MODULE *TLAPROOFVECTSUM*

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

CONSTANTS $n0$, $v0$

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

$pre(u, v) \triangleq u \in Nat \land u \neq 0 \land v \in [1 \,..\, n0 \rightarrow Int]$

$v0 \triangleq [i \in 1 \,..\, n0 \mapsto i]$

```
--algorithm sumvect {
variables n = n0, v = v0, i = 0, cu = 0, r ;
{
w1: while ( i ≠ n ) {
  w2: cu := cu + v[i + 1] ;
  i := i + 1 ;
 } ;
w3: r := cu ;
 }
 }
```

BEGIN TRANSLATION ($chksum(pcal) =$ "42832d85" $\land$ $chksum(tla) =$ "19fa4b63")

CONSTANT *defaultInitValue*

VARIABLES n, v, i, cu, r, pc

$vars \triangleq \langle n, v, i, cu, r, pc \rangle$

$Init \triangleq$ Global variables
$\land n = n0$
$\land v = v0$
$\land i = 0$
$\land cu = 0$
$\land r \in Int$
$\land pc =$ "w1"

$w1 \triangleq \land pc =$ "w1"
$\land$ IF $i \neq n$
THEN $\land pc' =$ "w2"
ELSE $\land pc' =$ "w3"
$\land$ UNCHANGED $\langle n, v, i, cu, r \rangle$

$w2 \triangleq \land pc =$ "w2"
$\land cu' = cu + v[i + 1]$
$\land i' = i + 1$
$\land pc' =$ "w1"
$\land$ UNCHANGED $\langle n, v, r \rangle$

$w3 \triangleq \land pc =$ "w3"

$\land\ r' = cu$
$\land\ pc' =$ "Done"
$\land$ UNCHANGED $\langle n,\ v,\ i,\ cu\rangle$

Allow infinite stuttering to prevent deadlock on termination.
$Terminating \triangleq pc =$ "Done" $\land$ UNCHANGED $vars$

$Next \triangleq w1 \lor w2 \lor w3$
$\lor\ Terminating$

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

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

END TRANSLATION

$u[k \in 0\,..\,n0] \triangleq$ IF $k = 0$ THEN 0 ELSE $u[k-1] + v0[k]$
$i00 \triangleq cu = u[i] \land (pc =$ "w1" $\Rightarrow i \leq n) \land (pc =$ "w2" $\Rightarrow i < n) \land (pc =$ "w3" $\Rightarrow i = n)$
$i0 \triangleq typeInt(n) \land typeInt(i) \land typeInt(cu) \land typeInt(r) \land v = v0 \land n = n0 \land i \in 0\,..\,n0$
$i2 \triangleq cu = u[i]$
$i1 \triangleq pc =$ "w3" $\Rightarrow cu = u[n] \land i = n$

$InductiveInvariant \triangleq i1 \land i0 \land i00$

AXIOM $U1 \triangleq u[0] = 0$
AXIOM $U2 \triangleq \forall\, k \in 0\,..\,n0 - 1 : u[k+1] = u[k] + v0[k+1]$

ASSUME $Assumption \triangleq pre(n0,\ v0)$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$
$\langle 1\rangle$ SUFFICES ASSUME $Init$
PROVE $InductiveInvariant$
OBVIOUS
$\langle 1\rangle 1.$ $n = n0$BY $Assumption$ DEF $Init$
$\langle 1\rangle 2.$ $pre(n0,\ v0)$ BY $Assumption$ DEF $Init$
$\langle 1\rangle 3.$ $v = v0$BY DEF $Init$
$\langle 1\rangle 4.$ $i = 0$BY DEF $Init$
$\langle 1\rangle 5.$ $cu = 0$BY DEF $Init$
$\langle 1\rangle 6.$ $r \in Int$ BY DEF $Init$
$\langle 1\rangle 7.$ $pc =$ "w1"BY DEF $Init$
$\langle 1\rangle 8.$ $cu = u[0]$BY $U1$ DEF $Init$
$\langle 1\rangle 9.$ $(pc =$ "w1" $\Rightarrow i \leq n)$BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 4$, $\langle 1\rangle 7$, SMT DEF $Init$, pre, $i00$, $i0$, $i1$
$\langle 1\rangle 10.$ $(pc =$ "w2" $\Rightarrow i < n)$BY DEF $Init$
$\langle 1\rangle 11.$ $(pc =$ "w3" $\Rightarrow i = n)$ BY DEF $Init$
$\langle 1\rangle 12.$ QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$, $\langle 1\rangle 6$, $\langle 1\rangle 7$, $\langle 1\rangle 8$, $\langle 1\rangle 9$, $\langle 1\rangle 10$, $\langle 1\rangle 11$ DEF $InductiveInvariant$, $i1$, $i0$,

