MODULE *TLAPROOFMAX2*

EXTENDS *Naturals*, *Integers*, *TLAPS*

CONSTANTS $a0$, $b0$

$typeInt(u) \triangleq u \in Int$
$pre(u, v) \triangleq u \in Int \land v \in Int$
$maximum(u, v) \triangleq \text{IF } u < v \text{ THEN } v \text{ ELSE } u$

```
--algorithm maximum {
variables  a = a0, b = b0, r ;
{
w1: if ( a < b ) {
     r := b ;  }
     else {
     r := a ;
      } ;
      }
      }
```

BEGIN TRANSLATION ($chksum(pcal) =$ "$511d800d$" $\land\ chksum(tla) =$ "$67c371db$")

CONSTANT *defaultInitValue*

VARIABLES a, b, r, pc

$vars \triangleq \langle a, b, r, pc \rangle$

$Init \triangleq$ Global variables

$\land\ a = a0$
$\land\ b = b0$
$\land\ r \in Int$
$\land\ pc =$ "w1"

$w1 \triangleq \land\ pc =$ "w1"
$\land\ \text{IF } a < b$
$\quad \text{THEN } \land\ r' = b$
$\quad \text{ELSE } \land\ r' = a$
$\land\ pc' =$ "Done"
$\land\ \text{UNCHANGED } \langle a, b \rangle$

Allow infinite stuttering to prevent deadlock on termination.

$Terminating \triangleq pc =$ "Done" $\land\ \text{UNCHANGED } vars$

$Next \triangleq w1$
$\quad \lor\ Terminating$

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

$Termination \triangleq \Diamond(pc =$ "Done"$)$

END TRANSLATION

Definitions of invariants

$i0 \triangleq typeInt(a) \wedge typeInt(b) \wedge typeInt(r) \wedge a = a0 \wedge b = b0$
$i1 \triangleq pc = \text{"Done"} \Rightarrow r = maximum(a0, b0)$
$InductiveInvariant \triangleq i1 \wedge i0$

ASSUME $Assumption \triangleq pre(a0, b0)$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$
$\langle 1 \rangle$ SUFFICES ASSUME $Init$
PROVE $InductiveInvariant$
OBVIOUS
$\langle 1 \rangle 1.$ $a = a0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 2.$ $b = b0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 3.$ $pre(a0, b0)$ BY $Assumption$ DEF $Init$, pre
$\langle 1 \rangle 4.$ $r \in Int$ BY DEF $Init$
$\langle 1 \rangle 5.$ $pc = \text{"w1"}$BY DEF $Init$
$\langle 1 \rangle 6.$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $\langle 1 \rangle 4$, $\langle 1 \rangle 5$, $Assumption$ DEF $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $Init$

Preservation of $i1$ by $w1$

$stut \triangleq$ UNCHANGED $vars$

LEMMA $w1po1 \triangleq$
ASSUME $InductiveInvariant$, $w1$
PROVE $i1'$
$\langle 1 \rangle$.USE DEF $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre
$\langle 1 \rangle 1.$ $a = a0 \wedge b = b0 \wedge ((a < b) \vee (a \geq b))$ BY SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, ma
$\langle 1 \rangle$a.CASE $a < b$
$\langle 2 \rangle 1.$ $pc = \text{"w1"} \wedge a < b \wedge r' = b \wedge pc' = \text{"Done"} \wedge$ UNCHANGED $\langle a, b \rangle$
BY $\langle 1 \rangle$a, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$
$\langle 2 \rangle 2.$ $pc' = \text{"Done"} \Rightarrow r' = maximum(a0, b0)$
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$
$\langle 2 \rangle 3.$ $i1'$
BY $\langle 2 \rangle 2$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$
$\langle 2 \rangle$.QED
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, SMTDEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$
$\langle 1 \rangle$b.CASE $a \geq b$
$\langle 2 \rangle 1.$ $pc = \text{"w1"} \wedge a \geq b \wedge r' = a \wedge pc' = \text{"Done"} \wedge$ UNCHANGED $\langle a, b \rangle$
BY $\langle 1 \rangle$b, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$
$\langle 2 \rangle 2.$ $pc' = \text{"Done"} \Rightarrow r' = maximum(a0, b0)$
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $w1$, $typeInt$, pre, $maximum$

$\langle 2\rangle 3.$ $i1'$
BY $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 2\rangle 2$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*
$\langle 2\rangle$.QED
BY $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, *SMT*DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*
$\langle 1\rangle 2.$ QED
BY $\langle 1\rangle$a, $\langle 1\rangle$b, *SMT*DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

Preservation of $i1$ by *Terminating*

LEMMA *Terminatingpo*1 $\triangleq$
ASSUME *InductiveInvariant*, *Terminating*
PROVE $i1'$
$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i1$, $w1$, *typeInt*, *pre*, *vars*
$\langle 1\rangle 1$ $pc =$ "Done" $\land$ UNCHANGED *vars*
BY *SMT* DEF *Terminating*
$\langle 1\rangle 2$ $i1'$
BY *SMT* DEF *Terminating*
$\langle 1\rangle 3$ QED
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, *SMT*

Preservation of $i1$ by stuttering

LEMMA *stutteringpo* $\triangleq$
ASSUME *InductiveInvariant*, *stut*
PROVE $i1'$
$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i1$, *stut*, *typeInt*, *pre*, *vars*
$\langle 1\rangle 1$ $i1'$
BY *SMT*
$\langle 1\rangle 2$ QED
BY $\langle 1\rangle 1$, *SMT*

