MODULE *Quicksort*

This module contains an abstract version of the *Quicksort* algorithm. If you are not already familiar with that algorithm, you should look it up on the Web and understand how it works–including what the partition procedure does, without worrying about how it does it. The version presented here does not specify a partition procedure, but chooses in a single step an arbitrary value that is the result that any partition procedure may produce.

The module also has a structured informal proof of *Quicksort*'s partial correctness property–namely, that if it terminates, it produces a sorted permutation of the original sequence. As described in the note "Proving Safety Properties", the proof uses the *TLAPS* proof system to check the decomposition of the proof into substeps, and to check some of the substeps whose proofs are trivial.

The version of *Quicksort* described here sorts a finite sequence of integers. It is one of the examples in Section 7.3 of "Proving Safety Properties", which is at

http://*lamport.azurewebsites.net*/tla/proving-*safety.pdf*

EXTENDS *Integers*, *Sequences*, *FiniteSets*, *TLAPS*, *SequenceTheorems*, *FiniteSetTheorems*

This statement imports some standard modules, including ones used by the *TLAPS* proof system.

To aid in model checking the spec, we assume that the sequence to be sorted are elements of a set *Values* of integers.

CONSTANT *Values*

ASSUME $ValAssump \triangleq Values \subseteq Int$

We define $PermsOf(s)$ to be the set of permutations of a sequence s of integers. In TLA+, a sequence is a function whose domain is the set $1 \,..\, Len(s)$. A permutation of s is the composition of s with a permutation of its domain. It is defined as follows, where:

- $Automorphisms(S)$ is the set of all permutations of S, if S is a finite set–that is all functions f from S to S such that every element y of S is the image of some element of S under f.
- $f ** g$ is defined to be the composition of the functions f and g.

In TLA+, DOMAIN f is the domain of a function f.

$$Automorphisms(S) \triangleq \{f \in [S \to S] : \forall y \in S : \exists x \in S : f[x] = y\}$$

$$f ** g \triangleq [x \in \text{DOMAIN } g \mapsto f[g[x]]]$$

$$PermsOf(s) \triangleq \{s ** f : f \in Automorphisms(\text{DOMAIN } s)\}$$

LEMMA $AutomorphismsCompose \triangleq$
    ASSUME NEW S, NEW $f \in Automorphisms(S)$, NEW $g \in Automorphisms(S)$
    PROVE $f ** g \in Automorphisms(S)$
BY DEF *Automorphisms*, $**$

LEMMA $PermsOfLemma \triangleq$
    ASSUME NEW T, NEW $s \in Seq(T)$, NEW $t \in PermsOf(s)$
    PROVE $\land\ t \in Seq(T)$
    $\land\ Len(t) = Len(s)$

$\land \forall i \in 1 \, .. \, Len(s) : \exists j \in 1 \, .. \, Len(s) : t[i] = s[j]$
$\land \forall i \in 1 \, .. \, Len(s) : \exists j \in 1 \, .. \, Len(t) : t[j] = s[i]$
BY DOMAIN $t =$ DOMAIN s DEF $PermsOf$, $Automorphisms$, $**$

LEMMA $PermsOfPermsOf \triangleq$
ASSUME NEW T, NEW $s \in Seq(T)$, NEW $t \in PermsOf(s)$, NEW $u \in PermsOf(t)$
PROVE $u \in PermsOf(s)$
$\langle 1 \rangle 1.$ PICK $f \in Automorphisms($DOMAIN $s) : t = s ** f$
BY DEF $PermsOf$
$\langle 1 \rangle 2.$ PICK $g \in Automorphisms($DOMAIN $t) : u = t ** g$
BY DEF $PermsOf$
$\langle 1 \rangle 3.$ DOMAIN $t =$ DOMAIN s
BY $PermsOfLemma$
$\langle 1 \rangle 4.$ $f ** g \in Automorphisms($DOMAIN $s)$
BY $\langle 1 \rangle 3$, $AutomorphismsCompose$
$\langle 1 \rangle 5.$ $u = s ** (f ** g)$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $Zenon$ DEF $Automorphisms$, $**$
$\langle 1 \rangle$.QED BY $\langle 1 \rangle 4$, $\langle 1 \rangle 5$ DEF $PermsOf$

We define $Max(S)$ and $Min(S)$ to be the maximum and minimum, respectively, of a finite, nonempty set S of integers.

$Max(S) \triangleq$ CHOOSE $x \in S : \forall y \in S : x \geq y$
$Min(S) \triangleq$ CHOOSE $x \in S : \forall y \in S : x \leq y$

LEMMA $MinIsMin \triangleq$
ASSUME NEW $S \in$ SUBSET Int, NEW $x \in S$, $\forall y \in S : x \leq y$
PROVE $x = Min(S)$
BY DEF Min

LEMMA $MaxIsMax \triangleq$
ASSUME NEW $S \in$ SUBSET Int, NEW $x \in S$, $\forall y \in S : x \geq y$
PROVE $x = Max(S)$
BY DEF Max

LEMMA $NonemptyMin \triangleq$
ASSUME NEW $S \in$ SUBSET Int, $IsFiniteSet(S)$, NEW $x \in S$
PROVE $\land Min(S) \in S$
$\land Min(S) \leq x$
$\langle 1 \rangle$.DEFINE $P(T) \triangleq T \in$ SUBSET $Int \Rightarrow$
$\land T \neq \{\} \Rightarrow Min(T) \in T$
$\land \forall x \in T : Min(T) \leq x$
$\langle 1 \rangle 1.$ $P(\{\})$
OBVIOUS
$\langle 1 \rangle 2.$ ASSUME NEW T, NEW x, $x \notin T$, $P(T)$
PROVE $P(T \cup \{x\})$
$\langle 2 \rangle$.HAVE $T \cup \{x\} \in$ SUBSET Int