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

start

LEMMA $w1po1 \triangleq$
ASSUME $InductiveInvariant$, $w1$
PROVE $i1'$

$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre

$\langle 1 \rangle 1$ $(i \neq n) \lor (i = n)$
OBVIOUS

$\langle 1 \rangle$aCASE $i \neq n$
$\langle 2 \rangle 1$ $pc' =$ "w2" $\land$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$a, SMT
$\langle 2 \rangle 2$ $i1'$
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $U1$, $U2$, SMT
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMT
$\langle 1 \rangle$bCASE $i = n$
$\langle 2 \rangle 1$ $pc =$ "w1" $\land i = n \land cu' = u[i'] \land cu' = cu \land i' = i \land pc' =$ "w3" $\land$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$b, $U1$, $U2$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 2 \rangle 2$ $i1'$
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, $U1$, $U2$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMTDEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 1 \rangle 2$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle$a, $\langle 1 \rangle$b, $U1$, $U2$, SMTDEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre

LEMMA $w2po1 \triangleq$
ASSUME $InductiveInvariant$, $w2$
PROVE $i1'$
$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i1$, $w2$, $typeInt$, pre
$\langle 1 \rangle 1$ $pc =$ "w2" $\land cu' = cu + v[i+1] \land i' = i + 1 \land pc' =$ "w1" $\land$ UNCHANGED $\langle n, v, r \rangle$
BY $U2$, SMT
$\langle 1 \rangle 2$ $i1'$
BY $\langle 1 \rangle 1$, SMT
$\langle 1 \rangle 3$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, SMT

LEMMA $w3po1 \triangleq$
ASSUME $InductiveInvariant$, $w3$
PROVE $i1'$
$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i1$, $w3$, $typeInt$, pre
$\langle 1 \rangle 1$ $pc =$ "w3" $\land r' = cu \land pc' =$ "Done" $\land$ UNCHANGED $\langle n, v, i, cu \rangle$
BY $U2$, SMT

$\langle 1 \rangle 2\ i = n \wedge cu = u[n]$ BY $U1,\ U2,\ SMT$
$\langle 1 \rangle 3\ i1'$
BY $\langle 1 \rangle 1,\ \langle 1 \rangle 2,\ U2,\ SMT$
$\langle 1 \rangle 4$ QED BY $\langle 1 \rangle 1,\ \langle 1 \rangle 2,\ \langle 1 \rangle 3,\ U2,\ SMT$

LEMMA $Terminatingpo1 \triangleq$
ASSUME $InductiveInvariant,\ Terminating$
PROVE $i1'$
$\langle 1 \rangle$ USE DEF $InductiveInvariant,\ i1,\ w3,\ typeInt,\ pre,\ vars$
$\langle 1 \rangle 1\ pc =$ "Done" $\wedge$ UNCHANGED $vars$
BY SMT DEF $Terminating$
$\langle 1 \rangle 2\ i1'$
BY SMT DEF $Terminating$
$\langle 1 \rangle 3$ QED
BY $\langle 1 \rangle 1,\ \langle 1 \rangle 2,\ SMT$

$stut \triangleq$ UNCHANGED $vars$

LEMMA $stutteringpo1 \triangleq$
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 $\langle 1 \rangle 1,\ SMT$

