MODULE $appex3\_10$

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

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

---

precondition

ASSUME $n0 \in Nat \land n0 \neq 0 \ \land f0 = def0 \land i0 \in Int$

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

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

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

$$\begin{aligned} l2l3 \triangleq\ & \land pc = \text{“l2”} \\ & \land i < n \\ & \land pc' = \text{“l3”} \\ & \land \text{UNCHANGED } \langle n, f, m, i \rangle \end{aligned}$$

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

$$\begin{aligned} l3l4 \triangleq\ & \land pc = \text{“l3”} \\ & \land f[i] > m \\ & \land m' = m \end{aligned}$$

$\land\ i' = i$
$\land\ pc' = \text{“l4”}$
$\land$ UNCHANGED $\langle n, f \rangle$

$l3l6 \triangleq$ $\land\ pc = \text{“l3”}$
$\land\ (f[i] \leq m)$
$\land\ m' = m$
$\land\ i' = i$
$\land\ pc' = \text{“l6”}$
$\land$ UNCHANGED $\langle n, f \rangle$

$l4l5 \triangleq$ $\land\ pc = \text{“l4”}$
$\land\ m' = f[i]$
$\land\ i' = i$
$\land\ pc' = \text{“l5”}$
$\land$ UNCHANGED $\langle n, f \rangle$

$l5l6 \triangleq$ $\land\ pc = \text{“l5”}$
$\land\ m' = m$
$\land\ i' = i$
$\land\ pc' = \text{“l6”}$
$\land$ UNCHANGED $\langle n, f \rangle$

$l6l7 \triangleq$ $\land\ pc = \text{“l6”}$
$\land\ m' = m$
$\land\ i' = i + 1$
$\land\ pc' = \text{“l7”}$
$\land$ UNCHANGED $\langle n, f \rangle$

$l7l3 \triangleq$ $\land\ pc = \text{“l7”}$
$\land\ i < n$
$\land\ m' = m$
$\land\ i' = i$
$\land\ pc = \text{“l3”}$
$\land$ UNCHANGED $\langle n, f \rangle$

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

$$
\begin{array}{l}
Next \triangleq \lor\ l0l1 \\
\qquad\quad \lor\ l1l2 \\
\qquad\quad \lor\ l2l3 \\
\qquad\quad \lor\ l2l8 \\
\qquad\quad \lor\ l3l4 \\
\qquad\quad \lor\ l3l6 \\
\qquad\quad \lor\ l4l5 \\
\qquad\quad \lor\ l5l6 \\
\qquad\quad \lor\ l6l7 \\
\qquad\quad \lor\ l7l3 \\
\qquad\quad \lor\ l7l8 \\
\qquad\quad \lor\ \text{UNCHANGED}\ \langle n,\ m,\ i,\ f,\ pc\rangle
\end{array}
$$

$$
\begin{array}{l}
pre0 \triangleq\ n0 \in Nat \land n0 \neq 0\ \land f0 = def0 \land i0 \in Int \\
pre1 \triangleq\ f = f0 \land n = n0 \land pre0
\end{array}
$$

$$
\begin{array}{l}
\quad zinf \triangleq\ min\ ..\ max \\
\quad ninf \triangleq\ 0\ ..\ max
\end{array}
$$

$$
\begin{array}{l}
\quad Dl0l1 \triangleq\ \ 0 \leq 0 \land 0 \leq n0 - 1 \\
\quad Dl1l2 \triangleq\ 1 \in zinf \\
\ inv \triangleq \\
\quad \land\ pc \in \{\text{“l0”},\ \text{“l1”},\ \text{“l2”},\ \text{“l3”},\ \text{“l4”},\ \text{“l5”},\ \text{“l6”},\ \text{“l7”},\ \text{“l8”}\} \\
\quad \land\ n\ \in Int \land f = def0 \land i \in Int \land m \in Int \\
\quad \land\ pc = \text{“l0”} \Rightarrow\ \ f = f0 \land n = n0 \land m = m0 \land i = i0 \land pre0 \land Dl0l1 \\
\quad \land\ pc = \text{“l1”} \Rightarrow\ f = f0 \land n = n0 \land m = f[0] \land i = i0 \land pre0 \land Dl1l2 \\
\quad \land\ pc = \text{“l2”} \Rightarrow f = f0 \land n = n0 \land m = f[0] \land i = 1 \land pre0 \\
\quad \land\ pc = \text{“l3”} \Rightarrow\ (\exists\, j \in 0\ ..\ i-1 : f[j] = m) \land (\forall\, k \in 0\ ..\ i-1 : f[k] \leq m) \land (i < n) \land\ \ pre1 \\
\quad \land\ pc = \text{“l4”} \Rightarrow\ (\exists\, j \in 0\ ..\ i-1 : f[j] = m) \land (\forall\, k \in 0\ ..\ i-1 : f[k] \leq m) \land (i < n) \land (f[i] > m) \land pre1 \\
\quad \land\ pc = \text{“l5”}\ \ \Rightarrow\ (\exists\, j \in 0\ ..\ i-1 : f[j] = m) \land (\forall\, k \in 0\ ..\ i : f[k] \leq m) \land (i < n) \land (f[i] > m) \land pre1 \\
\quad \land\ pc = \text{“l6”} \Rightarrow\ \ (\exists\, j \in 0\ ..\ i : f[j] = m) \land (\forall\, k \in 0\ ..\ i : f[k] \leq m)\ \ \land pre1 \\
\quad \land\ pc = \text{“l7”} \Rightarrow\ \ (\exists\, j \in 0\ ..\ i-1 : f[j] = m) \land (\forall\, k \in 0\ ..\ i-1 : f[k] \leq m) \land (i \leq n)\ \ \land pre1 \\
\quad \land\ pc = \text{“l8”} \Rightarrow\ \ (\exists\, j \in 0\ ..\ i-1 : f[j] = m) \land (\forall\, k \in 0\ ..\ i : f[k] \leq m)\ \ \land pre1 \land i = n
\end{array}
$$

$$
runtimeerrors \triangleq\ \ m \in zinf \land i \in zinf \land n \in zinf
$$