MODULE *TLAPROOFINC*

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

CONSTANTS $x0$

$typeInt(u) \triangleq u \in Int$
$pre(u) \triangleq u \in Nat$

--algorithm *inc* **{**
variables $x = x0$ **;**
{
$x := x + 1$ **;**
}
}

BEGIN TRANSLATION ($chksum(pcal) =$ "e23deda2" $\wedge\ chksum(tla) =$ "9a71d89e")

VARIABLES x, pc

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

$Init \triangleq$ Global variables
$\wedge\ x = x0$
$\wedge\ pc =$ "Lbl_1"

$evt1 \triangleq \wedge\ pc =$ "Lbl_1"
$\wedge\ x' = x + 1$
$\wedge\ pc' =$ "Done"

Allow infinite stuttering to prevent deadlock on termination.

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

$Next \triangleq evt1$
$\vee\ Terminating$

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

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

END TRANSLATION

$i1 \triangleq typeInt(x) \wedge pc \in \{$"Lbl_1", "Done"$\}$
$i2 \triangleq x \in x0 \,..\, x0 + 1$
$i3 \triangleq pc =$ "Done" $\Rightarrow x = x0 + 1$
$i4 \triangleq pc =$ "Lbl_1" $\Rightarrow x = x0$
$InductiveInvariant \triangleq i1 \wedge i2 \wedge i3 \wedge i4$

ASSUME $Assumption \triangleq pre(x0)$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$
$\langle 1 \rangle$ SUFFICES ASSUME $Init$
PROVE $InductiveInvariant$
OBVIOUS
$\langle 1 \rangle 1$. $x = x0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 2$. $pre(x0)$ BY $Assumption$ DEF $Init$
$\langle 1 \rangle 3$. QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ DEF $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $Init$, $typeInt$, pre

THEOREM $Init \Rightarrow InductiveInvariant$
BY $Assumption$ DEF $Init$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $typeInt$, pre

LEMMA $evt1po1 \triangleq$
ASSUME $InductiveInvariant$, $evt1$
PROVE $i1'$
BY DEFS $InductiveInvariant$, $evt1$, $typeInt$, pre, $vars$, $i1$, $i2$, $i3$, $i4$

LEMMA $evt1po2 \triangleq$
ASSUME $InductiveInvariant$, $evt1$
PROVE $i2'$
BY DEFS $InductiveInvariant$, $evt1$, $typeInt$, pre, $vars$, $i1$, $i2$, $i3$, $i4$

LEMMA $evt1po3 \triangleq$
ASSUME $InductiveInvariant$, $evt1$
PROVE $i3'$
BY DEFS $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $evt1$, $typeInt$, pre, $vars$

LEMMA $evt1po4 \triangleq$
ASSUME $InductiveInvariant$, $evt1$
PROVE $i4'$
BY DEFS $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $evt1$, $typeInt$, pre, $vars$

LEMMA $evt1po \triangleq$
ASSUME $InductiveInvariant$, $evt1$
PROVE $InductiveInvariant'$
BY $evt1po1$, $evt1po2$, $evt1po3$, $evt1po4$, PTLDEFS $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $evt1$, $typeInt$, pre, $vars$

LEMMA $Terminatingpo \triangleq$

ASSUME $InductiveInvariant$, $Terminating$
PROVE $InductiveInvariant'$
BY DEFS $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $Terminating$, $typeInt$, pre, $vars$

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

BY $evt1po$, $Terminatingpo$, PTL DEF $Next$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $evt1$, $typeInt$, pre, $vars$

$stut \triangleq$ UNCHANGED $\langle x, pc \rangle$

LEMMA $stutteringpo \triangleq$
ASSUME $InductiveInvariant$, $stut$
PROVE $InductiveInvariant'$
BY DEFS $stut$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $evt1$, $typeInt$, pre, $vars$

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

BY $NextP$, $stutteringpo$, PTL DEF $Next$, $stut$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $stut$, $typeInt$, pre, $vars$

THEOREM $INV \triangleq InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY $NNextInvariant$DEFS $Next$, $stut$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $stut$, $typeInt$, pre, $vars$

THEOREM $Invariance \triangleq Spec \Rightarrow \Box InductiveInvariant$
$\langle 1 \rangle 1$ $InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY INV DEF $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $typeInt$
$\langle 1 \rangle 2$ $Init \Rightarrow InductiveInvariant$
BY $InitProperty$ DEF $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $typeInt$
$\langle 1 \rangle 3$ $Spec \Rightarrow \Box InductiveInvariant$
BY PTL, $InitProperty$, $NextP$, $\langle 1 \rangle 1$ DEF $Spec$, $InductiveInvariant$, $i1$, $i2$, $i3$, $i4$, $typeInt$
$\langle 1 \rangle$ QED
BY PTL, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$