$\langle 2\rangle$1.CASE $T = \{\}$
$\langle 3\rangle$1. $x = \mathit{Min}(T \cup \{x\})$
BY $\langle 2\rangle$1 DEF Min
$\langle 3\rangle$.QED BY $\langle 2\rangle$1, $\langle 3\rangle$1
$\langle 2\rangle$2.CASE $T \neq \{\}$
$\langle 3\rangle$1.CASE $x < \mathit{Min}(T)$
$\langle 4\rangle$1. $\land\, x \in T \cup \{x\}$
$\land\, \forall\, y \in T \cup \{x\} : x \leq y$
BY $\langle 1\rangle$2, $\langle 3\rangle$1
$\langle 4\rangle$2. $x = \mathit{Min}(T \cup \{x\})$
BY $\langle 4\rangle$1 DEF Min
$\langle 4\rangle$.QED BY $\langle 4\rangle$1, $\langle 4\rangle$2
$\langle 3\rangle$2.CASE $\neg(x < \mathit{Min}(T))$
$\langle 4\rangle$.DEFINE $\mathit{mn} \triangleq \mathit{Min}(T)$
$\langle 4\rangle$1. $\land\, \mathit{mn} \in T \cup \{x\}$
$\land\, \forall\, y \in T \cup \{x\} : \mathit{mn} \leq y$
BY $\langle 1\rangle$2, $\langle 2\rangle$2, $\langle 3\rangle$2
$\langle 4\rangle$.HIDE DEF mn
$\langle 4\rangle$2. $\mathit{mn} = \mathit{Min}(T \cup \{x\})$
BY $\langle 4\rangle$1 DEF Min
$\langle 4\rangle$.QED BY $\langle 4\rangle$1, $\langle 4\rangle$2
$\langle 3\rangle$.QED BY $\langle 3\rangle$1, $\langle 3\rangle$2
$\langle 2\rangle$.QED BY $\langle 2\rangle$1, $\langle 2\rangle$2
$\langle 1\rangle$3. $\forall\, T : \mathit{IsFiniteSet}(T) \Rightarrow P(T)$
$\langle 2\rangle$.HIDE DEF P
$\langle 2\rangle$.QED BY $\langle 1\rangle$1, $\langle 1\rangle$2, $\mathit{FS\_Induction}$, IsaM("blast")
$\langle 1\rangle$.QED BY $\langle 1\rangle$3

LEMMA $\mathit{NonemptyMax} \triangleq$
ASSUME NEW $S \in$ SUBSET Int, $\mathit{IsFiniteSet}(S)$, NEW $x \in S$
PROVE $\land\, \mathit{Max}(S) \in S$
$\land\, x \leq \mathit{Max}(S)$
$\langle 1\rangle$.DEFINE $P(T) \triangleq T \in$ SUBSET $\mathit{Int} \Rightarrow$
$\land\, T \neq \{\} \Rightarrow \mathit{Max}(T) \in T$
$\land\, \forall\, x \in T : x \leq \mathit{Max}(T)$
$\langle 1\rangle$1. $P(\{\})$
OBVIOUS
$\langle 1\rangle$2. ASSUME NEW T, NEW x, $x \notin T$, $P(T)$
PROVE $P(T \cup \{x\})$
$\langle 2\rangle$.HAVE $T \cup \{x\} \in$ SUBSET Int
$\langle 2\rangle$1.CASE $T = \{\}$
$\langle 3\rangle$1. $x = \mathit{Max}(T \cup \{x\})$
BY $\langle 2\rangle$1 DEF Max
$\langle 3\rangle$.QED BY $\langle 2\rangle$1, $\langle 3\rangle$1
$\langle 2\rangle$2.CASE $T \neq \{\}$

$\langle 3 \rangle 1.$CASE $x > Max(T)$
  $\langle 4 \rangle 1.\ \land\ x \in T \cup \{x\}$
  $\quad \land\ \forall\, y \in T \cup \{x\} : x \geq y$
  BY $\langle 1 \rangle 2$, $\langle 3 \rangle 1$
  $\langle 4 \rangle 2.\ x = Max(T \cup \{x\})$
  BY $\langle 4 \rangle 1$ DEF Max
  $\langle 4 \rangle.$QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$
$\langle 3 \rangle 2.$CASE $\neg(x > Max(T))$
  $\langle 4 \rangle.$DEFINE $mx \triangleq Max(T)$
  $\langle 4 \rangle 1.\ \land\ mx \in T \cup \{x\}$
  $\quad \land\ \forall\, y \in T \cup \{x\} : y \leq mx$
  BY $\langle 1 \rangle 2$, $\langle 2 \rangle 2$, $\langle 3 \rangle 2$
  $\langle 4 \rangle.$HIDE DEF mx
  $\langle 4 \rangle 2.\ mx = Max(T \cup \{x\})$
  BY $\langle 4 \rangle 1$ DEF Max
  $\langle 4 \rangle.$QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$
$\langle 3 \rangle.$QED BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$
$\langle 2 \rangle.$QED BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$
$\langle 1 \rangle 3.\ \forall\, T : IsFiniteSet(T) \Rightarrow P(T)$
  $\langle 2 \rangle.$HIDE DEF P
  $\langle 2 \rangle.$QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $FS\_Induction$, $IsaM($"blast"$)$
$\langle 1 \rangle.$QED BY $\langle 1 \rangle 3$

LEMMA $IntervalMinMax \triangleq$
  ASSUME NEW $i \in Int$, NEW $j \in Int$, $i \leq j$
  PROVE $i = Min(i \,..\, j) \land j = Max(i \,..\, j)$
BY DEF Min, Max

The operator *Partitions* is defined so that if I is an interval that's a subset of $1 \,..\, Len(s)$ and $p \in Min(I) \,..\, Max(I) - 1$, the $Partitions(I, p, seq)$ is the set of all new values of sequence *seq* that a partition procedure is allowed to produce for the subinterval I using the pivot index p. That is, it's the set of all permutations of *seq* that leaves $seq[i]$ unchanged if i is not in I and permutes the values of $seq[i]$ for i in I so that the values for $i \leq p$ are less than or equal to the values for $i > p$.

