) should be read as \textit{nearly stuttering invariant} – and is required for some stuttering invariance proofs.

**Lemma** \( \textit{stutinv}-\textit{strictly}-\textit{stronger} \):
- \textbf{Assumes} \( h \): \( \textit{STUTINV} \) \( F \)

\[ \langle \text{proof} \rangle \]

### 3.5.1 Properties of \textit{-stutinv}

This subsection proves stuttering invariance, preservation of stuttering invariance and introduction of stuttering invariance for different formulas. First, state predicates are stuttering invariant.

**Theorem** \( \textit{stut-before} \): \( \textit{STUTINV} \) \( \$F \)

\[ \langle \text{proof} \rangle \]

**Lemma** \( \textit{nstut-after} \): \( \textit{NSTUTINV} \) \( F\$ \)

\[ \langle \text{proof} \rangle \]

The always operator preserves stuttering invariance.

**Theorem** \( \textit{stut-always} \): \textbf{Assumes} \( H \): \( \textit{STUTINV} \) \( F \)

\[ \text{shows} \ \textit{STUTINV} \ \Box F \]

\[ \langle \text{proof} \rangle \]

Assuming that formula \( P \) is nearly stuttering invariant then \( \Box[P]-v \) will be stuttering invariant.

**Lemma** \( \textit{stut-action-lemma} \):
- \textbf{Assumes} \( H \): \( \textit{NSTUTINV} \) \( P \) and \( st \): \( s \approx t \) and \( P \): \( t \models □[P]-v \)

\[ \text{shows} \ s \models □[P]-v \]

\[ \langle \text{proof} \rangle \]

**Theorem** \( \textit{stut-action} \): \textbf{Assumes} \( H \): \( \textit{NSTUTINV} \) \( P \)

\[ \text{shows} \ \textit{STUTINV} \ \Box[P]-v \]

\[ \langle \text{proof} \rangle \]

The lemmas below shows that propositional and predicate operators preserve stuttering invariance.
lemma stut-and: $[\text{STUTINV } F; \text{STUTINV } G] \Rightarrow \text{STUTINV } (F \land G)$
  ⟨proof⟩

lemma stut-or: $[\text{STUTINV } F; \text{STUTINV } G] \Rightarrow \text{STUTINV } (F \lor G)$
  ⟨proof⟩

lemma stut-imp: $[\text{STUTINV } F; \text{STUTINV } G] \Rightarrow \text{STUTINV } (F \rightarrow G)$
  ⟨proof⟩

lemma stut-eq: $[\text{STUTINV } F; \text{STUTINV } G] \Rightarrow \text{STUTINV } (F = G)$
  ⟨proof⟩

lemma stut-noteq: $[\text{STUTINV } F; \text{STUTINV } G] \Rightarrow \text{STUTINV } (F \neq G)$
  ⟨proof⟩

lemma stut-not: $\text{STUTINV } F \Rightarrow \text{STUTINV } (\neg F)$
  ⟨proof⟩

lemma stut-all: $(\forall x. \text{STUTINV } (F x)) \Rightarrow \text{STUTINV } (\forall x. F x)$
  ⟨proof⟩

lemma stut-ex: $(\exists x. \text{STUTINV } (F x)) \Rightarrow \text{STUTINV } (\exists x. F x)$
  ⟨proof⟩

lemma stut-const: $\text{STUTINV } \#c$
  ⟨proof⟩

lemma stut-fun1: $\text{STUTINV } X \Rightarrow \text{STUTINV } (f <X>)$
  ⟨proof⟩

lemma stut-fun2: $[\text{STUTINV } X; \text{STUTINV } Y] \Rightarrow \text{STUTINV } (f <X,Y>)$
  ⟨proof⟩

lemma stut-fun3: $[\text{STUTINV } X; \text{STUTINV } Y; \text{STUTINV } Z] \Rightarrow \text{STUTINV } (f <X,Y,Z>)$
  ⟨proof⟩

lemma stut-fun4: $[\text{STUTINV } X; \text{STUTINV } Y; \text{STUTINV } Z; \text{STUTINV } W] \Rightarrow \text{STUTINV } (f <X,Y,Z,W>)$
  ⟨proof⟩

lemma stut-plus: $[\text{STUTINV } x; \text{STUTINV } y] \Rightarrow \text{STUTINV } (x+y)$
  ⟨proof⟩

3.5.2 Properties of -nstutinv

This subsection shows analogous properties about near stuttering invariance. If a formula $F$ is stuttering invariant then $\circ F$ is nearly stuttering invariant.
The lemmas below shows that propositional and predicate operators preserves near stuttering invariance.

**lemma nstut-and:** assumes $H: \text{STUTINV } F$ shows $\text{NSTUTINV } \circ F$

(proof)

**lemma nstut-or:** $[\text{NSTUTINV } F; \text{NSTUTINV } G] \implies \text{NSTUTINV } (F \lor G)$

(proof)

**lemma nstut-imp:** $[\text{NSTUTINV } F; \text{NSTUTINV } G] \implies \text{NSTUTINV } (F \rightarrow G)$

(proof)

**lemma nstut-eq:** $[\text{NSTUTINV } F; \text{NSTUTINV } G] \implies \text{NSTUTINV } (F = G)$

(proof)

**lemma nstut-not:** $\text{NSTUTINV } F \implies \text{NSTUTINV } (\neg F)$

(proof)

**lemma nstut-noteq:** $[\text{NSTUTINV } F; \text{NSTUTINV } G] \implies \text{NSTUTINV } (F \neq G)$

(proof)

**lemma nstut-all:** $(\forall x. \text{NSTUTINV } (F x)) \implies \text{NSTUTINV } (\forall x. F x)$

(proof)

**lemma nstut-ex:** $(\exists x. \text{NSTUTINV } (F x)) \implies \text{NSTUTINV } (\exists x. F x)$

(proof)

**lemma nstut-const:** $\text{NSTUTINV } \# c$

(proof)

**lemma nstut-fun1:** $\text{NSTUTINV } X \implies \text{NSTUTINV } (f <X>)$

(proof)

**lemma nstut-fun2:** $[\text{NSTUTINV } X; \text{NSTUTINV } Y] \implies \text{NSTUTINV } (f <X,Y>)$

(proof)

**lemma nstut-fun3:** $[\text{NSTUTINV } X; \text{NSTUTINV } Y; \text{NSTUTINV } Z] \implies \text{NSTUTINV } (f <X,Y,Z>)$

(proof)

**lemma nstut-fun4:** $[\text{NSTUTINV } X; \text{NSTUTINV } Y; \text{NSTUTINV } Z; \text{NSTUTINV } W] \implies \text{NSTUTINV } (f <X,Y,Z,W>)$

(proof)

**lemma nstut-plus:** $[\text{NSTUTINV } x; \text{NSTUTINV } y] \implies \text{NSTUTINV } (x+y)$

(proof)

24
### 3.5.3 Abbreviations

We show the obvious fact that the same properties holds for abbreviated operators.

**lemma** `nstut-before` = `stut-before[THEN stutinv-strictly-stronger]`

**lemma** `nstut-unch`: `NSTUTINV (Unchanged v)`

Formulas `[P] - v` are not TLA* formulas by themselves, but we need to reason about them when they appear wrapped inside `□[-].v`. We only require that it preserves nearly stuttering invariance. Observe that `[P] - v` trivially holds for a stuttering step, so it cannot be stuttering invariant.

**lemma** `nstut-actrans`: `NSTUTINV P \implies NSTUTINV [P] - v`

**lemma** `nstut-eventually`: `STUTINV F \implies STUTINV \Diamond F`

**lemma** `nstut-leadsto`: `[STUTINV F; STUTINV G] \implies STUTINV (F \leadsto G)`

**lemma** `nstut-angle-action`: `NSTUTINV P \implies STUTINV \Diamond (P) - v`

**lemma** `nstut-angle-acttrans`: `NSTUTINV P \implies NSTUTINV \langle P \rangle - v`

**lemmas** `stutinvs = stut-before stut-always stut-action stut-and stut-or stut-imp stut-eq stut-noteq stut-not stut-all stut-ex stut-eventually stut-leadsto stut-angle-action stut-const stut-fun1 stut-fun2 stut-fun3 stut-fun4`

**lemmas** `nstutinvs = nstut-after nstut-nexts nstut-actrans nstut-unch nstut-and nstut-or nstut-imp nstut-eq nstut-noteq nstut-not nstut-all nstut-ex nstut-angle-acttrans stutinv-strictly-stronger nstut-fun1 nstut-fun2 nstut-fun3 nstut-fun4 stutinvs[THEN stutinv-strictly-stronger]`

**lemmas** `bothstutinvs = stutinvs nstutinvs`

end

## 4 Reasoning about PreFormulas

**theory** `PreFormulas`

**imports** `Semantics`

**begin**
Semantic separation of formulas and pre-formulas requires a deep embedding. We introduce a syntactically distinct notion of validity, written \( \mathord{\not\vdash} A \), for pre-formulas. Although it is semantically identical to \( \vdash A \), it helps users distinguish pre-formulas from formulas in TLA\(^*\) proofs.

**definition** PreValid :: (\([w::world]\) form \(\Rightarrow\) bool

**syntax**

\[-\text{PreValid} :: \text{lift} \Rightarrow \text{bool} \quad (((\not\cdot \cdot) \: 5)\]

**translations**

-PreValid \(\Rightarrow\) CONST PreValid

**lemma** prefD[dest]: \( \not\vdash A \implies w \models A \) (proof)

**lemma** prefI[intro]: \( (\forall w. w \models A) \implies \not\vdash A \) (proof)

**lemma** pref-eq-reflection: assumes \( P1: \not\vdash x = y \) shows \( x \equiv y \) (ML)

**lemma** pref-True[simp]: \( \not\vdash \#\text{True} \)

**lemma** pref-eq: \( \not\vdash X = Y \implies X = Y \)

**lemma** pref-iffI:

assumes \( \not\vdash F \rightarrow G \) and \( \not\vdash G \rightarrow F \)

shows \( \not\vdash F = G \)

(proof)

**lemma** pref-iffD1: assumes \( \not\vdash F = G \) shows \( \not\vdash F \rightarrow G \)

(proof)

**lemma** pref-iffD2: assumes \( \not\vdash F = G \) shows \( \not\vdash G \rightarrow F \)

(proof)

**lemma** unl-pref-imp:

assumes \( \not\vdash F \rightarrow G \) \(\land\) \( w. w \models F \implies w \models G \)

(proof)

**lemma** pref-imp-trans:

assumes \( \not\vdash F \rightarrow G \) and \( \not\vdash G \rightarrow H \)

shows \( \not\vdash F \rightarrow H \)

(proof)
Many of the TLA axioms only require a state function witness which leaves the state space unchanged. An obvious witness is the $id$ function. The lemmas require that the given formula is invariant under stuttering.