Preservation of $i1$ by *Next*

LEMMA *NextP*1 $\triangleq$
ASSUME *InductiveInvariant*, *Next*
PROVE $i1'$

BY $w1po1$, *Terminatingpo*1 DEFS *Next*, *InductiveInvariant*, $i1$, $w1$, *Terminating*, *typeInt*, *pre*, *vars*, *maxim*

Preservation of $i0$ by $w1$

LEMMA $w1po0$ $\triangleq$
ASSUME *InductiveInvariant*, $w1$
PROVE $i0'$
$\langle 1\rangle$.USE DEF *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*
$\langle 1\rangle 1.$ $a = a0 \land b = b0$ BY *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*
$\langle 1\rangle$a.CASE $a < b$

$\langle 2\rangle 1.$ $pc = \text{"w1"} \wedge a' = a0 \wedge b' = b0 \wedge pc' = \text{"Done"} \wedge \textsc{unchanged}\ \langle a, b\rangle$

BY $\langle 1\rangle$a, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle 2.$ $a' = a0 \wedge b' = b0$

BY $\langle 1\rangle$a, $\langle 2\rangle 1$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle 3.$ $i0'$

BY $\langle 2\rangle 2$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle$.QED

BY $\langle 1\rangle$a, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, *SMT*DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 1\rangle$b.CASE $a \geq b$

$\langle 2\rangle 1.$ $pc = \text{"w1"} \wedge a' = a0 \wedge b' = b0 \wedge pc' = \text{"Done"} \wedge \textsc{unchanged}\ \langle a, b\rangle$

BY $\langle 1\rangle$b, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle 2.$ $a' = a0 \wedge b' = b0$

BY $\langle 1\rangle$b, $\langle 2\rangle 1$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle 3.$ $i0'$

BY $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 2\rangle 2$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 2\rangle$.QED

BY $\langle 1\rangle$b, $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, *SMT*DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

$\langle 1\rangle 2.$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle$a, $\langle 1\rangle$b, *SMT*DEFS *InductiveInvariant*, $i1$, $i0$, $w1$, *typeInt*, *pre*, *maximum*

LEMMA *Terminatingpo*0 $\triangleq$

ASSUME *InductiveInvariant*, *Terminating*

PROVE $i0'$

$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i0$, $w1$, *typeInt*, *pre*, *vars*

$\langle 1\rangle 1$ $pc = \text{"Done"} \wedge \textsc{unchanged}\ vars$

BY *SMT* DEF *Terminating*

$\langle 1\rangle 2$ $i0'$

BY *SMT* DEF *Terminating*

$\langle 1\rangle 3$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, *SMT*

Preservation of $w1$ by *Terminating*

LEMMA *stutteringpo*0 $\triangleq$

ASSUME *InductiveInvariant*, *stut*

PROVE $i0'$

$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i0$, *stut*, *typeInt*, *pre*, *vars*

$\langle 1\rangle 1$ $i0'$

BY *SMT*

$\langle 1\rangle 2$ QED

BY $\langle 1\rangle 1$, *SMT*

Preservation of $i0$ by *Next*

LEMMA *NextP*0 $\triangleq$

ASSUME *InductiveInvariant*, *Next*

PROVE $i0'$

BY $w1po0$, $Terminatingpo0$ DEFS $Next$, $InductiveInvariant$, $i1$, $w1$, $Terminating$, $typeInt$, pre, $vars$, $maxim$

Preservation of *InductiveInvariant* by *Next*

LEMMA $NextP \triangleq$
ASSUME $InductiveInvariant$, $Next$
PROVE $InductiveInvariant'$

BY $NextP1$, $NextP0$DEFS $Next$, $InductiveInvariant$, $i1$, $i0$,
$w1$, $Terminating$, $typeInt$, pre, $vars$

Preservation of *InductiveInvariant* by *Next* with stuttering

LEMMA $NNextInvariant \triangleq$
ASSUME $InductiveInvariant$, $[Next]_{vars}$
PROVE $InductiveInvariant'$

BY $NextP$, $stutteringpo$, $stutteringpo0$, PTL DEF $Next$, $stut$, $InductiveInvariant$, $vars$

Preservation of *InductiveInvariant* by *Next* with stuttering

THEOREM $INV \triangleq InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY $NNextInvariant$DEFS $InductiveInvariant$, $i1$, $w1$, $Terminating$, $typeInt$, pre, $vars$

The *PlusCal* algorithm satisfies *InductiveInvariant*
THEOREM $Invariance \triangleq Spec \Rightarrow \Box InductiveInvariant$
$\langle 1 \rangle 1$ $InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY INV DEF $InductiveInvariant$, $i1$, $w1$, $Terminating$, $typeInt$, pre, $vars$
$\langle 1 \rangle 2$ $Init \Rightarrow InductiveInvariant$
BY $InitProperty$ DEF $InductiveInvariant$, $i1$, $w1$, $Terminating$, $typeInt$, pre, $vars$
$\langle 1 \rangle 3$ $Spec \Rightarrow \Box InductiveInvariant$
BY PTL, $InitProperty$, $NextP$, $\langle 1 \rangle 1$ DEF $Spec$, $InductiveInvariant$, $i1$, $w1$, $Terminating$, $typeInt$, pre, $vars$
$\langle 1 \rangle$ QED
BY PTL, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$