$Partitions(I, p, s) \triangleq$
  $\{t \in PermsOf(s) :$
  $\quad \land\ \forall\, i \in (1 \,..\, Len(s)) \setminus I : t[i] = s[i]$
  $\quad \land\ \forall\, i \in I : \exists\, j \in I : t[i] = s[j]$
  $\quad \land\ \forall\, i, j \in I : (i \leq p) \land (p < j) \Rightarrow (t[i] \leq t[j])\}$

LEMMA $PartitionsLemma \triangleq$
  ASSUME NEW T, NEW $s \in Seq(T)$, NEW $I \in$ SUBSET $(1 \,..\, Len(s))$,
  NEW $p \in I$, NEW $t \in Partitions(I, p, s)$
  PROVE $\land\ t \in Seq(T)$
  $\quad \land\ Len(t) = Len(s)$
  $\quad \land\ \forall\, i \in (1 \,..\, Len(s)) \setminus I : t[i] = s[i]$
  $\quad \land\ \forall\, i \in I : \exists\, j \in I : t[i] = s[j]$

$\wedge \forall i, j \in I : i \leq p \wedge p < j \Rightarrow t[i] \leq t[j]$
BY *PermsOfLemma* DEF *Partitions*

Our algorithm has three variables:

- *seq* : The array to be sorted.
- *seq*0 : Holds the initial value of *seq*, for checking the result.
- U : A set of intervals that are subsets of $1 \mathrel{..} Len(seq0)$, an interval being a nonempty set I of integers that equals $Min(I) \mathrel{..} Max(I)$. Initially, U equals the set containing just the single interval consisting of the entire set $1 \mathrel{..} Len(seq0)$.

The algorithm repeatedly does the following:

- Chose an arbitrary interval I in U.
- If I consists of a single element, remove I from U.
- Otherwise :
  - Let $I1$ be an initial interval of I and $I2$ be the rest of I.
  - Let *newseq* be an array that's the same as *seq* except that the elements $seq[x]$ with x in I are permuted so that $newseq[y] \leq newseq[z]$ for any y in $I1$ and z in $I2$.
  - Set *seq* to *newseq*.
  - Remove I from U and add $I1$ and $I2$ to U.

It stops when U is empty. Below is the algorithm written in *PlusCal*.

```
*************************************************************************
--fair algorithm Quicksort{
  variables  seq ∈ Seq(Values) \ {⟨⟩}, seq0 = seq,   U = {1 .. Len(seq)} ;
  { a: while ( U ≠ {} )
        { with ( I ∈ U )
            { if ( Cardinality(I) = 1 )
                { U := U \ {I} }
              else
                { with ( p ∈ Min(I) .. (Max(I) − 1),
                         I1 = Min(I) .. p,
                         I2 = (p + 1) .. Max(I),
                         newseq ∈ Partitions(I, p, seq) )
                    { seq := newseq ;
                      U := (U \ {I}) ∪ {I1, I2} }      }    }    }    }    }
*************************************************************************
```

Below is the TLA+ translation of the *PlusCal* code.

BEGIN TRANSLATION

VARIABLES *seq*, *seq*0, U, *pc*

$vars \triangleq \langle seq, seq0, U, pc \rangle$

$Init \triangleq$ Global variables
$\quad \wedge seq \in Seq(Values) \setminus \{\langle\rangle\}$

$$
\begin{array}{l}
\quad\quad\land\ seq0 = seq \\
\quad\quad\land\ U = \{1 \,..\, Len(seq)\} \\
\quad\quad\land\ pc = \text{"a"}
\end{array}
$$

$$
\begin{array}{l}
a \triangleq \land\ pc = \text{"a"} \\
\quad\quad \land\ \text{IF } U \neq \{\} \\
\quad\quad\quad \text{THEN } \land\ \exists\, I \in U : \\
\quad\quad\quad\quad\quad \text{IF } Cardinality(I) = 1 \\
\quad\quad\quad\quad\quad\quad \text{THEN } \land\ U' = U \setminus \{I\} \\
\quad\quad\quad\quad\quad\quad\quad\quad \land\ seq' = seq \\
\quad\quad\quad\quad\quad\quad \text{ELSE } \land\ \exists\, p \in Min(I) \,..\, (Max(I) - 1) : \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \text{LET } I1 \triangleq Min(I) \,..\, p \text{IN} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \text{LET } I2 \triangleq (p+1) \,..\, Max(I) \text{IN} \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \exists\, newseq \in Partitions(I,\, p,\, seq) : \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\ seq' = newseq \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\ U' = ((U \setminus \{I\}) \cup \{I1,\, I2\}) \\
\quad\quad\quad\quad\quad\quad \land\ pc' = \text{"a"} \\
\quad\quad\quad \text{ELSE } \land\ pc' = \text{"Done"} \\
\quad\quad\quad\quad\quad\quad \land\ \text{UNCHANGED } \langle seq,\, U\rangle \\
\quad\quad \land\ seq0' = seq0
\end{array}
$$

Allow infinite stuttering to prevent deadlock on termination.

$$Terminating \triangleq pc = \text{"Done"} \land \text{UNCHANGED } vars$$

$$
\begin{array}{l}
Next \triangleq a \\
\quad\quad\quad \lor\ Terminating
\end{array}
$$

$$
\begin{array}{l}
Spec \triangleq \land\ Init \land \Box[Next]_{vars} \\
\quad\quad\quad \land\ \mathrm{WF}_{vars}(Next)
\end{array}
$$

$$Termination \triangleq \Diamond(pc = \text{"Done"})$$

END TRANSLATION

PCorrect is the postcondition invariant that the algorithm should satisfy. You can use *TLC* to check this for a model in which $Seq(S)$ is redefined to equal the set of sequences of at elements in S with length at most 4. A little thought shows that it then suffices to let *Values* be a set of 4 integers.

$$
\begin{array}{l}
PCorrect \triangleq (pc = \text{"Done"}) \Rightarrow \\
\quad\quad\quad\quad \land\ seq \in PermsOf(seq0) \\
\quad\quad\quad\quad \land\ \forall\, p,\, q \in 1 \,..\, Len(seq) : p < q \Rightarrow seq[p] \leq seq[q]
\end{array}
$$

Below are some definitions leading up to the definition of the inductive invariant *Inv* used to prove the postcondition *PCorrect*. The partial TLA+ proof follows. As explained in "Proving Safety Properties", you can use *TLC* to check the level $- \langle 1 \rangle$ proof steps. *TLC* can do those checks on a model in which all sequences have length at most 3.

