MODULE $malgtd1ex12$

computing the maximum value of an array f

EXTENDS $Naturals, TLC, Integers$

CONSTANTS $undef, n0, f0, i0, m0, min, max$

VARIABLES n, f, m, i, pc

Auxiliary defintions

an exampe for an array

$def0 \triangleq [j \in 0 \,..\, n0-1 \mapsto n0-j]$

defintion of the range of a function

$ran(g) \triangleq \{u \in Nat : (\exists j \in \text{DOMAIN } g : g[j] = u)\}$

defintion of the restriction of a function

$Rest(g, l) \triangleq [k \in 0 \,..\, l \mapsto g[k]]$

precondition

$$\begin{array}{l} pre \triangleq \\ \quad \land\, n0 \in Nat \land n0 \neq 0 \\ \quad \land\, f0 = def0 \\ \quad \land\, i0 \in Int \land m0 \in Int \end{array}$$

$pre1 \triangleq f = f0 \land n = n0 \land pre$

Integers for your computer

$zinf \triangleq min \,..\, max$

Naturals for your computer

$ninf \triangleq 0 \,..\, max$

---

assuming precondition over initial values of variables

ASSUME pre

Initialisaton for tyhe TLA model

$$\begin{array}{lll} Init \triangleq & \land\, i & = i0 \\ & \land\, m & = m0 \\ & \land\, f & = f0 \\ & \land\, n & = n0 \\ & \land\, pc & = \text{“l0”} \end{array}$$

---

actions for transition

$$\begin{array}{lll} l0l1 \triangleq & \land\, pc & = \text{“l0”} \\ & \land\, m' & = f[0] \\ & \land\, pc' & = \text{“l1”} \\ & \land\, \text{UNCHANGED } \langle n, f, i \rangle & \end{array}$$

$$\begin{array}{lll} l1l2 \triangleq & \land\, pc & = \text{“l1”} \\ & \land\, i' & = 1 \\ & \land\, pc' & = \text{“l2”} \\ & \land\, \text{UNCHANGED } \langle n, f, m \rangle & \end{array}$$

$$
\begin{array}{lll}
l2l3 & \triangleq & \land\ pc = \text{“}\textsf{l2}\text{”} \\
 & & \land\ i < n \\
 & & \land\ pc' = \text{“}\textsf{l3}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f,\ m,\ i \rangle
\end{array}
$$

$$
\begin{array}{lll}
l2l8 & \triangleq & \land\ pc = \text{“}\textsf{l2}\text{”} \\
 & & \land\ (i \geq n) \\
 & & \land\ m' = m \\
 & & \land\ i' \ \ = i \\
 & & \land\ pc' = \text{“}\textsf{l8}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f \rangle
\end{array}
$$

$$
\begin{array}{lll}
l3l4 & \triangleq & \land\ pc = \text{“}\textsf{l3}\text{”} \\
 & & \land\ f[i] > m \\
 & & \land\ m' = m \\
 & & \land\ i' \ \ = i \\
 & & \land\ pc' = \text{“}\textsf{l4}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f \rangle
\end{array}
$$

$$
\begin{array}{lll}
l3l6 & \triangleq & \land\ pc = \text{“}\textsf{l3}\text{”} \\
 & & \land\ (f[i] \leq m) \\
 & & \land\ m' = m \\
 & & \land\ i' \ \ = i \\
 & & \land\ pc' = \text{“}\textsf{l6}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f \rangle
\end{array}
$$

$$
\begin{array}{lll}
l4l5 & \triangleq & \land\ pc \ \ = \text{“}\textsf{l4}\text{”} \\
 & & \land\ m' = f[i] \\
 & & \land\ i' \ \ = i \\
 & & \land\ pc' = \text{“}\textsf{l5}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f \rangle
\end{array}
$$

$$
\begin{array}{lll}
l5l6 & \triangleq & \land\ pc \ \ = \text{“}\textsf{l5}\text{”} \\
 & & \land\ m' = m \\
 & & \land\ i' \ \ = i \\
 & & \land\ pc' = \text{“}\textsf{l6}\text{”} \\
 & & \land\ \textsc{unchanged}\ \langle n,\ f \rangle
\end{array}
$$

$$
\begin{array}{lll}
l6l7 & \triangleq & \land\ pc \ \ = \text{“}\textsf{l6}\text{”} \\
 & & \land\ m' = m \\
 & & \land\ i' \ \ = i + 1 \\
 & & \land\ pc' = \text{“}\textsf{l7}\text{”} \\
 & \multicolumn{2}{l}{\land\ \textsc{unchanged}\ \langle n,\ f \rangle}
\end{array}
$$

$$
\begin{array}{lll}
l7l3 & \triangleq & \land\ pc = \text{“}\textsf{l7}\text{”} \\
 & & \land\ i < n
\end{array}
$$