**Lemma pre-id-unch:**
assumes $h$: stutter F
shows $\neg F \land \text{Unchanged } id \rightarrow oF$

**Lemma pre-ex-unch:**
assumes $h$: stutter F
shows $\exists (v::a::world \Rightarrow 'a)$. ($\neg F \land \text{Unchanged } v \rightarrow oF$)

**Lemma unch-pair:** $\neg \text{Unchanged } (x,y) = (\text{Unchanged } x \land \text{Unchanged } y)$

**Lemmas unch-eq1 = unch-pair[THEN pref-eq]**
**Lemmas unch-eq2 = unch-pair[THEN prefeq-reflection]**

**Lemma angle-actrans-sem:** $\neg \langle F \rangle_{v} = (F \land v$ $\neq v)$

**Lemmas angle-actrans-sem-eq = angle-actrans-sem[THEN pref-eq]**

### 4.2 Lemmas about after

**Lemma after-const:** $\neg (\# c)' = \# c$

**Lemma after-fun1:** $\neg f<x>' = f<x'>$

**Lemma after-fun2:** $\neg f<x,y>' = f<x',y'>$

**Lemma after-fun3:** $\neg f<x,y,z>' = f<x',y',z'>$

**Lemma after-fun4:** $\neg f<x,y,z,zz>' = f<x',y',z',zz'>$

**Lemma after-forall:** $\neg (\forall x. P x)' = (\forall x. (P x)')$

**Lemma after-exists:** $\neg (\exists x. P x)' = (\exists x. (P x)')$

**Lemma after-exists1:** $\neg (\exists! x. P x)' = (\exists! x. (P x)')$
lemmas all-after = after-const after-fun1 after-fun2 after-fun3 after-fun4 after-forall after-exists after-exists1

lemmas all-after-unl = all-after[THEN prefD]
lemmas all-after-eq = all-after[THEN prefeq-reflection]

4.3 Lemmas about before

lemma before-const: \( \vdash \#(\# c) = \# c \)

lemma before-fun1: \( \vdash (f<x>) = f <\$x> \)

lemma before-fun2: \( \vdash (f<x,y>) = f <\$x,\$y> \)

lemma before-fun3: \( \vdash (f<x,y,z>) = f <\$x,\$y,\$z> \)

lemma before-fun4: \( \vdash (f<x,y,z,zz>) = f <\$x,\$y,\$z,\$zz> \)

lemma before-forall: \( \vdash (\forall x. P x) = (\forall x. $(P x)) \)

lemma before-exists: \( \vdash (\exists x. P x) = (\exists x. $(P x)) \)

lemma before-exists1: \( \vdash (\exists! x. P x) = (\exists! x. $(P x)) \)

lemmas all-before = before-const before-fun1 before-fun2 before-fun3 before-fun4 before-forall before-exists before-exists1

lemmas all-before-unl = all-before[THEN intD]
lemmas all-before-eq = all-before[THEN inteq-reflection]

4.4 Some general properties

lemma angle-actrans-conj: \( \lnot ((F \land G)\cdot v) = (F\cdot v \land (G)\cdot v) \)

lemma angle-actrans-disj: \( \lnot ((F \lor G)\cdot v) = (F\cdot v \lor (G)\cdot v) \)

lemma int-eq-true: \( \vdash P \implies \vdash P = \# True \)
lemma pref-eq-true: \( \neg P \Rightarrow \neg P = \# True \)

4.5 Unlifting attributes and methods

Attribute which unlifts an intensional formula or preformula

Attribute which turns an intensional formula or preformula into a rewrite rule. Formulas \( F \) that are not equalities are turned into \( F \equiv \# True \).

5 A Proof System for TLA*

theory Rules
imports PreFormulas
begin

We prove soundness of the proof system of TLA*, from which the system verification rules from Lamport’s original TLA paper will be derived. This theory is still state-independent, thus state-dependent enableness proofs, required for proofs based on fairness assumptions, and flexible quantification, are not discussed here.

The TLA* paper [8] suggest both a heterogeneous and a homogeneous proof system for TLA*. The homogeneous version eliminates the auxiliary definitions from the Preformula theory, creating a single provability relation. This axiomatisation is based on the fact that a pre-formula can only be used via the \textit{sq} rule. In a nutshell, \textit{sq} is applied to \textit{pax1} to \textit{pax5}, and \textit{nex}, \textit{pre} and \textit{pmp} are changed to accommodate this. It is argued that while the heterogeneous version is easier to understand, the homogenous system avoids the introduction of an auxiliary provability relation. However, the price to pay is that reasoning about pre-formulas (in particular, actions) has to be performed in the scope of temporal operators such as \( \square [P] - v \), which is notationally quite heavy. We prefer here the heterogeneous approach, which exposes the pre-formulas and lets us use standard HOL rules more directly.

5.1 The Basic Axioms

theorem fmp: assumes \( \vdash F \) and \( \vdash F \rightarrow G \) shows \( \vdash G \)

theorem pmp: assumes \( \neg F \) and \( \neg F \rightarrow G \) shows \( \neg G \)
Theorem to show that universal quantification distributes over the always
operator. Since the TLA∗ paper only addresses the propositional fragment, this theorem does not appear there.

**Theorem allT:** \( \forall x. \Box(F(x)) = (\Box(\forall x. F(x))) \)

(\textit{proof})

**Theorem allActT:** \( \forall x. \Box[F(x)] = (\Box[\forall x. F(x)]) \)

(\textit{proof})

### 5.2 Derived Theorems

This section includes some derived theorems based on the axioms, taken from the TLA∗ paper [8]. We mimic the proofs given there and avoid semantic reasoning whenever possible.

The \textit{alw} theorem of [8] states that if \( F \) holds in all worlds then it always holds, i.e. \( F \models \Box F \). However, the derivation of this theorem (using the proof rules above) relies on access of the set of free variables (FV), which is not available in a shallow encoding.

However, we can prove a similar rule \textit{alw2} using an additional hypothesis \( \sim F \land \text{Unchanged } v \rightarrow \circ F \).

**Theorem alw2:**
- \textit{assumes} \( h1: \models F \) and \( h2: \sim F \land \text{Unchanged } v \rightarrow \circ F \)
- \textit{shows} \( \Box F \)

(\textit{proof})

Similar theorem, assuming that \( F \) is stuttering invariant.

**Theorem alw3:**
- \textit{assumes} \( h1: \models F \) and \( h2: \text{stutinv } F \)
- \textit{shows} \( \Box F \)

(\textit{proof})

In a deep embedding, we could prove that all (proper) TLA∗ formulas are stuttering invariant and then get rid of the second hypothesis of rule \textit{alw3}. In fact, the rule is even true for pre-formulas, as shown by the following rule, whose proof relies on semantical reasoning.

**Theorem alw:** \textit{assumes} \( H1: \models F \) \textit{shows} \( \Box F \)

(\textit{proof})

**Theorem alw-valid-iff-valid:** \( \models (\Box F) = (\Box[\forall x. F(x)]) \)

(\textit{proof})

[8] proves the following theorem using the deduction theorem of TLA∗: \( \models F \implies \models G \implies \models \Box F \implies G \), which can only be proved by induction on the formula structure, in a deep embedding.

**Theorem TI[simp-unl]:** \( \Box \Box F = \Box F \)

(\textit{proof})
theorem T2[simp-und]: \( \vdash \Box \Box [P] \rightarrow \Box [P] \)
(proof)

theorem T3[simp-und]: \( \vdash \Box[[P] \rightarrow \Box [P] \)
(proof)

theorem M2:
assumes h: \( \sim F \rightarrow G \)
shows \( \vdash \Box [F] \rightarrow \Box [G] \)
(proof)

theorem N1:
assumes h: \( \vdash F \rightarrow G \)
shows \( \vdash \sim \circ F \rightarrow \circ G \)
(proof)

theorem T4: \( \vdash \Box [P] \rightarrow \Box [[P] \rightarrow \Box [P] \)
(proof)

theorem T5: \( \vdash \Box [[P] \rightarrow \Box [[P] \rightarrow \Box [P] \)
(proof)

theorem T6: \( \vdash \Box F \rightarrow \Box [\circ F] \)
(proof)

theorem T7:
assumes h: \( \sim F \wedge \text{Unchanged} v \rightarrow \circ F \)
shows \( \sim (F \wedge \Box \circ F) = \Box F \)
(proof)

theorem T8: \( \sim (\circ (F \wedge G) = (\circ F \wedge \circ G) \)
(proof)

lemma T9: \( \sim \Box [A] \rightarrow [A] \)
(proof)

theorem H1:
assumes h1: \( \vdash \Box[P] \rightarrow \Box[P \rightarrow Q] \)
and h2: \( \vdash [P \rightarrow Q] \)
shows \( \vdash [Q] \)
(proof)

theorem H2: assumes h1: \( \vdash F \) shows \( \vdash [F] \)
(proof)

theorem H3:
assumes h1: \( \vdash [P \rightarrow Q] \)
and h2: \( \vdash [Q \rightarrow R] \)
shows \( \vdash [P \rightarrow R] \)
(proof)
theorem $H_4$: $\vdash \Box [P] \rightarrow P$
\begin{proof}
\end{proof}

theorem $H_5$: $\vdash \Box \Box F \rightarrow \Diamond \Box F$
\begin{proof}
\end{proof}

5.3 Some other useful derived theorems

theorem $P_1$: $\neg \Box F \rightarrow \Diamond F$
\begin{proof}
\end{proof}

theorem $P_2$: $\neg \Box F \rightarrow F \land \Diamond F$
\begin{proof}
\end{proof}

theorem $P_3$: $\vdash \Box F \rightarrow \Box [F]$
\begin{proof}
\end{proof}

theorem $P_4$: $\vdash \Box [P] \rightarrow \Box [\Box P]$-v
\begin{proof}
\end{proof}

theorem $M_0$: $\vdash \Box F \rightarrow \Box [F] \rightarrow \Diamond F$
\begin{proof}
\end{proof}

theorem $M_1$: $\vdash \Box F \rightarrow \Box [F \land \Diamond F]$-v
\begin{proof}
\end{proof}

theorem $M_2$: assumes $h: \vdash F$ shows $\vdash \Box [\Diamond F]$-v
\begin{proof}
\end{proof}

lemma $M_3$: $\vdash \Box [\Diamond (F \land G)] = (\Diamond F \land \Diamond G)$-v
\begin{proof}
\end{proof}

theorem $M_4$: $\vdash \Box [\Diamond (F \land G)] \rightarrow \Diamond [\Diamond (F \land G)]$-v
\begin{proof}
\end{proof}

theorem $M_5$: $\vdash [\Box [P] \rightarrow \Box [\Box P]]$-w
\begin{proof}
\end{proof}

theorem $M_6$: $\vdash \Box [F \land G] \rightarrow \Box [F] \land \Box [G]$-v
\begin{proof}
\end{proof}

theorem $M_7$: $\vdash \Box [F] \land \Box [G] \rightarrow \Box [F \land G]$-v
\begin{proof}
\end{proof}

theorem $M_8$: $\vdash \Box [F \land G] = (\Box [F] \land \Box [G])$
\begin{proof}
\end{proof}

theorem $M_9$: $\vdash \Box F \rightarrow F \land \Diamond F$
\begin{proof}
\end{proof}

theorem $M_{10}$:
assumes $h: \lnot F \land Unchanged v \rightarrow \circ F$
shows $\lnot F \land \circ \Box F \rightarrow \Box F$
⟨proof⟩

**Theorem M11:**
assumes $h: \lnot [A]-f \rightarrow [B]-g$
shows $\vdash \Box[A]-f \rightarrow \Box[B]-g$
⟨proof⟩

**Theorem M12:** $\vdash (\Box[A]-f \land \Box[B]-g) = \Box[[A]-f \land [B]-g]-f,g)$
⟨proof⟩

We now derive Lamport’s 6 simple temporal logic rules (STL1)-(STL6) [5].
Firstly, STL1 is the same as $\vdash ?F = \vdash \Box ?F$ derived above.