$$UV \triangleq U \cup \{\{i\} : i \in 1 \,..\, Len(seq) \setminus \text{UNION } U\}$$

$$
\begin{array}{l}
\mathit{DomainPartitions} \triangleq \{\mathit{DP} \in \textsc{subset subset } (1 \mathrel{..} \mathit{Len}(\mathit{seq}0)) : \\
\quad \land (\textsc{union } \mathit{DP}) = 1 \mathrel{..} \mathit{Len}(\mathit{seq}0) \\
\quad \land \forall I \in \mathit{DP} : I = \mathit{Min}(I) \mathrel{..} \mathit{Max}(I) \\
\quad \land \forall I \in \mathit{DP} : \exists\, \mathit{mn}, \mathit{mx} \in 1 \mathrel{..} \mathit{Len}(\mathit{seq}0) : I = \mathit{mn} \mathrel{..} \mathit{mx} \\
\quad \land \forall I, J \in \mathit{DP} : (I \neq J) \Rightarrow (I \cap J = \{\})\}
\end{array}
$$

$$
\mathit{RelSorted}(I, J) \triangleq \forall i \in I, j \in J : (i < j) \Rightarrow (\mathit{seq}[i] \leq \mathit{seq}[j])
$$

$$
\begin{array}{l}
\mathit{TypeOK} \triangleq \land \mathit{seq} \in \mathit{Seq}(\mathit{Values}) \setminus \{\langle\rangle\} \\
\qquad\quad \land \mathit{seq}0 \in \mathit{Seq}(\mathit{Values}) \setminus \{\langle\rangle\} \\
\qquad\quad \land U \in \textsc{subset } ((\textsc{subset } (1 \mathrel{..} \mathit{Len}(\mathit{seq}0))) \setminus \{\{\}\}) \\
\qquad\quad \land \mathit{pc} \in \{\text{“a”}, \text{“Done”}\}
\end{array}
$$

$$
\begin{array}{l}
\mathit{Inv} \triangleq \land \mathit{TypeOK} \\
\qquad \land (\mathit{pc} = \text{“Done”}) \Rightarrow (U = \{\}) \\
\qquad \land \mathit{UV} \in \mathit{DomainPartitions} \\
\qquad \land \mathit{seq} \in \mathit{PermsOf}(\mathit{seq}0) \\
\qquad \land \textsc{union } \mathit{UV} = 1 \mathrel{..} \mathit{Len}(\mathit{seq}0) \\
\qquad \land \forall I, J \in \mathit{UV} : (I \neq J) \Rightarrow \mathit{RelSorted}(I, J)
\end{array}
$$

THEOREM $\mathit{Spec} \Rightarrow \Box \mathit{PCorrect}$

$\langle 1\rangle 1.$ $\mathit{Init} \Rightarrow \mathit{Inv}$

  $\langle 2\rangle$ SUFFICES ASSUME Init
    PROVE Inv
    OBVIOUS

  $\langle 2\rangle 1.$ TypeOK

    $\langle 3\rangle 1.$ $\mathit{seq} \in \mathit{Seq}(\mathit{Values}) \setminus \{\langle\rangle\}$
      BY DEF Init, Inv, TypeOK, $\mathit{DomainPartitions}$, $\mathit{RelSorted}$, UV

    $\langle 3\rangle 2.$ $\mathit{seq}0 \in \mathit{Seq}(\mathit{Values}) \setminus \{\langle\rangle\}$
      BY DEF Init, Inv, TypeOK, $\mathit{DomainPartitions}$, $\mathit{RelSorted}$, UV

    $\langle 3\rangle 3.$ $U \in \textsc{subset } ((\textsc{subset } (1 \mathrel{..} \mathit{Len}(\mathit{seq}0))) \setminus \{\{\}\})$

      $\langle 4\rangle 1.$ $\mathit{Len}(\mathit{seq}0) \in \mathit{Nat} \land \mathit{Len}(\mathit{seq}0) > 0$
        BY $\langle 3\rangle 1$, $\mathit{EmptySeq}$, $\mathit{LenProperties}$ DEF Init

      $\langle 4\rangle 2.$ $1 \mathrel{..} \mathit{Len}(\mathit{seq}0) \neq \{\}$
        BY $\langle 4\rangle 1$

      $\langle 4\rangle 3.$ QED
        BY $\langle 4\rangle 2$, $U = \{1 \mathrel{..} \mathit{Len}(\mathit{seq}0)\}$ DEF Init

    $\langle 3\rangle 4.$ $\mathit{pc} \in \{\text{“a”}, \text{“Done”}\}$
      BY DEF Init, Inv, TypeOK, $\mathit{DomainPartitions}$, $\mathit{RelSorted}$, UV

    $\langle 3\rangle 5.$ QED
      BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEF TypeOK

  $\langle 2\rangle 2.$ $\mathit{pc} = \text{“Done”} \Rightarrow U = \{\}$
    BY DEF Init

  $\langle 2\rangle 3.$ $\mathit{UV} \in \mathit{DomainPartitions}$
    BY DEF Init, UV, $\mathit{DomainPartitions}$

  $\langle 2\rangle 4.$ $\mathit{seq} \in \mathit{PermsOf}(\mathit{seq}0)$

⟨3⟩1. $seq \in PermsOf(seq)$

⟨4⟩.DEFINE $f \triangleq [i \in 1 \,..\, Len(seq) \mapsto i]$

⟨4⟩. $\wedge f \in [\text{DOMAIN } seq \rightarrow \text{DOMAIN } seq]$
$\wedge \forall y \in \text{DOMAIN } seq : \exists x \in \text{DOMAIN } seq : f[x] = y$

BY DEF $Init$

⟨4⟩.QED BY DEF $Init$, $PermsOf$, $Automorphisms$, $**$

⟨3⟩2. QED

BY ⟨3⟩1 DEF $Init$

⟨2⟩5. UNION $UV = 1 \,..\, Len(seq0)$

BY DEF $Init$, Inv, $TypeOK$, $DomainPartitions$, $RelSorted$, UV

⟨2⟩6. $\forall I, J \in UV : (I \neq J) \Rightarrow RelSorted(I, J)$

BY DEF $Init$, Inv, $TypeOK$, $DomainPartitions$, $RelSorted$, UV

⟨2⟩7. QED

BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6 DEF Inv

⟨1⟩2. $Inv \wedge [Next]_{vars} \Rightarrow Inv'$

⟨2⟩ SUFFICES ASSUME Inv,
$[Next]_{vars}$
PROVE Inv'

OBVIOUS

⟨2⟩1.CASE a

⟨3⟩ USE ⟨2⟩1

⟨3⟩1.CASE $U \neq \{\}$

⟨4⟩1. $\wedge\, pc =$ “a”
$\wedge\, pc' =$ “a”

BY ⟨3⟩1 DEF a

⟨4⟩2. PICK $I \in U : a!2!2!1!(I)$

$a!2!2!1(I)$ is the formula following $\exists I \in U :$ in the definition of a.