$\wedge\ m' = m$
$\wedge\ i' \ = i$
$\wedge\ pc' = \text{``l3''}$
$\wedge\ \text{UNCHANGED}\ \langle n,\ f \rangle$

$l7l8\ \triangleq$
$\wedge\ pc = \text{``l7''}$
$\wedge\ i \geq n$
$\wedge\ m' = m$
$\wedge\ i' \ = i$
$\wedge\ pc' = \text{``l8''}$
$\wedge\ \text{UNCHANGED}\ \langle n,\ f \rangle$

Next relatioon over values variables

$Next\ \triangleq\ \vee\ l0l1$
$\vee\ l1l2$
$\vee\ l2l3$
$\vee\ l2l8$
$\vee\ l3l4$
$\vee\ l3l6$
$\vee\ l4l5$
$\vee\ l5l6$
$\vee\ l6l7$
$\vee\ l7l3$
$\vee\ l7l8$
$\vee\ \text{UNCHANGED}\ \langle n,\ m,\ i,\ f,\ pc \rangle$

$Dl0l1\ \triangleq\ \ 0 \leq 0 \wedge 0 \leq n0 - 1$
$Dl1l2\ \triangleq\ 1 \in zinf$
$inv\ \triangleq$
$\wedge\ pc \in \{\text{``l0''},\ \text{``l1''},\ \text{``l2''},\ \text{``l3''},\ \text{``l4''},\ \text{``l5''},\ \text{``l6''},\ \text{``l7''},\ \text{``l8''}\}$
$\wedge\ n\ \in Int \wedge f = def0 \wedge i \in Int \wedge m \in Int$
$\wedge\ pc = \text{``l0''} \Rightarrow\ \ f = f0 \wedge n = n0 \wedge m = m0 \wedge i = i0 \wedge pre$
$\wedge\ pc = \text{``l1''} \Rightarrow\ f = f0 \wedge n = n0 \wedge m = f[0] \wedge i = i0 \wedge pre$
$\wedge\ pc = \text{``l2''} \Rightarrow\ i = 1\ \ \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i-1))) \wedge (\forall\, k\ \ \in 0\,..\,i-1 : f[k] \leq m) \wedge pre1$
$\wedge\ pc = \text{``l3''} \Rightarrow\ \ \ \ (i \in 1\,..\,n-1) \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i-1))) \wedge (\forall\, k\ \ \in 0\,..\,i-1 : f[k] \leq m)$
$\wedge\ pc = \text{``l4''} \Rightarrow\ \ \ f[i] > m \wedge (i \in 1\,..\,n-1) \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i-1))) \wedge (\forall\, k\ \ \in 0\,..\,i-1 :$
$\wedge\ pc = \text{``l5''}\ \ \Rightarrow\ \ f[i] > m \wedge (i \in 1\,..\,n-1) \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i))) \wedge (\forall\, k\ \ \in 0\,..\,i : f[k] \leq m$
$\wedge\ pc = \text{``l6''} \Rightarrow\ \ \ (i \in 1\,..\,n-1) \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i))) \wedge (\forall\, k\ \ \in 0\,..\,i : f[k] \leq m) \wedge pre1$
$\wedge\ pc = \text{``l7''} \Rightarrow\ \ \ (i \in 1\,..\,n) \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i-1))) \wedge (\forall\, k\ \ \in 0\,..\,i-1 : f[k] \leq m) \wedge pre$
$\wedge\ pc = \text{``l8''} \Rightarrow\ \ i = n \wedge\ \ m \in Nat \wedge (m \in ran(Rest(f,\ i-1))) \wedge (\forall\, k\ \ \in 0\,..\,i-1 : f[k] \leq m) \wedge pre1$

$partialcorrectness\ \triangleq\ pc = \text{``l8''} \Rightarrow m \in Nat \wedge (m \in ran(Rest(f,\ n-1))) \wedge (\forall\, k\ \ \in 0\,..\,n-1 : f[k] \leq m) \wedge pre$

$runtimeerrors\ \triangleq\ \ m \in zinf \wedge i \in zinf \qquad \wedge n \in zinf$

$$safe \triangleq inv \land runtimeerrors \land partialcorrectness$$