**Theorems STL1 = alw**

STL2 and STL3 have also already been derived.

**Theorems STL2 = ax1**

**Theorems STL3 = T1**

As with the derivation of $\vdash ?F = \vdash \Box ?F$, a purely syntactic derivation of (STL4) relies on an additional argument – either using Unchanged or STUTINV.

**Theorem STL4-2:**
assumes $h1: \vdash F \rightarrow G$ and $h2: \lnot G \land Unchanged v \rightarrow \circ G$
shows $\vdash \Box F \rightarrow \Box G$
⟨proof⟩

**Lemma STL4-3:**
assumes $h1: \vdash F \rightarrow G$ and $h2: STUTINV G$
shows $\vdash \Box F \rightarrow \Box G$
⟨proof⟩

Of course, the original rule can be derived semantically

**Lemma STL4:** assumes $h: \vdash F \rightarrow G$ shows $\vdash \Box F \rightarrow \Box G$
⟨proof⟩

Dual rule for ◊

**Lemma STL4-eve:** assumes $h: \vdash F \rightarrow G$ shows $\vdash \Diamond F \rightarrow \Diamond G$
⟨proof⟩

Similarly, a purely syntactic derivation of (STL5) requires extra hypotheses.

**Theorem STL5-2:**
assumes $h1: \lnot F \land Unchanged f \rightarrow \circ F$
and $h2: \lnot G \land Unchanged g \rightarrow \circ G$
shows $\vdash \Box(F \land G) = (\Box F \land \Box G)$

34
\[\text{proof}\]

\textbf{Theorem STL5-21:} \\
\textbf{Assumes} \(h_1: \text{stutinv } F\) \text{ and } \(h_2: \text{stutinv } G\) \\
\textbf{Shows} \(\vdash \Box(F \land G) = (\Box F \land \Box G)\) \\
\(\text{proof}\)

We also derive STL5 semantically. \\
\textbf{Lemma STL5:} \(\vdash \Box(F \land G) = (\Box F \land \Box G)\) \\
\(\text{proof}\)

Elimination rule corresponding to STL5 in unlifted form. \\
\textbf{Lemma box-conjE:} \\
\textbf{Assumes} \(s \models \Box F\) \text{ and } \(s \models \Box G\) \text{ and } \(s \models (F \land G) \Rightarrow P\) \\
\textbf{Shows} \(P\) \\
\(\text{proof}\)

\textbf{Lemma box-thin:} \\
\textbf{Assumes} \(h_1: s \models \Box F\) \text{ and } \(h_2: \text{PROP } W\) \\
\textbf{Shows} \(\text{PROP } W\) \\
\(\text{proof}\)

Finally, we derive STL6 (only semantically) \\
\textbf{Lemma STL6:} \(\vdash \Diamond \Box(F \land G) = (\Diamond \Box F \land \Diamond \Box G)\) \\
\(\text{proof}\)

\textbf{Lemma MM0:} \(\vdash \Box(F \rightarrow G) \rightarrow \Box F \rightarrow \Box G\) \\
\(\text{proof}\)

\textbf{Lemma MM1:} \textbf{Assumes} \(h: \vdash F = G\) \textbf{Shows} \(\vdash \Box F = \Box G\) \\
\(\text{proof}\)

\textbf{Theorem MM2:} \(\vdash \Box A \land \Box(B \rightarrow C) \rightarrow \Box(A \land B \rightarrow C)\) \\
\(\text{proof}\)

\textbf{Theorem MM3:} \(\vdash \Box \neg A \rightarrow \Box(A \land B \rightarrow C)\) \\
\(\text{proof}\)

\textbf{Theorem MM4\{simp-unl\}:} \(\vdash \Box \# F = \# F\) \\
\(\text{proof}\)

\textbf{Theorem MM4b\{simp-unl\}:} \(\vdash \Box \neg \# F = \neg \# F\) \\
\(\text{proof}\)

\textbf{Theorem MM5:} \(\vdash \Box F \lor \Box G \rightarrow \Box(F \lor G)\) \\
\(\text{proof}\)

\textbf{Theorem MM6:} \(\vdash \Box F \lor \Box G \rightarrow \Box(\Box F \lor \Box G)\) \\
\(\text{proof}\)

35
lemma MM10:
assumes h: \( \neg F = G \) shows \( \Box[F] \sim v = \Box[G] \sim v \)
⟨proof⟩

lemma MM9:
assumes h: \( \vdash F = G \) shows \( \Box[F] \sim v = \Box[G] \sim v \)
⟨proof⟩

theorem MM11: \( \vdash \Box[\neg(P \land Q)] \sim v \rightarrow \Box[P] \sim v \rightarrow \Box[P \land \neg Q] \sim v \)
⟨proof⟩

theorem MM12[simp-und]: \( \vdash \Box[\neg P] \sim v = \Box[P] \sim v \)
⟨proof⟩

5.4 Theorems about the eventually operator
— rules to push negation inside modal operators, sometimes useful for rewriting

theorem dualization:
\( \vdash \neg \Box F = \Diamond \neg F \)
\( \vdash \neg \Diamond F = \Box \neg F \)
\( \vdash \neg \Diamond (A) \sim v = \Diamond (\neg A) \sim v \)
\( \vdash \neg \Diamond (A) \sim v = \Box (\neg A) \sim v \)
⟨proof⟩

theorems dualization-rev = dualization[int-rewrite]
theorems dualization-und = dualization[undlifted]

theorem E1: \( \vdash \Diamond (F \lor G) = (\Diamond F \lor \Diamond G) \)
⟨proof⟩

theorem E3: \( \vdash F \rightarrow \Diamond F \)
⟨proof⟩

theorem E4: \( \vdash \Box F \rightarrow \Diamond F \)
⟨proof⟩

theorem E5: \( \vdash \Box F \rightarrow \Box \Diamond F \)
⟨proof⟩

theorem E6: \( \vdash \Box F \rightarrow \Diamond \Box F \)
⟨proof⟩

theorem E7:
assumes h: \( \neg F \land Unchanged \) shows \( \neg \Diamond F \rightarrow F \lor \Diamond F \)
⟨proof⟩

theorem E8: \( \vdash \Diamond (F \rightarrow G) \rightarrow \Box F \rightarrow \Diamond G \)

\begin{proof}

**Theorem E9**: \( \vdash \Box (F \rightarrow G) \rightarrow \Diamond F \rightarrow \Diamond G \)
\end{proof}

**Theorem E10** \([\text{simp-unl}]\): \( \vdash \Diamond \Diamond F = \Diamond F \)
\end{proof}

**Theorem E22**: 
\begin{enumerate}
\item Assumes \( h : \vdash F = G \)
\item Shows \( \vdash \Diamond F = \Diamond G \)
\end{enumerate}
\end{proof}

**Theorem E15** \([\text{simp-unl}]\): \( \vdash \Diamond \# F = \# F \)
\end{proof}

**Theorem E15b** \([\text{simp-unl}]\): \( \vdash \Diamond \neg \# F = \neg \# F \)
\end{proof}

**Theorem E16**: \( \vdash \Diamond \Box F \rightarrow \Diamond F \)
\end{proof}

An action version of STL6

**Lemma STL6-act**: \( \vdash \Diamond (\Box [F] \land \Box [G]) = (\Diamond \Box [F] \land \Diamond \Box [G]) \)
\end{proof}

**Lemma SE1**: \( \vdash \Box G \land \Diamond G \rightarrow \Diamond (\Box F \land G) \)
\end{proof}

**Lemma SE2**: \( \vdash \Box F \land \Diamond G \rightarrow \Diamond (F \land G) \)
\end{proof}

**Lemma SE3**: \( \vdash \Box F \land \Diamond G \rightarrow \Diamond (G \land F) \)
\end{proof}

**Lemma SE4**: 
\begin{enumerate}
\item Assumes \( h1 : s \models \Box F \) and \( h2 : s \models \Diamond G \) and \( h3 : \vdash \Box F \land G \rightarrow H \)
\item Shows \( s \models \Diamond H \)
\end{enumerate}
\end{proof}

**Theorem E17**: \( \vdash \Diamond \Box F \rightarrow \Box \Diamond F \)
\end{proof}

**Theorem E18**: \( \vdash \Diamond \Box F \rightarrow \Box \Diamond F \)
\end{proof}

**Theorem E19**: \( \vdash \Diamond \Box F \rightarrow \Box \Diamond \Box F \)
\end{proof}

37
**Theorem E20**: \( \vdash \Box \lozenge F \rightarrow \Box \lozenge F \)  
(\text{proof})

**Theorem E21 [simp-unl]**: \( \vdash \Box \lozenge \Box F = \lozenge \lozenge F \)  
(\text{proof})

**Theorem E27 [simp-unl]**: \( \vdash \Box \lozenge \Box F = \lozenge \Box F \)  
(\text{proof})

**Lemma E28**: \( \vdash \Box \lozenge F \land \Box \lozenge G \rightarrow \Box \lozenge (F \land G) \)  
(\text{proof})

**Lemma E23**: \( \vdash \neg \Diamond F \rightarrow \Diamond F \)  
(\text{proof})

**Lemma E24**: \( \vdash \Box \lozenge Q \rightarrow \Box \Diamond \langle A \rangle -v \)  
(\text{proof})

**Lemma E25**: \( \vdash \neg \Diamond A \rightarrow \Diamond \langle A \rangle -v \)  
(\text{proof})

**Lemma E26**: \( \vdash \Box \lozenge \langle A \rangle -v \rightarrow \Box \Diamond A \)  
(\text{proof})

**Lemma allBox**: \( (s \models \Box (\forall x. F x)) = (\forall x. s \models \Box (F x)) \)  
(\text{proof})

**Lemma E29**: \( \vdash \neg \Diamond F \rightarrow \Diamond F \)  
(\text{proof})

**Lemma E30**: \( \vdash F \rightarrow \Box F \) and \( \vdash \Diamond F \) shows \( \vdash \neg \Box \Diamond F \)  
(\text{proof})