BY ⟨3⟩1 DEF a

⟨4⟩3.CASE $Cardinality(I) = 1$

⟨5⟩1. $\wedge\, U' = U \setminus \{I\}$
$\wedge\, seq' = seq$
$\wedge\, seq0' = seq0$

BY ⟨4⟩2, ⟨4⟩3 DEF a

⟨5⟩.$IsFiniteSet(I)$

⟨6⟩.$IsFiniteSet(1 \,..\, Len(seq0))$

BY $FS\_Interval$ DEF Inv, $TypeOK$

⟨6⟩.$I \subseteq 1 \,..\, Len(seq0)$

BY DEF Inv, $TypeOK$

⟨6⟩.QED BY FS_Subset

⟨5⟩j. PICK $j : I = \{j\}$

BY ⟨4⟩3, $FS\_Singleton$

⟨5⟩2. QED

⟨6⟩1. $UV' = UV$

The action removes a singleton set $\{j\}$ from U, which adds j to the set $\{\{i\} : i \in 1 \,..\, Len(seq) \setminus \text{UNION } U\}$, thereby keeping it in UV.

$\langle 7\rangle 1.\ j \in 1 \,..\, Len(seq)$
BY $\langle 5\rangle$j, *PermsOfLemma* DEF *Inv*, *TypeOK*
$\langle 7\rangle 2.\ \forall\, J \in U : I \neq J \Rightarrow j \notin J$
BY $\langle 5\rangle$j, *Zenon* DEF *Inv*, *TypeOK*, *DomainPartitions*, *UV*
$\langle 7\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle$j, $\langle 7\rangle 1$, $\langle 7\rangle 2$ DEF *UV*
$\langle 6\rangle 2.\ TypeOK'$
BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 1$
DEF *Inv*, *TypeOK*, *DomainPartitions*, *PermsOf*, *RelSorted*, *Min*, *Max*, *UV*
$\langle 6\rangle 3.\ ((pc = \text{"Done"}) \Rightarrow (U = \{\}))'$
BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 1$
DEF *Inv*, *TypeOK*, *DomainPartitions*, *PermsOf*, *RelSorted*, *Min*, *Max*, *UV*
$\langle 6\rangle 4.\ (UV \in DomainPartitions)'$
BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 1$, $\langle 6\rangle 1$
DEF *Inv*, *TypeOK*, *DomainPartitions*
$\langle 6\rangle 5.\ (seq \in PermsOf(seq0))'$
BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 1$, *Isa*
DEF *Inv*, *TypeOK*, *PermsOf*
$\langle 6\rangle 6.\ (\text{UNION } UV = 1 \,..\, Len(seq0))'$
BY $\langle 5\rangle 1$, $\langle 6\rangle 1$ DEF *Inv*
$\langle 6\rangle 7.\ (\forall\, I\_1,\ J \in UV : (I\_1 \neq J) \Rightarrow RelSorted(I\_1,\ J))'$
BY $\langle 4\rangle 1$, $\langle 4\rangle 3$, $\langle 5\rangle 1$, $\langle 6\rangle 1$
DEF *Inv*, *TypeOK*, *RelSorted*
$\langle 6\rangle 8.$ QED
BY $\langle 6\rangle 2$, $\langle 6\rangle 3$, $\langle 6\rangle 4$, $\langle 6\rangle 5$, $\langle 6\rangle 6$, $\langle 6\rangle 7$ DEF *Inv*
$\langle 4\rangle 4.$CASE $Cardinality(I) \neq 1$
$\langle 5\rangle 1.\ seq0' = seq0$
BY DEF *a*
$\langle 5\rangle$I. PICK $mn \in 1 \,..\, Len(seq0),\ mx \in 1 \,..\, Len(seq0) : I = mn \,..\, mx$
BY DEF *Inv*, *UV*, *DomainPartitions*
$\langle 5\rangle$mn. $mn < mx$
$\langle 6\rangle$.SUFFICES ASSUME $mn \geq mx$PROVE FALSE
OBVIOUS
$\langle 6\rangle 1.$CASE $mn > mx$
$\langle 7\rangle .I = \{\}$
BY $\langle 5\rangle$I, $\langle 6\rangle 1$
$\langle 7\rangle$.QED BY DEF *Inv*, *TypeOK*
$\langle 6\rangle 2.$CASE $mn = mx$
$\langle 7\rangle .I = \{mn\}$
BY $\langle 5\rangle$I, $\langle 6\rangle 2$
$\langle 7\rangle$.QED BY $\langle 4\rangle 4$, *FS_Singleton*
$\langle 6\rangle$.QED BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle$ DEFINE $I1(p) \triangleq mn \,..\, p$
$I2(p) \triangleq (p+1) \,..\, mx$
$\langle 5\rangle 2.$ PICK $p \in mn \,..\, (mx - 1) :$
$\land\ seq' \in Partitions(I,\ p,\ seq)$

$\wedge\ U' = ((U \setminus \{I\}) \cup \{I1(p),\ I2(p)\})$

BY $\langle 4\rangle 2$, $\langle 4\rangle 4$, $\langle 5\rangle$I, $\langle 5\rangle$mn, *IntervalMinMax*

