MODULE *appex4_1_4*

EXTENDS *Integers*, *TLC*

* – *wfNext*

--algorithm *test* **{**
variables $x = 11,\ y = 13,\ z$ **;**
{
$l1$: **assert** $x = 11 \land y = 13$ **;**
$z := x$ **;** $x := y$ **;** $y := z$ **;**
$l2$: **assert** $x = 26 \div 2 \land y = 33 \div 3$ **;**

$l3$: **print** $\langle x,\ y \rangle$ **;**
}
}

BEGIN TRANSLATION

CONSTANT *defaultInitValue*

VARIABLES $x,\ y,\ z,\ pc$

$vars \triangleq \langle x,\ y,\ z,\ pc \rangle$

$Init \triangleq$ Global variables
$\land\ x = 11$
$\land\ y = 13$
$\land\ z = defaultInitValue$
$\land\ pc =$ "l1"

$l1 \triangleq \land\ pc =$ "l1"
$\land\ Assert(x = 11 \land y = 13,$ "Failure of assertion at line 11, column 4.")
$\land\ z' = x$
$\land\ x' = y$
$\land\ y' = z'$
$\land\ pc' =$ "l2"

$l2 \triangleq \land\ pc =$ "l2"
$\land\ Assert(x = 26 \div 2 \land y = 33 \div 3,$
"Failure of assertion at line 13, column 4.")
$\land\ pc' =$ "l3"
$\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

$l3 \triangleq \land\ pc =$ "l3"
$\land\ PrintT(\langle x,\ y \rangle)$
$\land\ pc' =$ "Done"
$\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

Allow infinite stuttering to prevent deadlock on termination.

$Terminating \triangleq pc =$ "Done" $\land$ UNCHANGED $vars$

$Next \triangleq\ l1 \lor l2 \lor l3$
$\qquad\qquad \lor\ Terminating$

$Spec \triangleq\ Init \land \Box[Next]_{vars}$

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

END TRANSLATION

$MAX \triangleq 32768$ 16 bits
$D \triangleq 0\,..\,32768$
$x \leq 32760$

$DD(X) \triangleq\ (X \in D)$

$Safety\_absence \triangleq\ \ DD(x)\ \land DD(y)$

$Inv \triangleq$
$\quad \land\ pc = \text{“l1”} \Rightarrow\ \ x = 11 \land y = 13$
$\quad \land\ pc = \text{“l2”} \Rightarrow\ \ x = 26 \div 2 \land y = 33 \div 3$