**Lemma E31**: \( \vdash \Box (F \rightarrow \Box F) \land \Box F \rightarrow \Box \lozenge F \)  
(\text{proof})

**Lemma allActBox**: \( (s \models \Box (\forall x. F x) -v) = (\forall x. s \models \Box (F x) -v) \)  
(\text{proof})

**Theorem exEE**: \( \vdash (\exists x. \Diamond (F x)) = \Diamond (\exists x. F x) \)  
(\text{proof})

**Theorem exActE**: \( \vdash (\exists x. \Diamond (F x) -v) = \Diamond (\exists x. F x) -v \)  
(\text{proof})
5.5 Theorems about the leadsto operator

theorem LT1: ⊢ F ⇝ F
⟨proof⟩

theorem LT2: assumes h: ⊢ F → G shows ⊢ F → ♦G
⟨proof⟩

theorem LT3: assumes h: ⊢ F → G shows ⊢ F → G
⟨proof⟩

theorem LT4: ⊢ F → (F ⇝ G) → ♦G
⟨proof⟩

theorem LT5: ⊢ □(F → ♦G) → ♦F → ♦G
⟨proof⟩

theorem LT6: ⊢ ♦F → (F ⇝ G) → ♦G
⟨proof⟩

theorem LT9[simp-unl]: ⊢ □(F ⇝ G) = (F ⇝ G)
⟨proof⟩

theorem LT7: ⊢ □♦F → (F ⇝ G) → □♦G
⟨proof⟩

theorem LT8: ⊢ □♦G → (F ⇝ G)
⟨proof⟩

theorem LT13: ⊢ (F ⇝ G) → (G ⇝ H) → (F ⇝ H)
⟨proof⟩

theorem LT11: ⊢ (F ⇝ G) → (F ⇝ (G ∨ H))
⟨proof⟩

theorem LT12: ⊢ (F ⇝ H) → (F ⇝ (G ∨ H))
⟨proof⟩

theorem LT14: ⊢ ((F ∨ G) ⇝ H) → (F ⇝ H)
⟨proof⟩

theorem LT15: ⊢ ((F ∨ G) ⇝ H) → (G ⇝ H)
⟨proof⟩

theorem LT16: ⊢ (F ⇝ H) → (G ⇝ H) → ((F ∨ G) ⇝ H)
⟨proof⟩

theorem LT17: ⊢ ((F ∨ G) ⇝ H) = ((F ⇝ H) ∧ (G ⇝ H))
⟨proof⟩
\textbf{theorem LT10:}
\begin{itemize}
\item assumes $h : \vdash (F \land \neg G) \rightarrow G$
\item shows $\vdash F \rightarrow G$
\end{itemize}
\textbf{proof}\n
\begin{itemize}
\item theorem LT18: $\vdash (A \rightarrow (B \lor C)) \rightarrow (B \rightarrow D) \rightarrow (C \rightarrow D) \rightarrow (A \rightarrow D)$
\item theorem LT19: $\vdash (A \rightarrow (D \lor B)) \rightarrow (B \rightarrow D) \rightarrow (A \rightarrow D)$
\item theorem LT20: $\vdash (A \rightarrow (B \lor D)) \rightarrow (B \rightarrow D) \rightarrow (A \rightarrow D)$
\item theorem LT21: $\vdash ((\exists x. F x) \rightarrow G) = (\forall x. (F x \rightarrow G))$
\item theorem LT22: $\vdash (F \rightarrow (G \lor H)) \rightarrow \Box \neg G \rightarrow (F \rightarrow H)$
\item lemma LT23: $\vdash (\neg (P \rightarrow \diamond Q)) \rightarrow (P \rightarrow \lozenge Q)$
\item theorem LT24: $\vdash \Box I \rightarrow ((P \land I) \rightarrow Q) \rightarrow P \rightarrow Q$
\item theorem LT25[simp-und]: $\vdash (F \rightarrow \# \text{False}) = \Box \neg F$
\item lemma LT28:
\begin{itemize}
\item assumes $h : \vdash \neg P \rightarrow \circ P \lor \circ Q$
\item shows $\vdash (P \rightarrow \circ P) \lor \lozenge Q$
\end{itemize}
\item lemma LT29:
\begin{itemize}
\item assumes $h1 : \vdash \neg P \rightarrow \circ P \lor \circ Q$ \textbf{and} $h2 : \vdash \neg P \land \text{Unchanged} v \rightarrow \circ P$
\item shows $\vdash P \rightarrow \Box P \lor \lozenge Q$
\end{itemize}
\item lemma LT30:
\begin{itemize}
\item assumes $h : \vdash \neg P \land N \rightarrow \circ P \lor \circ Q$
\item shows $\vdash N \rightarrow (P \rightarrow \circ P) \lor \lozenge Q$
\end{itemize}
\item lemma LT31:
\begin{itemize}
\item assumes $h1 : \vdash \neg P \land N \rightarrow \circ P \lor \circ Q$ \textbf{and} $h2 : \vdash \neg P \land \text{Unchanged} v \rightarrow \circ P$
\item shows $\vdash \Box N \rightarrow P \rightarrow \Box P \lor \lozenge Q$
\end{itemize}
\textbf{proof}\n
40
lemma LT33: \( \vdash ((\# P \land F) \rightarrow G) = (\# P \rightarrow (F \rightarrow G)) \)
\( \langle \text{proof} \rangle \)

lemma AA1: \( \vdash \Box[\# \text{False}]-v \rightarrow \neg \Diamond\langle Q \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA2: \( \vdash \Box[P]-v \land \Diamond\langle Q \rangle-v \rightarrow \Diamond\langle P \land Q \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA3: \( \vdash \Box P \land \Box[P \rightarrow Q]-v \land \Diamond\langle A \rangle-v \rightarrow \Diamond Q \)
\( \langle \text{proof} \rangle \)

lemma AA4: \( \vdash \Diamond\langle\langle A \rangle-v\rangle-w \rightarrow \Diamond\langle\langle A \rangle-w\rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA7: assumes \( h: \neg F \rightarrow G \) shows \( \vdash \Diamond\langle F \rangle-v \rightarrow \Diamond\langle G \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA6: \( \vdash \Box[P \rightarrow Q]-v \land \Diamond\langle P \rangle-v \rightarrow \Diamond\langle Q \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA8: \( \vdash \Box[P]-v \land \Diamond\langle A \rangle-v \rightarrow \Diamond\langle \Box[P]-v \land A \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA9: \( \vdash \Box[P]-v \land \Diamond\langle A \rangle-v \rightarrow \Diamond\langle[P]-v \land A \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA10: \( \vdash \neg(\Box[P]-v \land \Diamond\langle \neg P \rangle-v) \)
\( \langle \text{proof} \rangle \)

lemma AA11: \( \vdash \neg\langle v = v \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA15: \( \vdash \Diamond\langle P \land Q \rangle-v \rightarrow \Diamond\langle P \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA16: \( \vdash \Diamond\langle P \land Q \rangle-v \rightarrow \Diamond\langle Q \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA13: \( \vdash \Diamond\langle P \rangle-v \rightarrow \Diamond\langle v \neq v \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA14: \( \vdash \Diamond\langle P \lor Q \rangle-v = (\Diamond\langle P \rangle-v \lor \Diamond\langle Q \rangle-v) \)
\( \langle \text{proof} \rangle \)

lemma AA17: \( \vdash \Diamond\langle[P]-v \land A \rangle-v \rightarrow \Diamond\langle P \land A \rangle-v \)
\( \langle \text{proof} \rangle \)

lemma AA19: \( \vdash \Box P \land \Diamond\langle A \rangle-v \rightarrow \Diamond\langle P \land A \rangle-v \)
lemma AA20:
assumes h1: \[ \sim P \rightarrow \circ P \lor \circ Q \]
and h2: \[ \sim P \land A \rightarrow \circ Q \]
and h3: \[ \sim P \land Unchanged w \rightarrow \circ P \]
shows \( \vdash \Box (\Box P \rightarrow \Diamond (A) \cdot v) \rightarrow (P \leadsto Q) \)

lemma AA21: \[ \sim \Diamond (\circ F) \cdot v \rightarrow \circ \Diamond F \]

theorem AA24[simp-unl]: \( \vdash \Diamond (\Diamond P) \cdot f = \Diamond (P) \cdot f \)

lemma AA22:
assumes h1: \[ \sim P \land N \rightarrow \circ P \lor \circ Q \]
and h2: \[ \sim P \land N \land \langle A \rangle \cdot v \rightarrow \circ Q \]
and h3: \[ \sim P \land Unchanged w \rightarrow \circ P \]
shows \( \vdash \Box N \land \Box (\Box P \rightarrow \Diamond (A) \cdot v) \rightarrow (P \leadsto Q) \)

lemma AA23:
assumes \[ \sim P \land N \rightarrow \circ P \lor \circ Q \]
and \[ \sim P \land N \land \langle A \rangle \cdot v \rightarrow \circ Q \]
and \[ \sim P \land Unchanged w \rightarrow \circ P \]
shows \( \vdash \Box N \land \Box \Diamond (A) \cdot v \rightarrow (P \leadsto Q) \)

lemma AA25:
assumes h: \[ \sim \langle P \rangle \cdot v \rightarrow \langle Q \rangle \cdot w \]
shows \( \vdash \Diamond (P) \cdot v \rightarrow \Diamond (Q) \cdot w \)

lemma AA26:
assumes h: \[ \sim \langle A \rangle \cdot v = \langle B \rangle \cdot w \]
shows \( \vdash \Diamond (A) \cdot v = \Diamond (B) \cdot w \)

theorem AA28[simp-unl]: \( \vdash \Diamond \Diamond (A) \cdot v = \Diamond (A) \cdot v \)

theorem AA29: \( \vdash \Box (\Box N \land A \land \Box A) \cdot v \rightarrow \Box (\Box N \land A) \cdot v \)

theorem AA30[simp-unl]: \( \vdash \Diamond (\Diamond (P) \cdot f) \cdot f = \Diamond (P) \cdot f \)

theorem AA31: \( \vdash \Diamond (\circ F) \cdot v \rightarrow \Diamond F \)
\begin{proof}

**Lemma AA32[\text{simp-und}]:** \( \vdash \Box \Box [A] \Rightarrow v = \Box [A] \Rightarrow v \)

\begin{proof}

**Lemma AA33[\text{simp-und}]:** \( \vdash \Box \Box (A) \Rightarrow v = \Box (A) \Rightarrow v \)

\end{proof}

\end{proof}

5.6 Lemmas about the next operator

**Lemma N2:** assumes \( h: \vdash F = G \) shows \( \lnot oF = oG \)

\begin{proof}

**Lemmas next-and \( = T8 \)**

**Lemma next-or:** \( \lnot o(F \lor G) = (oF \lor oG) \)

\begin{proof}

**Lemma next-imp:** \( \lnot o(F \rightarrow G) = (oF \rightarrow oG) \)

\end{proof}

**Lemmas next-not \( = \text{pax1} \)**

**Lemma next-eq:** \( \lnot o(F = G) = (oF = oG) \)

\begin{proof}

**Lemma next-noteq:** \( \lnot o(F \neq G) = (oF \neq oG) \)

\end{proof}

**Lemma next-const[\text{simp-und}]:** \( \lnot oP = \#P \)

\begin{proof}

The following are proved semantically because they are essentially first-order theorems.