$\langle 5\rangle$p. $mn \leq p \wedge p < mx$

BY $\langle 5\rangle$mn

$\langle 5\rangle 3$. $\wedge\ \wedge\ I1(p) \neq \{\}$
$\quad\quad \wedge\ I1(p) \subseteq 1 \mathrel{..} Len(seq0)$
$\quad \wedge\ \wedge\ I2(p) \neq \{\}$
$\quad\quad \wedge\ I2(p) \subseteq 1 \mathrel{..} Len(seq0)$
$\quad \wedge\ I1(p) \cap I2(p) = \{\}$
$\quad \wedge\ I1(p) \cup I2(p) = I$
$\quad \wedge\ \forall\, i \in I1(p),\ j \in I2(p) : (i < j)\ \wedge\ (seq[i] \leq seq[j])$

$\langle 6\rangle 1$. $mn \in I1(p) \wedge mx \in I2(p)$

BY $\langle 5\rangle$p

$\langle 6\rangle 2$. $\wedge\ I1(p) \subseteq 1 \mathrel{..} Len(seq0)$
$\quad \wedge\ I2(p) \subseteq 1 \mathrel{..} Len(seq0)$

BY DEF *Inv*, *TypeOK*

$\langle 6\rangle 4$. $I1(p) \cup I2(p) = I$

BY $\langle 5\rangle$I

$\langle 6\rangle$.QED BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 4$

Since I is in U, invariant *Inv* implies I is a non-empty subinterval of $1 \mathrel{..} Len(seq)$, and the $\langle 4\rangle 4$ case assumption implies $Min(I) < Max(I)$. Therefore $I1(p)$ and $I2(p)$ are nonempty subintervals of $1 \mathrel{..} Len(seq)$. It's clear from the definitions of $I1(p)$ and $I2(p)$ that they are disjoint sets whose union is I. The final conjunct follows from the definition of $Partitions(I,\ p,\ seq)$.

$\langle 5\rangle 4$. $\wedge\ seq' \in Seq(Values)$
$\quad \wedge\ Len(seq) = Len(seq')$
$\quad \wedge\ Len(seq) = Len(seq0)$

BY $\langle 5\rangle 2$, *PermsOfLemma* DEF *Partitions*, *Inv*, *TypeOK*

$\langle 5\rangle 5$. UNION U = UNION U'

BY $\langle 5\rangle 2$, $\langle 5\rangle 3$

$\langle 5\rangle 6$. $UV' = (UV \setminus \{I\}) \cup \{I1(p),\ I2(p)\}$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$ DEF *UV*

$\langle 5\rangle 7$. $TypeOK'$

$\langle 6\rangle 1$. $(seq \in Seq(Values) \setminus \{\langle\rangle\})'$

BY $\langle 5\rangle 4$ DEF *Inv*, *TypeOK*

$\langle 6\rangle 2$. $(seq0 \in Seq(Values) \setminus \{\langle\rangle\})'$

BY $\langle 5\rangle 1$ DEF *TypeOK*, *Inv*

$\langle 6\rangle 3$. $(U \in \text{SUBSET } ((\text{SUBSET } (1 \mathrel{..} Len(seq0))) \setminus \{\{\}\}))'$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF *Inv*, *TypeOK*

$\langle 6\rangle 4$. $(pc \in \{\text{"a"},\ \text{"Done"}\})'$

BY $\langle 4\rangle 1$

$\langle 6\rangle 5$. QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$, $\langle 6\rangle 4$ DEF *TypeOK*

$\langle 5\rangle 8$. $((pc = \text{"Done"}) \Rightarrow (U = \{\}))'$

BY $\langle 4\rangle 1$

$\langle 5\rangle 9.\ (UV \in \mathit{DomainPartitions})'$

  $\langle 6\rangle$ HIDE DEF $I1,\ I2$

  $\langle 6\rangle 1.\ UV' \in$ SUBSET SUBSET $(1\ ..\ \mathit{Len}(\mathit{seq}0'))$

    BY $\langle 5\rangle 6,\ \langle 5\rangle 3,\ \langle 5\rangle 4,\ \langle 5\rangle 1$ DEF Inv

  $\langle 6\rangle 2.$ UNION $UV' = 1\ ..\ \mathit{Len}(\mathit{seq}0')$

    BY $\langle 5\rangle 6,\ \langle 5\rangle 3,\ \langle 5\rangle 4,\ \langle 5\rangle 1$ DEF Inv

  $\langle 6\rangle 3.$ ASSUME NEW $J \in UV'$

      PROVE $\exists\, i, j \in 1\ ..\ \mathit{Len}(\mathit{seq}0') : J = i\ ..\ j$

    BY $\langle 5\rangle 1,\ \langle 5\rangle \mathrm{mn},\ \langle 5\rangle 6$ DEF $\mathit{Inv},\ \mathit{TypeOK},\ \mathit{DomainPartitions}$

  $\langle 6\rangle 4.$ ASSUME NEW $J \in UV'$, NEW $K \in UV'$, $J \neq K$

      PROVE $J \cap K = \{\}$

    $\langle 7\rangle 1.$CASE $J \in UV \land K \in UV$

      BY $\langle 6\rangle 4,\ \langle 7\rangle 1$ DEF $\mathit{Inv},\ \mathit{DomainPartitions}$

    $\langle 7\rangle 2.$CASE $J \in (UV \setminus \{I\}) \land K \in \{I1(p),\ I2(p)\}$

      $\langle 8\rangle .J \cap I = \{\}$

        BY $\langle 7\rangle 2$ DEF $UV,\ \mathit{Inv},\ \mathit{DomainPartitions}$

      $\langle 8\rangle .$QED BY $\langle 7\rangle 2,\ \langle 5\rangle \mathrm{I}$

    $\langle 7\rangle 3.$CASE $J \in \{I1(p),\ I2(p)\} \land K \in (UV \setminus \{I\})$

      $\langle 8\rangle .K \cap I = \{\}$

        BY $\langle 7\rangle 3$ DEF $UV,\ \mathit{Inv},\ \mathit{DomainPartitions}$

      $\langle 8\rangle .$QED BY $\langle 7\rangle 3,\ \langle 5\rangle \mathrm{I}$

    $\langle 7\rangle 4.$CASE $J \in \{I1(p),\ I2(p)\} \land K \in \{I1(p),\ I2(p)\}$

