MODULE *TLAPROOFINC1*

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

CONSTANTS $x0$

auxiliary definitions

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

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

PlusCal algorithm

```
--algorithm inc{
  variables x = x0 ;
  {
  evt1: x := x + 1 ;
   }
 }
```

invariants

$i1 \triangleq typeInt(x) \land pc \in \{\text{"evt1"}, \text{"Done"}\}$

$i2 \triangleq x \in x0 \,..\, x0 + 1$

$i3 \triangleq pc = \text{"Done"} \Rightarrow x = x0 + 1$

$i4 \triangleq pc = \text{"evt1"} \Rightarrow x = x0$

$InductiveInvariant \triangleq i1 \land i2 \land i3 \land i4$

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 $\mathit{InductiveInvariant}$, $[\mathit{Next}]_{\mathit{vars}}$
PROVE $\mathit{InductiveInvariant}'$

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

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

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