**Lemma next-fun1:** \( \lnot o\langle x \rangle = f\langle o\langle x \rangle \rangle \)

\begin{proof}

**Lemma next-fun2:** \( \lnot o\langle x, y \rangle = f\langle o\langle x, y \rangle \rangle \)

\end{proof}

**Lemma next-fun3:** \( \lnot o\langle x, y, z \rangle = f\langle o\langle x, y, z \rangle \rangle \)

\begin{proof}

**Lemma next-fun4:** \( \lnot o\langle x, y, z, z \rangle = f\langle o\langle x, y, z, z \rangle \rangle \)

\end{proof}

**Lemma next-forall:** \( \lnot o(\forall x. P x) = (\forall x. o P x) \)

\end{proof}

43
lemma next-exists: \[ \sim \circ (\exists \, x. \ P \, x) = (\exists \, x. \circ \ P \, x) \]

⟨proof⟩

lemma next-exists1: \[ \sim \circ (\exists! \, x. \ P \, x) = (\exists! \, x. \circ \ P \, x) \]

⟨proof⟩

Rewrite rules to push the “next” operator inward over connectives. (Note that axiom pax1 and theorem next-const are anyway active as rewrite rules.)

lemmas next-commutes = next-and next-or next-imp next-eq next-fun1 next-fun2 next-fun3 next-fun4 next-forall next-exists next-exists1

lemmas ifs-eq = after-fun3 next-fun3 before-fun3

lemmas next-always = pax3

lemma t1: \[ \sim \circ x = x \circ \]

⟨proof⟩

Theorem next-eventually should not be used ”blindly”.

lemma next-eventually:

assumes h: \[ \sim \ F \]

shows \(\vdash \Box F \rightarrow \neg F \rightarrow \circ \Box F \)

⟨proof⟩

lemma next-action: \[ \sim \Box[P]-v \rightarrow \circ \Box[P]-v \]

⟨proof⟩

5.7 Higher Level Derived Rules

In most verification tasks the low-level rules discussed above are not used directly. Here, we derive some higher-level rules more suitable for verification. In particular, variants of Lamport’s rules TLA1, TLA2, INV1 and INV2 are derived, where \(\sim\) is used where appropriate.

theorem TLA1:

assumes H: \[ \sim P \land \text{Unchanged} \ f \rightarrow \circ P \]

shows \(\vdash \Box P = (P \land \Box[P]-f) \)

⟨proof⟩

theorem TLA2:

assumes h1: \(\vdash P \rightarrow Q \)

and h2: \[ \sim P \land \circ P \land [A]-f \rightarrow [B]-g \]

shows \(\vdash \Box P \land \Box[A]-f \rightarrow \Box Q \land \Box[B]-g \)

⟨proof⟩

theorem INV1:

assumes H: \[ \sim I \land [N]-f \rightarrow \circ I \]

44
shows ⊢ I ∧ □[N]-f → □I

(⟨proof⟩)

**theorem INV2:** ⊢ □I → □[N]-f = □[N ∧ I ∧ ◦I]-f

(⟨proof⟩)

**lemma R1:**
assumes H: ¬ Unchanged w → Unchanged v
shows ⊢ □[F]-w → □[F]-v

(⟨proof⟩)

**theorem invmono:**
assumes h1: ⊢ I → P
and h2: ¬ P ∧ [N]-f → ◦P
shows ⊢ I ∧ □[N]-f → □P

(⟨proof⟩)

**theorem preimpsplit:**
assumes ¬ I ∧ N → Q
and ¬ I ∧ Unchanged v → Q
shows ¬ I ∧ [N]-v → Q

(⟨proof⟩)

**theorem refinement1:**
assumes h1: ⊢ P → Q
and h2: ¬ I ∧ ◦I ∧ [A]-f → [B]-g
shows ⊢ P ∧ □I ∧ □[A]-f → Q ∧ □[B]-g

(⟨proof⟩)

**theorem inv-join:**
assumes ⊢ P → □Q and ⊢ P → □R
shows ⊢ P → □(Q ∧ R)

(⟨proof⟩)

**lemma inv-cases:** ⊢ □(A → B) ∧ □(¬A → B) → □B

(⟨proof⟩)

end

6 Liveness

**theory Liveness**

**imports** Rules

**begin**

This theory derives proof rules for liveness properties.

**definition** enabled :: 'a formula ⇒ 'a formula

**where** enabled F ≜ λ s. ∃ t. (first s) # t) ⊨ F

45
Lamport’s TLA defines the above notions for actions. In TLA∗, (pre-)formulas generalise TLA’s actions and the above definition is the natural generalisation of enabledness to pre-formulas. In particular, we have chosen to define enabled such that it yields itself a temporal formula, although its value really just depends on the first state of the sequence it is evaluated over. Then, the definitions of weak and strong fairness are exactly as in TLA.

**Syntax**
- **WF** :: \[\text{lift, lift}\] ⇒ lift ((WF′ ‘(-)-) [20,10000] 90)
- **SF** :: \[\text{lift, lift}\] ⇒ lift ((SF′ ‘(-)-) [20,10000] 90)
- **WFsp** :: \[\text{lift, lift}\] ⇒ lift ((WF ′ ‘(·)-) [20,10000] 90)
- **SFsp** :: \[\text{lift, lift}\] ⇒ lift ((SF ‘(·)-) [20,10000] 90)

**Translations**
- **WF** ⇒ CONST WeakF
- **SF** ⇒ CONST StrongF
- **WFsp** ⇒ CONST WeakF
- **SFsp** ⇒ CONST StrongF

### 6.1 Properties of **Enabled**

**Theorem** enabledI: ⊢ F ⇒ Enabled F

**Theorem** enabledE:
- assumes s ⊨ Enabled F and \( \land u. (\text{first s} ## u) \models F \Rightarrow Q \)
- shows Q

**Lemma** enabled-mono:
- assumes w ⊨ Enabled F and ⊢ F ⇒ G
- shows w ⊨ Enabled G

**Lemma** Enabled-disj1: ⊢ Enabled F ⇒ Enabled (F ∨ G)

**Lemma** Enabled-disj2: ⊢ Enabled F ⇒ Enabled (G ∨ F)
lemma Enabled-conj1: ․ Enabled (F ∧ G) → Enabled F
  ⟨proof⟩

lemma Enabled-conj2: ․ Enabled (G ∧ F) → Enabled F
  ⟨proof⟩

lemma Enabled-disjD: ․ Enabled (F ∨ G) → Enabled F ∨ Enabled G
  ⟨proof⟩

lemma Enabled-disj: ․ Enabled (F ∨ G) = (Enabled F ∨ Enabled G)
  ⟨proof⟩

lemmas enabled-disj-rew = Enabled-disj[<int-rewrite>]

lemma Enabled-ex: ․ Enabled (∃ x F x) = (∃ x Enabled (F x))
  ⟨proof⟩

6.2 Fairness Properties

lemma WF-alt: ․ WF(A)-v = (□◊¬Enabled (A)-v ∨ ◊□¬(A)-v)
  ⟨proof⟩

lemma SF-alt: ․ SF(A)-v = (◊□¬Enabled (A)-v ∨ □◊¬(A)-v)
  ⟨proof⟩

lemma alwaysWFI: ․ WF(A)-v → □WF(A)-v
  ⟨proof⟩

theorem WF-always[simp-unl]: ․ □WF(A)-v = WF(A)-v
  ⟨proof⟩

theorem WF-eventually[simp-unl]: ․ ◊WF(A)-v = WF(A)-v
  ⟨proof⟩

lemma alwaysSFI: ․ SF(A)-v → □SF(A)-v
  ⟨proof⟩

theorem SF-always[simp-unl]: ․ □SF(A)-v = SF(A)-v
  ⟨proof⟩

theorem SF-eventually[simp-unl]: ․ ◊SF(A)-v = SF(A)-v
  ⟨proof⟩

theorem SF-imp-WF: ․ SF (_A)-v → WF (_A)-v
  ⟨proof⟩

lemma enabled-WFSF: ․ □Enabled (F)-v → (WF(F)-v = SF(F)-v)
  ⟨proof⟩
theorem WF1-general:
assumes h1: \(\neg P \land N \rightarrow P \lor Q\)
and h2: \(\neg P \land (N \land \langle A \rangle \cdot v) \rightarrow Q\)
and h3: \(\vdash P \land N \rightarrow \text{Enabled} \langle A \rangle \cdot v\)
and h4: \(\neg P \land \text{Unchanged} w \rightarrow P\)
shows \(\vdash \Box N \land WF(A) \cdot v \rightarrow (P \leadsto Q)\)
⟨proof⟩

Lamport’s version of the rule is derived as a special case.

theorem WF1:
assumes h1: \(\neg P \land [N] \cdot v \rightarrow P \lor Q\)
and h2: \(\neg P \land (N \land \langle A \rangle \cdot v) \rightarrow Q\)
and h3: \(\vdash P \rightarrow \text{Enabled} \langle A \rangle \cdot v\)
and h4: \(\neg P \land \text{Unchanged} v \rightarrow P\)
shows \(\vdash \Box [N] \cdot v \land WF(A) \cdot v \rightarrow (P \leadsto Q)\)
⟨proof⟩

The corresponding rule for strong fairness has an additional hypothesis \(\Box F\), which is typically a conjunction of other fairness properties used to prove that the helpful action eventually becomes enabled.