      BY $\langle 6\rangle 4,\ \langle 7\rangle 4$

    $\langle 7\rangle .$QED BY $\langle 5\rangle 6,\ \langle 7\rangle 1,\ \langle 7\rangle 2,\ \langle 7\rangle 3,\ \langle 7\rangle 4$

  $\langle 6\rangle 5.$ QED

    BY $\langle 6\rangle 1,\ \langle 6\rangle 2,\ \langle 6\rangle 3,\ \langle 6\rangle 4$ DEF $\mathit{DomainPartitions}$ $,\ \mathit{Min},\ \mathit{Max}$

$\langle 5\rangle 10.\ (\mathit{seq} \in \mathit{PermsOf}(\mathit{seq}0))'$

  BY $\langle 5\rangle 1,\ \langle 5\rangle 2,\ \mathit{PermsOfPermsOf}$ DEF $\mathit{Inv},\ \mathit{TypeOK},\ \mathit{Partitions}$

$\langle 5\rangle 11.$ (UNION $UV = 1\ ..\ \mathit{Len}(\mathit{seq}0))'$

  BY $\langle 5\rangle 6,\ \langle 5\rangle 3,\ \langle 5\rangle 4,\ \langle 5\rangle 1$ DEF Inv

$\langle 5\rangle 12.\ (\forall\, \mathit{II},\ \mathit{JJ} \in UV : (\mathit{II} \neq \mathit{JJ}) \Rightarrow \mathit{RelSorted}(\mathit{II},\ \mathit{JJ}))'$

  $\langle 6\rangle$ SUFFICES ASSUME NEW $\mathit{II} \in UV'$, NEW $\mathit{JJ} \in UV'$,

        $\mathit{II} \neq \mathit{JJ}$,

        NEW $i \in \mathit{II}$, NEW $j \in \mathit{JJ}$,

        $i < j$

      PROVE $\mathit{seq}'[i] \leq \mathit{seq}'[j]$

    BY DEF $\mathit{RelSorted}$

  $\langle 6\rangle .\ \land\ i \in 1\ ..\ \mathit{Len}(\mathit{seq})$

      $\land\ j \in 1\ ..\ \mathit{Len}(\mathit{seq})$

    BY $\langle 5\rangle 1,\ \langle 5\rangle 4,\ \langle 5\rangle 9$ DEF $\mathit{DomainPartitions}$

  $\langle 6\rangle \mathrm{I}.\ \land\ I \in$ SUBSET $(1\ ..\ \mathit{Len}(\mathit{seq}))$

      $\land\ p \in I$

    BY $\langle 5\rangle \mathrm{I},\ \langle 5\rangle 2,\ \mathit{PermsOfLemma}$ DEF $\mathit{Inv},\ \mathit{TypeOK}$

  $\langle 6\rangle 1.$CASE $\mathit{II} \in UV \setminus \{I\} \land \mathit{JJ} \in UV \setminus \{I\}$

    BY $\langle 5\rangle 2,\ \langle 6\rangle 1,\ \mathit{Zenon}$

DEF Inv, $TypeOK$, UV, $DomainPartitions$, $Partitions$, $RelSorted$

$\langle 6\rangle 2.$CASE $II \in UV \setminus \{I\} \land JJ \in \{I1(p), I2(p)\}$

$\langle 7\rangle 1.$ $JJ \subseteq I$

BY $\langle 5\rangle 3$, $\langle 6\rangle 2$

$\langle 7\rangle 3.$ PICK $k \in I : seq'[j] = seq[k]$

BY $\langle 5\rangle 2$, $\langle 7\rangle 1$, $\langle 6\rangle$I, $PartitionsLemma$ DEF Inv, $TypeOK$

$\langle 7\rangle 4.$ $II \cap I = \{\}$

BY $\langle 6\rangle 2$, $Zenon$ DEF UV, Inv, $DomainPartitions$

$\langle 7\rangle 5.$ PICK $mnI, mxI \in 1 \,..\, Len(seq0) : II = mnI \,..\, mxI$

BY $\langle 6\rangle 2$ DEF Inv, $DomainPartitions$

$\langle 7\rangle 5.$ $i < k$

BY $\langle 5\rangle$I, $\langle 6\rangle 2$, $\langle 7\rangle 1$, $\langle 7\rangle 4$ DEF Inv, $TypeOK$

$\langle 7\rangle 6.$ $seq[i] \leq seq[k]$

BY $\langle 6\rangle 2$, $\langle 7\rangle 1$, $\langle 7\rangle 5$ DEF Inv, $RelSorted$, UV

$\langle 7\rangle 7.$ $seq'[i] = seq[i]$

BY $\langle 5\rangle 2$, $\langle 6\rangle 2$, $\langle 6\rangle$I, $\langle 7\rangle 4$, $PartitionsLemma$ DEF Inv, $TypeOK$

$\langle 7\rangle.$QED BY $\langle 7\rangle 3$, $\langle 7\rangle 6$, $\langle 7\rangle 7$

$\langle 6\rangle 3.$CASE $II \in \{I1(p), I2(p)\} \land JJ \in UV \setminus \{I\}$

$\langle 7\rangle 1.$ $II \subseteq I$

BY $\langle 5\rangle 3$, $\langle 6\rangle 3$

$\langle 7\rangle 3.$ PICK $k \in I : seq'[i] = seq[k]$

BY $\langle 5\rangle 2$, $\langle 7\rangle 1$, $\langle 6\rangle$I, $PartitionsLemma$ DEF Inv, $TypeOK$

$\langle 7\rangle 4.$ $JJ \cap I = \{\}$

BY $\langle 6\rangle 3$, $Zenon$ DEF UV, Inv, $DomainPartitions$

$\langle 7\rangle 5.$ PICK $mnJ, mxJ \in 1 \,..\, Len(seq0) : JJ = mnJ \,..\, mxJ$

BY $\langle 6\rangle 3$ DEF Inv, $DomainPartitions$

$\langle 7\rangle 5.$ $k < j$

BY $\langle 5\rangle$I, $\langle 6\rangle 3$, $\langle 7\rangle 1$, $\langle 7\rangle 4$ DEF Inv, $TypeOK$

$\langle 7\rangle 6.$ $seq[k] \leq seq[j]$

BY $\langle 6\rangle 3$, $\langle 7\rangle 1$, $\langle 7\rangle 5$ DEF Inv, $RelSorted$, UV

