MODULE *algo_squareroot*

EXTENDS *Integers*, *TLC*

CONSTANTS x, U x is the input

VARIABLES pc, $y1$, $y2$, $y3$, z

$vars \triangleq \langle pc, y1, y2, y3, z \rangle$

$al0l1 \triangleq pc = \text{“l0”} \land y1' = 0 \land y2' = 1 \land y3' = 1 \land pc' = \text{“l1”} \land z' = z$
$al1l2 \triangleq pc = \text{“l1”} \land y2 \leq x \land pc' = \text{“l2”} \land \text{UNCHANGED } \langle y1, y2, y3, z \rangle$
$al1l4 \triangleq pc = \text{“l1”} \land y2 > x \land pc' = \text{“l4”} \land \text{UNCHANGED } \langle y1, y2, y3, z \rangle$
$al2l3 \triangleq pc = \text{“l2”} \land y1' = y1 + 1 \land y2' = y2 + y3 + 2 \land y3' = y3 + 2 \land pc' = \text{“l3”} \land z' = z$
$al3l2 \triangleq pc = \text{“l3”} \land y2 \leq x \land pc' = \text{“l2”} \land \text{UNCHANGED } \langle y1, y2, y3, z \rangle$
$al3l4 \triangleq pc = \text{“l3”} \land y2 > x \land pc' = \text{“l4”} \land \text{UNCHANGED } \langle y1, y2, y3, z \rangle$
$al4l5 \triangleq pc = \text{“l4”} \land z' = y1 \land pc' = \text{“l5”} \land \text{UNCHANGED } \langle y1, y2, y3 \rangle$

$Init \triangleq y1 = U \land y2 = U \land y3 = U \land z = U \land pc = \text{“l0”}$
$Next \triangleq al0l1 \lor al1l2 \lor al1l4 \lor al2l3 \lor al3l2 \lor al3l4 \lor al4l5$

$MAX \triangleq 32767$ 16 bits
$MIN \triangleq -32768$
$D \triangleq MIN \,..\, MAX$
$x \leq 32760$
$Safety\_absence \triangleq (y1 \in D) \land (y2 \in D) \land (y3 \in D) \land (z \in D)$
$i \triangleq$
$\land pc = \text{“l0”} \Rightarrow y1 \in D \land y2 \in D \land y3 \in D \land z \in D$
$\land pc = \text{“l1”} \Rightarrow y2 = (y1+1)*(y1+1) \land y3 = 2*y1+1 \land y1*y1 \leq x$
$\land pc = \text{“l2”} \Rightarrow y2 = (y1+1)*(y1+1) \land y3 = 2*y1+1 \land y1*y1 \leq x \land y2 \leq x$
$\land pc = \text{“l3”} \Rightarrow y2 = (y1+1)*(y1+1) \land y3 = 2*y1+1 \land y1*y1 \leq x$
$\land pc = \text{“l4”} \Rightarrow y2 = (y1+1)*(y1+1) \land y3 = 2*y1+1 \land y1*y1 \leq x \land x < y2$
$\land pc = \text{“l5”} \Rightarrow y2 = (y1+1)*(y1+1) \land y3 = 2*y1+1 \land z*z \leq x \land x < (z+1)*(z+1)$
$Safety\_partialcorrectness \triangleq pc = \text{“l5”} \Rightarrow z*z \leq x \land x < (z+1)*(z+1)$

$Qtermination \triangleq pc \neq \text{“l5”}$