MODULE *appex*1_4

modules de base importables

EXTENDS *Naturals*, *Integers*, *TLC*

CONSTANTS $x1,\ x2,\ U,\ MAX$

$MIN \triangleq -MAX$

VARIABLES $y1,\ y2,\ y3,\ z1,\ z2,\ pc$

$locs \triangleq \{\text{“START”},\ \text{“HALT”},\ \text{“LOOP”}\}$

$BF(X) \triangleq X \neq U \Rightarrow X \in MIN\ ..\ MAX$

ASSUME $BF(x1) \land BF(x2)$

$Init \triangleq pc = \text{“START”} \land y1 = U \land y2 = U \land y3 = U \land z1 = U \land z2 = U$

$actionSTART\_LOOP \triangleq$

$\land\ pc = \text{“START”}$
$\land\ pc' = \text{“LOOP”}$
$\land\ y1' = 0$
$\land\ y2' = 0$
$\land\ y3' = x1$
$\land$ UNCHANGED $\langle z1,\ z2\rangle$

$actionLOOP\_HALT \triangleq$

$\land\ pc = \text{“LOOP”}$
$\land\ y3 = 0$
$\land\ pc' = \text{“HALT”}$
$\land\ y1' = y1$
$\land\ y2' = y2$
$\land\ y3' = y3$
$\land\ z1' = y1$
$\land\ z2' = y2$

$actionLOOP\_LOOP \triangleq$

$\land\ pc = \text{“LOOP”}$
$\land\ y3 \neq 0$
$\land\ pc' = pc$
$\land\ y1' =$ IF $y2 + 1 = x2$ THEN $y1 + 1$ ELSE $y1$
$\land\ y2' =$ IF $y2 + 1 = x2$ THEN 0 ELSE $y2 + 1$
$\land\ y3' = y3 - 1$

$$\begin{array}{ll} \wedge & z1' = z1 \\ \wedge & z2' = z2 \end{array}$$

$skip \triangleq$ UNCHANGED $\langle y1,\ y2,\ y3,\ z1,\ z2,\ pc \rangle$

$$\begin{array}{l} Next \triangleq \\ \quad \vee\ actionSTART\_LOOP \\ \quad \vee\ \ actionLOOP\_HALT \\ \quad \vee\ actionLOOP\_LOOP \\ \quad \vee\ skip \end{array}$$

---

vérification du contrôle

$safety1 \triangleq\ pc \in locs$

correction partielle

$safety2 \triangleq\ pc = \text{“HALT”} \Rightarrow z1 = x1 \div x2 \wedge z2 = x1\%x2 \wedge PrintT(z1) \wedge PrintT(z2)$

$safety3 \triangleq\ pc = \text{“HALT”} \Rightarrow \quad x1 = z1 * x2 + z2\ \ \wedge 0 \leq z2 \wedge z2 < x2$

vérification de l'absence d'erreurs à l'exé&cution ou *RTE*

$safety4 \triangleq\ BF(z1) \wedge BF(z2) \wedge BF(y1) \wedge BF(y2) \wedge BF(y3)$

$Safety \triangleq\ safety1\ \ \wedge safety2\ \ \wedge safety3\ \ \wedge safety4$