$\langle 7\rangle 7.$ $seq'[j] = seq[j]$

$\langle 8\rangle 1.$ $j \in (1 \,..\, Len(seq)) \setminus I$

BY $\langle 7\rangle 4$

$\langle 8\rangle 2.$ $\land\ seq \in Seq(Values)$
$\land\ seq' \in Partitions(I, p, seq)$

BY $\langle 5\rangle 2$ DEF Inv, $TypeOK$

$\langle 8\rangle.$QED BY $\langle 6\rangle$I, $\langle 8\rangle 1$, $\langle 8\rangle 2$, $PartitionsLemma$

$\langle 7\rangle.$QED BY $\langle 7\rangle 3$, $\langle 7\rangle 6$, $\langle 7\rangle 7$

$\langle 6\rangle 4.$CASE $II = I1(p) \land JJ = I2(p)$

BY $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 6\rangle$I, $\langle 6\rangle 4$, $PartitionsLemma$ DEF Inv, $TypeOK$

$\langle 6\rangle 5.$CASE $II = I2(p) \land JJ = I2(p)$

BY $\langle 6\rangle 5$ contradiction: $i < j$ impossible

$\langle 6\rangle$ QED BY $\langle 5\rangle 6$, $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$, $\langle 6\rangle 4$, $\langle 6\rangle 5$

$\langle 5\rangle 13.$ QED

BY $\langle 5\rangle 7$, $\langle 5\rangle 8$, $\langle 5\rangle 9$, $\langle 5\rangle 10$, $\langle 5\rangle 11$, $\langle 5\rangle 12$ DEF Inv

$\langle 4\rangle 5.$ QED
BY $\langle 4\rangle 3$, $\langle 4\rangle 4$
$\langle 3\rangle 2.$CASE $U = \{\}$
$\langle 4\rangle$ USE $\langle 3\rangle 2$ DEF a, Inv, $TypeOK$, $DomainPartitions$, $PermsOf$, $RelSorted$, Min, Max, UV
$\langle 4\rangle 1.$ $TypeOK'$
OBVIOUS
$\langle 4\rangle 2.$ $((pc = \text{"Done"}) \Rightarrow (U = \{\}))'$
OBVIOUS
$\langle 4\rangle 3.$ $(UV \in DomainPartitions)'$
BY Isa
$\langle 4\rangle 4.$ $(seq \in PermsOf(seq0))'$
BY Isa
$\langle 4\rangle 5.$ (UNION $UV = 1 \,..\, Len(seq0))'$
OBVIOUS
$\langle 4\rangle 6.$ $(\forall I, J \in UV : (I \neq J) \Rightarrow RelSorted(I, J))'$
OBVIOUS
$\langle 4\rangle 7.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$, $\langle 4\rangle 6$, $Zenon$ DEF Inv
$\langle 3\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 2\rangle 2.$CASE UNCHANGED $vars$
$\langle 3\rangle 1.$ $TypeOK'$
BY $\langle 2\rangle 2$ DEF $vars$, Inv, $TypeOK$
$\langle 3\rangle 2.$ $((pc = \text{"Done"}) \Rightarrow (U = \{\}))'$
BY $\langle 2\rangle 2$ DEF $vars$, Inv
$\langle 3\rangle 3.$ $(UV \in DomainPartitions)'$
BY $\langle 2\rangle 2$, Isa DEF $vars$, Inv, $TypeOK$, $DomainPartitions$, UV
$\langle 3\rangle 4.$ $(seq \in PermsOf(seq0))'$
BY $\langle 2\rangle 2$, Isa DEF $vars$, Inv, $TypeOK$, $DomainPartitions$, $PermsOf$
$\langle 3\rangle 5.$ (UNION $UV = 1 \,..\, Len(seq0))'$
BY $\langle 2\rangle 2$ DEF $vars$, Inv, UV
$\langle 3\rangle 6.$ $(\forall I, J \in UV : (I \neq J) \Rightarrow RelSorted(I, J))'$
BY $\langle 2\rangle 2$ DEF $vars$, Inv, $TypeOK$, $DomainPartitions$, $PermsOf$, $RelSorted$, UV
$\langle 3\rangle 7.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF Inv
$\langle 2\rangle 3.$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$ DEF $Next$, $Terminating$
$\langle 1\rangle 3.$ $Inv \Rightarrow PCorrect$
$\langle 2\rangle$ SUFFICES ASSUME Inv,
$pc = \text{"Done"}$
PROVE $\land\ seq \in PermsOf(seq0)$
$\land\ \forall p, q \in 1 \,..\, Len(seq) : p < q \Rightarrow seq[p] \leq seq[q]$
BY DEF $PCorrect$
$\langle 2\rangle 1.$ $seq \in PermsOf(seq0)$
BY DEF Inv

$\langle 2 \rangle 2.\ \forall\, p,\ q \in 1 \, .. \, Len(seq) : p < q \Rightarrow seq[p] \leq seq[q]$

$\langle 3 \rangle$ SUFFICES ASSUME NEW $p \in 1 \, .. \, Len(seq)$, NEW $q \in 1 \, .. \, Len(seq)$, $p < q$

PROVE $seq[p] \leq seq[q]$

OBVIOUS

$\langle 3 \rangle 1.\ \land\ Len(seq) = Len(seq0)$

$\land\ Len(seq) \in Nat$

$\land\ Len(seq) > 0$

BY *PermsOfLemma* DEF *Inv*, *TypeOK*

$\langle 3 \rangle 2.\ UV = \{\{i\} : i \in 1 \, .. \, Len(seq)\}$

BY $U = \{\}$ DEF *Inv*, *TypeOK*, *UV*

$\langle 3 \rangle 3.\ \{p\} \in UV \land \{q\} \in UV$

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$

$\langle 3 \rangle$ QED

BY $\langle 3 \rangle 3$ DEF *Inv*, *RelSorted*

$\langle 2 \rangle 3.$ QED

BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$

$\langle 1 \rangle 4.$ QED

BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, *PTL* DEF *Spec*

* Created *Mon Jun* 27 08:20:07 *PDT* 2016 by lamport