theorem SF1-general:
assumes h1: \(\neg P \land [N] \cdot v \rightarrow P \lor Q\)
and h2: \(\neg P \land (N \land \langle A \rangle \cdot v) \rightarrow Q\)
and h3: \(\vdash \Box P \land \Box N \land \Box F \rightarrow \Diamond \text{Enabled} \langle A \rangle \cdot v\)
and h4: \(\neg P \land \text{Unchanged} w \rightarrow P\)
shows \(\vdash \Box [N] \cdot v \land SF(A) \cdot v \land \Box F \rightarrow (P \leadsto Q)\)
⟨proof⟩

theorem SF1:
assumes h1: \(\neg P \land [N] \cdot v \rightarrow P \lor Q\)
and h2: \(\neg P \land (N \land \langle A \rangle \cdot v) \rightarrow Q\)
and h3: \(\vdash \Box P \land \Box N \land \Box F \rightarrow \Diamond \text{Enabled} \langle A \rangle \cdot v\)
and h4: \(\neg P \land \text{Unchanged} v \rightarrow P\)
shows \(\vdash \Box [N] \cdot v \land SF(A) \cdot v \land \Box F \rightarrow (P \leadsto Q)\)
⟨proof⟩

Lamport proposes the following rule as an introduction rule for \(WF\) formulas.

theorem WF2:
assumes h1: \(\neg \langle N \land B \rangle \cdot f \rightarrow \langle M \rangle \cdot g\)
and h2: \(\neg P \land \circ P \land \langle N \land A \rangle \cdot f \rightarrow B\)
and h3: \(\vdash P \land \text{Enabled} \langle M \rangle \cdot g \rightarrow \text{Enabled} \langle A \rangle \cdot f\)
and h4: \(\vdash \Box [N \land \neg B] \cdot f \land WF(A) \cdot f \land \Box F \land \Diamond \text{Enabled} \langle M \rangle \cdot g \rightarrow \Diamond \Box P\)
shows \(\vdash \Box [N] \cdot f \land WF(A) \cdot f \land \Box F \rightarrow WF(M) \cdot g\)
⟨proof⟩

Lamport proposes an analogous theorem for introducing strong fairness, and
its proof is very similar, in fact, it was obtained by copy and paste, with minimal modifications.

**Theorem SF2:**

assumes $h1$: $\sim (N \land B) \rightarrow (M) \rightarrow g$

and $h2$: $\sim P \land \circ P \land (N \land A) \rightarrow B$

and $h3$: $\vdash P \land \operatorname{Enabled} (M) \rightarrow \operatorname{Enabled} (A) \rightarrow f$

and $h4$: $\vdash (N \land \neg B) \rightarrow (M) \rightarrow g$

shows $\vdash (N \land g) \land SF(A) \land g \rightarrow SF(M) \rightarrow g$

\[\langle \text{proof} \rangle\]

This is the lattice rule from TLA

**Theorem wf-leadsto:**

assumes $h1$: $\text{wf } r$

and $h2$: $\forall x. \vdash F x \leadsto (G \lor (\exists y. \#((y, x) \in r) \land F y))$

shows $\vdash F x \leadsto G$

\[\langle \text{proof} \rangle\]

### 6.3 Stuttering Invariance

**Theorem stut-Enabled:** $\text{STUTINV} \text{ Enabled } (F) - v$

\[\langle \text{proof} \rangle\]

**Theorem stut-WF:** $\text{NSTUTINV} F \implies \text{STUTINV} WF (F) - v$

\[\langle \text{proof} \rangle\]

**Theorem stut-SF:** $\text{NSTUTINV} F \implies \text{STUTINV} SF (F) - v$

\[\langle \text{proof} \rangle\]

**Lemmas** $\text{livenessinv} = \text{stut-WF} \text{ stut-SF} \text{ stut-Enabled}$

\[\text{end}\]

### 7 Representing state in TLA*

**Theory** State

**Imports** Liveness

**Begin**

We adopt the hidden state approach, as used in the existing Isabelle/HOL TLA embedding [7]. This approach is also used in [3]. Here, a state space is defined by its projections, and everything else is unknown. Thus, a variable is a projection of the state space, and has the same type as a state function. Moreover, strong typing is achieved, since the projection function may have any result type. To achieve this, the state space is represented by an undefined type, which is an instance of the world class to enable use with the Intensional theory.

**Typedecl** state
instance state :: world ⟨proof⟩

```plaintext
type-synonym 'a statefun = (state,'a) stfun
type-synonym statepred = bool statefun

type-synonym 'a tempfun = (state,'a) formfun
type-synonym temporal = state formula
```

Formalizing type state would require formulas to be tagged with their underlying state space and would result in a system that is much harder to use. (Unlike Hoare logic or Unity, TLA has quantification over state variables, and therefore one usually works with different state spaces within a single specification.) Instead, state is just an anonymous type whose only purpose is to provide Skolem constants. Moreover, we do not define a type of state variables separate from that of arbitrary state functions, again in order to simplify the definition of flexible quantification later on. Nevertheless, we need to distinguish state variables, mainly to define the enabledness of actions. The user identifies (tuples of) “base” state variables in a specification via the “meta predicate” basevars, which is defined here.

```plaintext
definition stvars :: 'a statefun ⇒ bool
where basevars-def: stvars ≡ surj
```

```plaintext
syntax PRED :: lift ⇒ 'a (PRED -
-stvars :: lift ⇒ bool (basevars -)
```

```plaintext
translations PRED P → (P::state => -) 
-stvars = CONST stvars
```

Base variables may be assigned arbitrary (type-correct) values. In the following lemma, note that `vs` may be a tuple of variables. The correct identification of base variables is up to the user who must take care not to introduce an inconsistency. For example, basevars (x, x) would definitely be inconsistent.

```plaintext
lemma basevars: basevars vs ⇒ ∃ u. vs u = c
⟨proof⟩
```

```plaintext
lemma baseE:
  assumes H1: basevars v and H2:∀ x. v x = c ⇒ Q
  shows Q
  ⟨proof⟩
```

A variant written for sequences rather than single states.

```plaintext
lemma first-baseE:
  assumes H1: basevars v and H2: ∀ x. v (first x) = c ⇒ Q
  shows Q
```

50
lemma base-pair1:
assumes \( h: \text{basevars} \ (x,y) \)
shows \( \text{basevars} \ x \)
(\proof)

lemma base-pair2:
assumes \( h: \text{basevars} \ (x,y) \)
shows \( \text{basevars} \ y \)
(\proof)

lemma base-pair: \( \text{basevars} \ (x,y) \Rightarrow \text{basevars} \ x \land \text{basevars} \ y \)
(\proof)

Since the unit type has just one value, any state function of unit type satisfies the predicate basevars. The following theorem can sometimes be useful because it gives a trivial solution for basevars premises.

lemma unit-base: \( \text{basevars} \ (v::\text{state} \Rightarrow \text{unit}) \)
(\proof)

A pair of the form \((x,x)\) will generally not satisfy the predicate basevars – except for pathological cases such as \(x::\text{unit}\).

lemma
fixes \( x :: \text{state} \Rightarrow \text{bool} \)
assumes \( h1: \text{basevars} \ (x,x) \)
shows \( \text{False} \)
(\proof)

lemma
fixes \( x :: \text{state} \Rightarrow \text{nat} \)
assumes \( h1: \text{basevars} \ (x,x) \)
shows \( \text{False} \)
(\proof)

The following theorem reduces the reasoning about the existence of a state sequence satisfying an enabledness predicate to finding a suitable value \(c\) at the successor state for the base variables of the specification. This rule is intended for reasoning about standard TLA specifications, where Enabled is applied to actions, not arbitrary pre-formulas.

lemma base-enabled:
assumes \( h1: \text{basevars} \ vs \)
and \( h2: \bigwedge u. \ vs \ (\text{first} \ u) = c \implies ((\text{first} \ s) \#\# u) \models F \)
shows \( s \models \text{Enabled} \ F \)
(\proof)
7.1 Temporal Quantifiers

In [5], Lamport gives a stuttering invariant definition of quantification over (flexible) variables. It relies on similarity of two sequences (as supported in our Sequence theory), and equivalence of two sequences up to a variable (the bound variable). However, sequence equivalence up to a variable, requires state equivalence up to a variable. Our state representation above does not support this, hence we cannot encode Lamport’s definition in our theory. Thus, we need to axiomatise quantification over (flexible) variables. Note that with a state representation supporting this, our theory should allow such an encoding.

consts
\[ EEx :: (∃x. statefun ⇒ temporal) ⇒ temporal \quad (\text{binder } Eex 10) \]
\[ AAll :: (∀x. statefun ⇒ temporal) ⇒ temporal \quad (\text{binder } Aall 10) \]

syntax
\[ EEx :: [idts, lift] ⇒ lift ((∃EEx -/-) [0,10] 10) \]
\[ AAll :: [idts, lift] ⇒ lift ((∀AAll -/-) [0,10] 10) \]

translations
\[ EEx v A == Eex v . A \]
\[ AAll v A == Aall v . A \]

syntax (xsymbols)
\[ EEx :: [idts, lift] ⇒ lift ((∃∃x. -/-) [0,10] 10) \]
\[ AAll :: [idts, lift] ⇒ lift ((∀∀x. -/-) [0,10] 10) \]

axiomatization where
\[ eexI: \vdash F x \longrightarrow (∃x. F x) \]
and \[ eexE: [s \models (∃x. F x) ; basevars vs; (!x. [basevars (x,vs); s \models F x] ⇒ s \models G)] \] \[ \longrightarrow (s \models G) \]
and \[ all-def: \vdash (∀x. F x) = (¬(∃x. ¬(F x))) \]
and \[ eexSTUT: STUTINV F x \Longrightarrow STUTINV (∃x. F x) \]
and \[ history: \vdash (I ∧ □[A]v) = (∃h. (§h = ha) ∧ I ∧ □[A ∧ h§=hb]-(h,v)) \]

lemmas \[ eexI-unl = eexI[unlift-rule] \quad w \models F x \Longrightarrow w \models (∃x. F x) \]

TLAdefs can be used to unfold TLA definitions into lowest predicate level. This is particularly useful for reasoning about enabledness of formulas.

lemmas \[ tla-defs = unch-def before-def after-def first-def second-def suffix-def \]
\[ tail-def nexts-def app-def angle-actrans-def actrans-def \]
8 A simple illustrative example

theory Even
imports State
begin

A trivial example illustrating invariant proofs in the logic, and how Isabelle/HOL can help with specification. It proves that \( x \) is always even in a program where \( x \) is initialized as 0 and always incremented by 2.

inductive-set
Even :: \( \text{nat} \rightarrow \text{set} \)
where
  even-zero: \( 0 \in \text{Even} \)
| even-step: \( n \in \text{Even} \quad \implies \quad \text{Suc}(\text{Suc} n) \in \text{Even} \)

locale Program =
  fixes \( x \) :: \( \text{state} \rightarrow \text{nat} \)
  and init :: \( \text{temporal} \)
  and act :: \( \text{temporal} \)
  and phi :: \( \text{temporal} \)
defines init \( \equiv \text{TEMP} \$x = \#\ 0 \)
and act \( \equiv \text{TEMP} \ x' = \text{Suc}<\text{Suc}\<$x$>> \)
and phi \( \equiv \text{TEMP} \ \text{init} \land \Box[\text{act}]^{-x} \)

lemma (in Program) stutinvprog: \( \text{STUTINV} \ \phi \)
  (proof)

lemma (in Program) inveven: \( \vdash \phi \quad \implies \quad \Box(\$x \in \# \text{Even}) \)
  (proof)

end

9 Lamport’s Inc example

theory Inc
imports State
begin

This example illustrates use of the embedding by mechanising the running example of Lamports original TLA paper [5].

