```
──────────────── MODULE pluscal_max ────────────────
EXTENDS Naturals, Integers, TLC

CONSTANTS a, b, min, max
x0 ≜ a
y0 ≜ b

pre ≜ a ∈ min . . max ∧ b ∈ min . . max

ASSUME pre

--algorithm max{
  variables x = a,
            y = b,
            z ;

{
 l0: assert x = a ∧ y = b ∧ pre ;
 if ( x < y ) {
  l1:  assert x = a ∧ y = b ∧ x < y  ∧ pre ;
  z := y ;
  l2: assert x = a ∧ y = b ∧ z ∈  {a, b} ∧ a ≤ z ∧ b ≤ z  ∧ pre ;
   }
else
{
 l3: assert x = a ∧ y = b ∧  x ≥ y  ∧ pre ;
 z := x ;
 l4: assert x = a ∧ y = b ∧ z ∈  {a, b} ∧ a ≤ z ∧ b ≤ z ∧ pre ;
  } ;
 l5:    assert z ∈  {a, b} ∧ a ≤ z ∧ b ≤ z ∧ pre ;
 print "done" ;
 l6: assert z ∈  {a, b} ∧ a ≤ z ∧ b ≤ z ∧ pre ;
 }
 }
 BEGIN TRANSLATION
CONSTANT defaultInitValue
VARIABLES x, y, z, pc

vars ≜ ⟨x, y, z, pc⟩

Init ≜  Global variables
          ∧ x = a
          ∧ y = b
          ∧ z = defaultInitValue
          ∧ pc = "l0"

l0 ≜ ∧ pc = "l0"
```

```
         $\land$ $Assert(x = a \land y = b \land pre,$
                   "Failure of assertion at line 20, column 5.")
         $\land$ IF $x < y$
              THEN $\land$ $pc' =$ "l1"
              ELSE $\land$ $pc' =$ "l3"
         $\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

$l1$ $\triangleq$ $\land$ $pc =$ "l1"
         $\land$ $Assert(x = a \land y = b \land x < y \land pre,$
                   "Failure of assertion at line 22, column 8.")
         $\land$ $z' = y$
         $\land$ $pc' =$ "l2"
         $\land$ UNCHANGED $\langle x,\ y \rangle$

$l2$ $\triangleq$ $\land$ $pc =$ "l2"
         $\land$ $Assert(x = a \land y = b \land z \in \{a,\ b\} \land a \leq z \land b \leq z \land pre,$
                   "Failure of assertion at line 24, column 7.")
         $\land$ $pc' =$ "l5"
         $\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

$l3$ $\triangleq$ $\land$ $pc =$ "l3"
         $\land$ $Assert(x = a \land y = b \land x \geq y \land pre,$
                   "Failure of assertion at line 28, column 6.")
         $\land$ $z' = x$
         $\land$ $pc' =$ "l4"
         $\land$ UNCHANGED $\langle x,\ y \rangle$

$l4$ $\triangleq$ $\land$ $pc =$ "l4"
         $\land$ $Assert(x = a \land y = b \land z \in \{a,\ b\} \land a \leq z \land b \leq z \land pre,$
                   "Failure of assertion at line 30, column 6.")
         $\land$ $pc' =$ "l5"
         $\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

$l5$ $\triangleq$ $\land$ $pc =$ "l5"
         $\land$ $Assert(z \in \{a,\ b\} \land a \leq z \land b \leq z \land pre,$
                   "Failure of assertion at line 32, column 6.")
         $\land$ $PrintT($"done"$)$
         $\land$ $pc' =$ "l6"
         $\land$ UNCHANGED $\langle x,\ y,\ z \rangle$

$l6$ $\triangleq$ $\land$ $pc =$ "l6"
         $\land$ $Assert(z \in \{a,\ b\} \land a \leq z \land b \leq z \land pre,$
                   "Failure of assertion at line 34, column 6.")
         $\land$ $pc' =$ "Done"
         $\land$ UNCHANGED $\langle x,\ y,\ z \rangle$
```

Allow infinite stuttering to prevent deadlock on termination.

$$\mathit{Terminating} \triangleq pc = \text{“Done”} \land \text{UNCHANGED } \mathit{vars}$$

$$\begin{aligned}\mathit{Next} \triangleq\ & l0 \lor l1 \lor l2 \lor l3 \lor l4 \lor l5 \lor l6\\ & \lor \mathit{Terminating}\end{aligned}$$

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

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

END TRANSLATION

$$\mathit{ISDEF}(X,\ Y) \triangleq X \neq \mathit{defaultInitValue} \Rightarrow X \in Y$$

$$\begin{aligned}&\mathit{Inv} \triangleq\\ &\quad \land pc \in \{\text{“l0”},\ \text{“l1”},\ \text{“l2”},\ \text{“l3”},\ \text{“l4”},\ \text{“l5”},\ \text{“l6”},\ \text{“Done”}\}\\ &\quad \land \mathit{ISDEF}(x,\ \mathit{Int}) \land \mathit{ISDEF}(y,\ \mathit{Int}) \land \mathit{ISDEF}(z,\ \mathit{Int})\\ &\quad \land pc = \text{“l0”} \Rightarrow x = a \land y = b\\ &\quad \land pc = \text{“l1”} \Rightarrow x = a \land y = b \land x < y\\ &\quad \land pc = \text{“l2”} \Rightarrow x = a \land y = b \land z \in \{a,\ b\} \land a \leq z \land b \leq z\\ &\quad \land pc = \text{“l3”} \Rightarrow x = a \land y = b \land x \geq y\\ &\quad \land pc = \text{“l4”} \Rightarrow x = a \land y = b \land z \in \{a,\ b\} \land a \leq z \land b \leq z\\ &\quad \land pc = \text{“l5”} \Rightarrow z \in \{a,\ b\} \land a \leq z \land b \leq z\\ &\quad \land pc = \text{“l6”} \Rightarrow z \in \{a,\ b\} \land a \leq z \land b \leq z\\ &\quad \land pc = \text{“Done”} \Rightarrow z \in \{a,\ b\} \land a \leq z \land b \leq z\end{aligned}$$

$$\mathit{DD}(X) \triangleq X \neq \mathit{defaultInitValue} \Rightarrow X \in \mathit{min} \mathrel{..} \mathit{max}$$

$$\mathit{safetyrte} \triangleq \mathit{DD}(x) \land \mathit{DD}(y) \land \mathit{DD}(z)$$

$$\mathit{safetypc} \triangleq pc = \text{“Done”} \Rightarrow z \in \{a,\ b\} \land a \leq z \land b \leq z$$

$$\mathit{myprop} \triangleq \Box(x = a \land y = b)$$

\* Modification History
\* Last modified *Thu Feb* 16 11:48:27 *CET* 2023 by *mery*
\* Created *Wed Sep* 09 17:02:47 *CEST* 2015 by *mery*