datatype pcount = a | b | g

locale Firstprogram =
  fixes \( x \) :: \( \text{state} \rightarrow \text{nat} \)
  and \( y \) :: \( \text{state} \rightarrow \text{nat} \)
  and init :: \( \text{temporal} \)
  and m1 :: \( \text{temporal} \)
and $m_2 :: \text{temporal}$
and $\phi :: \text{temporal}$
and $\text{Live} :: \text{temporal}$
defines $\text{init} \equiv \text{TEMP } x = \# 0 \land y = \# 0$
and $m_1 \equiv \text{TEMP } x' = \text{Suc}<$x$> \land y' = y$
and $m_2 \equiv \text{TEMP } y' = \text{Suc}$<y$> \land x' = x$
and $\text{Live} \equiv \text{TEMP } \text{WF}(m_1)-(x,y) \land \text{WF}(m_2)-(x,y)$
and $\phi \equiv \text{TEMP } (\text{init} \land \square[m_1 \lor m_2]-(x,y) \land \text{Live})$
assumes bvar: basevars (x,y)

lemma (in Firstprogram) $\text{STUTINV } \phi$
(proof)

lemma (in Firstprogram) enabled-m1: $\vdash \text{Enabled } \langle m_1 \rangle-(x,y)$
(proof)

lemma (in Firstprogram) enabled-m2: $\vdash \text{Enabled } \langle m_2 \rangle-(x,y)$
(proof)

locale Secondprogram = Firstprogram +
fixes $\text{sem} :: \text{state }\Rightarrow \text{nat}$
and $\text{pc}_1 :: \text{state }\Rightarrow \text{pcount}$
and $\text{pc}_2 :: \text{state }\Rightarrow \text{pcount}$
and $\text{vars}$
and $\text{initPsi} :: \text{temporal}$
and $\text{alpha}_1 :: \text{temporal}$
and $\text{alpha}_2 :: \text{temporal}$
and $\text{beta}_1 :: \text{temporal}$
and $\text{beta}_2 :: \text{temporal}$
and $\text{gamma}_1 :: \text{temporal}$
and $\text{gamma}_2 :: \text{temporal}$
and $\text{n}_1 :: \text{temporal}$
and $\text{n}_2 :: \text{temporal}$
and $\text{Live}_2 :: \text{temporal}$
and $\text{psi} :: \text{temporal}$
and $\text{I} :: \text{temporal}$
defines $\text{vars} \equiv \text{LIFT } (x,y,\text{sem},\text{pc}_1,\text{pc}_2)$
and $\text{initPsi} \equiv \text{TEMP } p\text{c}_1 = \# a \land p\text{c}_2 = \# a \land x = \# 0 \land y = \# 0 \land$
$\text{sem} = \# 1$
and $\text{alpha}_1 \equiv \text{TEMP } p\text{c}_1 = \# a \land \# 0 < \text{sem} \land p\text{c}_1\text{\$} = \# b \land \text{sem}\$ = $\text{sem}$
$- \# 1 \land \text{Unchanged } (x,y,\text{pc}_2)$
and $\text{alpha}_2 \equiv \text{TEMP } p\text{c}_2 = \# a \land \# 0 < \text{sem} \land p\text{c}_2\text{\$} = \# b \land \text{sem}\$ = $\text{sem}$
$- \# 1 \land \text{Unchanged } (x,y,\text{pc}_1)$
and $\text{beta}_1 \equiv \text{TEMP } p\text{c}_1 = \# b \land p\text{c}_1\text{\$} = \# g \land x' = \text{Suc}$<$x$> \land \text{Unchanged } (y,\text{sem},\text{pc}_2)$
and $\text{beta}_2 \equiv \text{TEMP } p\text{c}_2 = \# b \land p\text{c}_2\text{\$} = \# g \land y' = \text{Suc}$<$y$> \land \text{Unchanged } (x,\text{sem},\text{pc}_1)$
and $\text{gamma}_1 \equiv \text{TEMP } p\text{c}_1 = \# g \land p\text{c}_1\text{\$} = \# a \land \text{sem}' = \text{Suc}$<$\text{sem}\$ \land \text{Unchanged } (x,y,\text{pc}_2)$

54
\[ \gamma_2 \equiv TEMP (pc_2 = #a, sem' = Suc < sem >) \]

\[ \text{Unchanged } (x, y, pc_1) \]

\[ \text{and } n_1 \equiv TEMP (\alpha_1 \lor \beta_1 \lor \gamma_1) \]

\[ \text{and } n_2 \equiv TEMP (\alpha_2 \lor \beta_2 \lor \gamma_2) \]

\[ \text{and } \text{Live}_2 \equiv TEMP SF(n_1) - \text{vars} \land SF(n_2) - \text{vars} \]

\[ \psi \equiv TEMP (\text{initPsi} \land \Box [n_1 \lor n_2] - \text{vars} \land \text{Live}_2) \]

\[ I \equiv TEMP (\text{initPsi} \land \Box [pc_1 = #a \land \text{pc}_2 = #a] \land \Box [pc_1 = #a \land \text{pc}_2 = \{#b, #g\}] \land \Box [pc_1 = #a \land \text{pc}_2 = \{#b, #g\}]) \]

\[ \text{assumes } bvar_2 : \text{basevars vars} \]

\[ \text{lemmas (in Secondprogram)} \quad \text{Sact}_2 - \text{defs} = n_1 - \text{def} \; n_2 - \text{def} \; \alpha_1 - \text{def} \; \beta_1 - \text{def} \; \gamma_1 - \text{def} \; \alpha_2 - \text{def} \; \beta_2 - \text{def} \; \gamma_2 - \text{def} \]

Proving invariants is the basis of every effort of system verification. We show that \( I \) is an inductive invariant of specification \( \psi \).

\[ \text{lemma (in Secondprogram)} \quad \psi I : \vdash \psi \rightarrow \Box I \]

\[ \langle \text{proof} \rangle \]

Using this invariant we now prove step simulation, i.e. the safety part of the refinement proof.

\[ \text{theorem (in Secondprogram)} \quad \text{step-simulation: } \vdash \psi \rightarrow \text{init} \land \Box [m_1 \lor m_2] - \langle \text{x, y} \rangle \]

\[ \langle \text{proof} \rangle \]

Liveness proofs require computing the enabledness conditions of actions. The first lemma below shows that all steps are visible, i.e. they change at least one variable.

\[ \text{lemma (in Secondprogram)} \quad \text{n1-ch: } \vdash \sim \langle n_1 \rangle - \text{vars} = n_1 \]

\[ \langle \text{proof} \rangle \]

\[ \text{lemma (in Secondprogram)} \quad \text{enab-alpha1: } \vdash \text{pc}_1 = #a \rightarrow \# 0 < \text{sem} \rightarrow \text{Enabled alpha1} \]

\[ \langle \text{proof} \rangle \]

\[ \text{lemma (in Secondprogram)} \quad \text{enab-beta1: } \vdash \text{pc}_1 = #b \rightarrow \text{Enabled beta1} \]

\[ \langle \text{proof} \rangle \]

\[ \text{lemma (in Secondprogram)} \quad \text{enab-gamma1: } \vdash \text{pc}_1 = #g \rightarrow \text{Enabled gamma1} \]

\[ \langle \text{proof} \rangle \]

\[ \text{lemma (in Secondprogram)} \quad \text{enab-n1: } \vdash \text{Enabled } \langle n_1 \rangle - \text{vars} = (\text{pc}_1 = #a \rightarrow \# 0 < \text{sem}) \]

\[ \langle \text{proof} \rangle \]

The analogous properties for the second process are obtained by copy and paste.

\[ \text{lemma (in Secondprogram)} \quad \text{n2-ch: } \vdash \sim \langle n_2 \rangle - \text{vars} = n_2 \]

\[ \langle \text{proof} \rangle \]

55
lemma (in Secondprogram) enab-alpha2: \( \vdash \#_pc2 = \#_a \rightarrow \#_0 < \#_sem \rightarrow \text{Enabled alpha2} \)

(\text{proof})

lemma (in Secondprogram) enab-beta2: \( \vdash \#_pc2 = \#_b \rightarrow \text{Enabled beta2} \)

(\text{proof})

lemma (in Secondprogram) enab-gamma2: \( \vdash \#_pc2 = \#_g \rightarrow \text{Enabled gamma2} \)

(\text{proof})

lemma (in Secondprogram) enab-n2:
\( \vdash \text{Enabled (n2)-vars = (}\#_pc2 = \#_a \rightarrow \#_0 < \#_sem) \)

(\text{proof})

We use rule SF2 to prove that psi implements strong fairness for the abstract action m1. Since strong fairness implies weak fairness, it follows that psi refines the liveness condition of phi.

lemma (in Secondprogram) psi-fair-m1: \( \vdash \text{psi} \rightarrow \text{SF}(m1)-(x,y) \)

(\text{proof})

In the same way we prove that psi implements strong fairness for the abstract action m1. The proof is obtained by copy and paste from the previous one.

lemma (in Secondprogram) psi-fair-m2: \( \vdash \text{psi} \rightarrow \text{SF}(m2)-(x,y) \)

(\text{proof})

We can now prove the main theorem, which states that psi implements phi.

theorem (in Secondprogram) impl: \( \vdash \text{psi} \rightarrow \text{phi} \)

(\text{proof})

end

10 Refining a Buffer Specification

theory Buffer
imports State
begin

We specify a simple FIFO buffer and prove that two FIFO buffers in a row implement a FIFO buffer.

10.1 Buffer specification

The following definitions all take three parameters: a state function representing the input channel of the FIFO buffer, another representing the internal queue, and a third one representing the output channel. These parameters will be instantiated later in the definition of the double FIFO.
definition $\text{BInit}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{BInit ic q oc} \equiv \text{TEMP } q = \#[]$
       $\land \text{ic} = \text{oc}$ — initial condition of buffer

definition $\text{Enq}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{Enq ic q oc} \equiv \text{TEMP } q \neq \text{ic}$
       $\land \text{q} = \text{q} \hat{\circ} [\text{ic}]$
       $\land \text{oc} = \text{oc}$ — enqueue a new value

definition $\text{Deq}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{Deq ic q oc} \equiv \text{TEMP } \# 0 < \text{length q} < \text{oc} = \text{hd q}$
       $\land \text{q} = \text{tl q}$
       $\land \text{ic} = \text{ic}$ — dequeue value at front

definition $\text{Nxt}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{Nxt ic q oc} \equiv \text{TEMP } (\text{Enq ic q oc} \lor \text{Deq ic q oc})$
       — internal specification with buffer visible

definition $\text{ISpec}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{ISpec ic q oc} \equiv \text{TEMP } \text{BInit ic q oc}$
       $\land \square [\text{Nxt ic q oc}] - (\text{ic,q,oc})$
       $\land \text{WF(Deq ic q oc) - (ic,q,oc)}$
       — external specification: buffer hidden

definition $\text{Spec}$ :: 'a statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where $\text{Spec ic oc} == \text{TEMP } (\text{EEX q. ISpec ic q oc})$

10.2 Properties of the buffer

The buffer never enqueues the same element twice. We therefore have the
following invariant:

- any two subsequent elements in the queue are different, and the last
  element in the queue is different from the value of the output channel,

- if the queue is non-empty then the last element in the queue is the
  value that appears on the input channel,

- if the queue is empty then the values on the output and input channels
  are equal.

The following auxiliary predicate $\text{noreps}$ is true if no two subsequent
elements in a list are identical.

definition $\text{noreps}$ :: 'a list $\Rightarrow$ bool
where $\text{noreps } xs \equiv \forall i < \text{length } xs - 1. \text{xs}!i \neq \text{xs}!(\text{Suc } i)$

definition $\text{BInv}$ :: 'a statefun $\Rightarrow$ 'a list statefun $\Rightarrow$ 'a statefun $\Rightarrow$ temporal
where \( BInv ic q oc \equiv TEMP \text{List.last}<\$oc \# \$q> = \$ic \land \text{noreps}<\$oc \# \$q> \)

**lemmas** buffer-defs = BInit-def Enq-def Deq-def Nxt-def ISpec-def Spec-def BInv-def

**lemma** ISpec-stutinv: \( STUTINV \ (ISpec ic q oc) \)
\( \langle \text{proof} \rangle \)

**lemma** Spec-stutinv: \( STUTINV \ Spec ic oc \)
\( \langle \text{proof} \rangle \)

A lemma about lists that is useful in the following

**lemma** tl-self-iff-empty[simp]: \((tl \; xs = xs) = (xs = [])\)
\( \langle \text{proof} \rangle \)

**lemma** tl-self-iff-empty′[simp]: \((xs = tl \; xs) = (xs = [])\)
\( \langle \text{proof} \rangle \)

**lemma** Deq-visible:

* assumes \( v: \vdash \text{Unchanged} \; v \longrightarrow \text{Unchanged} \; q \)

* shows \( \sim <\text{Deq} \; ic \; q \; oc>-v = \text{Deq} \; ic \; q \; oc \)
\( \langle \text{proof} \rangle \)

**lemma** Deq-enabledE: \( \vdash \text{Enabled} <\text{Deq} \; ic \; q \; oc>-(ic,q,oc) \longrightarrow \$q \sim = \#[] \)
\( \langle \text{proof} \rangle \)

We now prove that \( BInv \) is an invariant of the Buffer specification.
We need several lemmas about \text{noreps} that are used in the invariant proof.

**lemma** noreps-empty [simp]: \( \text{noreps} [] \)
\( \langle \text{proof} \rangle \)

**lemma** noreps-singleton: \( \text{noreps} [x] \) — special case of following lemma
\( \langle \text{proof} \rangle \)

**lemma** noreps-cons [simp]:
\( \text{noreps} \; (x \neq xs) = (\text{noreps} \; xs \land (xs = [] \lor x \neq hd \; xs)) \)
\( \langle \text{proof} \rangle \)

**lemma** noreps-append [simp]:
\( \text{noreps} \; (xs \# ys) = (\text{noreps} \; xs \land \text{noreps} \; ys \land (xs = [] \lor ys = [] \lor \text{List.last} \; xs \neq hd \; ys)) \)
\( \langle \text{proof} \rangle \)

**lemma** ISpec-BInv-lemma:

\( \vdash BInit ic q oc \land \Box[Nxt ic q oc]-(ic,q,oc) \longrightarrow \Box(BInv ic q oc) \)
\( \langle \text{proof} \rangle \)

**theorem** ISpec-BInv: \( \vdash ISpec ic q oc \longrightarrow \Box(BInv ic q oc) \)
\( \langle \text{proof} \rangle \)
10.3 Two FIFO buffers in a row implement a buffer

locale DBuffer =
fixes inp :: 'a statefun — input channel for double FIFO
  and mid :: 'a statefun — channel linking the two buffers
  and out :: 'a statefun — output channel for double FIFO
  and q1 :: 'a list statefun — inner queue of first FIFO
  and q2 :: 'a list statefun — inner queue of second FIFO
  and vars
defines vars ≡ LIFT (inp,mid,out,q1,q2)
assumes DB-base: basevars vars

begin

We need to specify the behavior of two FIFO buffers in a row. Intuitively, that specification is just the conjunction of two buffer specifications, where the first buffer has input channel inp and output channel mid whereas the second one receives from mid and outputs on out. However, this conjunction allows a simultaneous enqueue action of the first buffer and dequeue of the second one. It would not implement the previous buffer specification, which excludes such simultaneous enqueueing and dequeueing (it is written in “interleaving style”). We could relax the specification of the FIFO buffer above, which is esthetically pleasant, but non-interleaving specifications are usually hard to get right and to understand. We therefore impose an interleaving constraint on the specification of the double buffer, which requires that enqueueing and dequeueing do not happen simultaneously.

definition DBSpec
where DBSpec ≡ TEMP ISpec inp q1 mid
   ∧ ISpec mid q2 out
   ∧ □[¬(Enq inp q1 mid ∧ Deq mid q2 out)]-vars

The proof rules of TLA are geared towards specifications of the form Init ∧ □[Next]-vars ∧ L, and we prove that DBSpec corresponds to a specification in this form, which we now define.

definition FullInit
where FullInit ≡ TEMP (BInit inp q1 mid ∧ BInit mid q2 out)

definition FullNxt
where FullNxt ≡ TEMP (Enq inp q1 mid ∧ Unchanged (q2,out)
   ∨ Deq inp q1 mid ∧ Enq mid q2 out
   ∨ Deq mid q2 out ∧ Unchanged (inp,q1))

definition FullSpec
where FullSpec ≡ TEMP FullInit
   ∧ □[FullNxt]-vars
   ∧ WF(Deq inp q1 mid)-vars
   ∧ WF(Deq mid q2 out)-vars

The concatenation of the two queues will serve as the refinement mapping.
**definition** \( \text{qc} :: \{ \text{a list statefun} \} \)

**where** \( \text{qc} \equiv \text{LIFT} \ (q2 \ @ \ q1) \)

**lemmas** \( db-defs = \text{buffer-defs DBSpec-def FullInit-def FullNxt-def FullSpec-def qc-def vars-def} \)

**lemma** \( DBSpec\text{-statinv}: \text{STUTINV DBSpec} \)

**lemma** \( FullSpec\text{-statinv}: \text{STUTINV FullSpec} \)

We prove that \( DBSpec \) implies \( FullSpec \). (The converse implication also holds but is not needed for our implementation proof.)

The following lemma is somewhat more bureaucratic than we'd like it to be. It shows that the conjunction of the next-state relations, together with the invariant for the first queue, implies the full next-state relation of the combined queues.

**lemma** \( DBNxt\text{-then-FullNxt}: \)

\[ \vdash \Box \text{BInv inp q1 mid} \]
\[ \land \Box [\text{Nxt inp q1 mid}] -(\text{inp,q1,mid}) \]
\[ \land \Box [\text{Nxt mid q2 out}] -(\text{mid,q2,out}) \]
\[ \land \Box [\neg (\text{Enq inp q1 mid} \land \text{Deq mid q2 out})]\text{-vars} \]
\[ \rightarrow \Box [\text{FullNxt}]\text{-vars} \]

\( \text{(is} \vdash \Box \Box \text{?inv} \land \text{?nxts} \rightarrow \Box [\text{FullNxt}]\text{-vars}) \)

**lemma** \( FullInit: \vdash FullInit \rightarrow BInit inp qc out \)

It is now easy to show that \( DBSpec \) refines \( FullSpec \).

**theorem** \( DBSpec\text{-impl-FullSpec}: \vdash DBSpec \rightarrow FullSpec \)

We now prove that two FIFO buffers in a row (as specified by formula \( FullSpec \)) implement a FIFO buffer whose internal queue is the concatenation of the two buffers. We start by proving step simulation.

**lemma** \( FullInit: \vdash FullInit \rightarrow BInit inp qc out \)

**lemma** \( Full-step-simulation: \)

\[ \vdash [\text{FullNxt}]\text{-vars} \rightarrow [\text{Nxt inp qc out}] -(\text{inp,qc,out}) \]

The liveness condition requires that the combined buffer eventually performs a \( \text{Deq} \) action on the output channel if it contains some element. The idea is to use the fairness hypothesis for the first buffer to prove that in that case, eventually the queue of the second buffer will be non-empty, and that it must therefore eventually dequeue some element.
The first step is to establish the enabledness conditions for the two \textit{Deq} actions of the implementation.

\textbf{lemma} \textit{Deq1-enabled}: \[\vdash \text{Enabled} \langle \text{Deq \, inp \, q1 \, mid} \rangle \text{-vars} = (q1 \neq \#\)]

\textbf{lemma} \textit{Deq2-enabled}: \[\vdash \text{Enabled} \langle \text{Deq \, mid \, q2 \, out} \rangle \text{-vars} = (q2 \neq \#\)]

We now use rule \textit{WF2} to prove that the combined buffer (behaving according to specification \textit{FullSpec}) implements the fairness condition of the single buffer under the refinement mapping.

\textbf{lemma} \textit{Full-fairness}:
\[\vdash \Box [\text{FullNxt}]-\text{vars} \land \text{WF}(\text{Deq \, mid \, q2 \, out})-\text{vars} \land \Box \text{WF}(\text{Deq \, inp \, q1 \, mid})-\text{vars} \rightarrow \text{WF}(\text{Deq \, inp \, qc \, out}-(\text{inp,qc,out}))\)

Putting everything together, we obtain that \textit{FullSpec} refines the Buffer specification under the refinement mapping.

\textbf{theorem} \textit{FullSpec-impl-ISpec}: \[\vdash \text{FullSpec} \rightarrow \text{ISpec \, inp \, qc \, out}\]

\textbf{theorem} \textit{FullSpec-impl-Spec}: \[\vdash \text{FullSpec} \rightarrow \text{Spec \, inp \, out}\]

By transitivity, two buffers in a row also implement a single buffer.

\textbf{theorem} \textit{DBSpec-impl-Spec}: \[\vdash \text{DBSpec} \rightarrow \text{Spec \, inp \, out}\]

\textbf{References}