LEMMA $NextP1 \triangleq$
ASSUME $InductiveInvariant,\ Next$
PROVE $i1'$

BY $w1po1,\ w2po1,\ w3po1,\ Terminatingpo1$ DEFS $Next,\ InductiveInvariant,\ i1,\ w1,\ w2,\ w3,\ Terminating,\ ty$

end

$i0$

LEMMA $w1po0 \triangleq$
ASSUME $InductiveInvariant,\ w1$
PROVE $i0'$

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

$\langle 1 \rangle 1$ $(i \neq n) \vee (i = n)$
OBVIOUS

$\langle 1 \rangle$aCASE $i \neq n$
$\langle 2 \rangle 1$ $pc' =$ "w2" $\wedge$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$a, SMT
$\langle 2 \rangle 2$ $i0'$
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, SMT
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMT
$\langle 1 \rangle$bCASE $i = n$
$\langle 2 \rangle 1$ $pc' =$ "w3" $\wedge$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$b, SMT
$\langle 2 \rangle 2$ $i0'$
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, SMT
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMT
$\langle 1 \rangle 2$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle$a, $\langle 1 \rangle$b, SMT

LEMMA $w2po0 \triangleq$
ASSUME $InductiveInvariant$, $w2$
PROVE $i0'$
$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i0$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 1$ $pc =$ "w2" $\wedge$ UNCHANGED $\langle n, v, r \rangle$
BY SMT
$\langle 1 \rangle 2$ $typeInt(n) \wedge typeInt(i) \wedge typeInt(cu) \wedge typeInt(r) \wedge v = v0 \wedge i \in 0 \,..\, n0 \wedge$ UNCHANGED $\langle n, v, r \rangle$
BY $U1$, SMT DEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 3$ $typeInt(n') \wedge typeInt(i') \wedge typeInt(cu') \wedge typeInt(r') \wedge v' = v0 \wedge$ UNCHANGED $\langle n, v, r \rangle$
BY SMT DEFS $InductiveInvariant$, $i0$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 4$ $i < n \wedge i' = i + 1$
BY SMT DEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 5$ $i \in 0 \,..\, n0 \wedge i < n$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 6$ $n = n0 \wedge i < n0$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 5$, $\langle 1 \rangle 3$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 7$ $i \in 0 \,..\, n0 - 1$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 5$, $\langle 1 \rangle 6$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 8$ $i' \in 0 \,..\, n0$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 5$, $\langle 1 \rangle 6$, $\langle 1 \rangle 7$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 9$ $n' = n0 \wedge v' = v0$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeInt$, pre, u
$\langle 1 \rangle 20$ $i0'$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $\langle 1 \rangle 4$, $\langle 1 \rangle 5$, $\langle 1 \rangle 6$, $\langle 1 \rangle 7$, $\langle 1 \rangle 8$, $\langle 1 \rangle 9$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w2$, $typeI$
$\langle 1 \rangle 21$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\langle 1\rangle 5$, $\langle 1\rangle 6$, $\langle 1\rangle 7$, $\langle 1\rangle 8$, $\langle 1\rangle 9$, $\langle 1\rangle 20$, *SMT* DEFS *InductiveInvariant*, $i0$, $i1$, $i00$, w

LEMMA $w3po0 \triangleq$
ASSUME *InductiveInvariant*, $w3$
PROVE $i0'$
$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i0$, $i1$, $i00$, $w3$, *typeInt*, *pre*
$\langle 1\rangle 1$ $pc = \text{"w3"} \land r' = cu \land pc' = \text{"Done"} \land \text{UNCHANGED } \langle n, v, i, cu\rangle$
BY $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i0$, $i1$, $i00$, $w3$, *typeInt*, *pre*
$\langle 1\rangle 2$ $i = n \land cu = u[n]$ BY $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i0$, $i1$, $i00$, $w3$, *typeInt*, *pre*
$\langle 1\rangle 3$ $i0'$
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i0$, $i1$, $i00$, $w3$, *typeInt*, *pre*
$\langle 1\rangle 4$ QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $\langle 1\rangle 3$, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i0$, $i1$, $i00$, $w3$, *typeInt*, *pre*

LEMMA $Terminatingpo0 \triangleq$
ASSUME *InductiveInvariant*, *Terminating*
PROVE $i0'$
$\langle 1\rangle$ USE DEF *InductiveInvariant*, $i0$, $w3$, *typeInt*, *pre*, *vars*
$\langle 1\rangle 1$ $pc = \text{"Done"} \land \text{UNCHANGED } vars$
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*

LEMMA $stutteringpo0 \triangleq$
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*

LEMMA $NextP0 \triangleq$
ASSUME *InductiveInvariant*, *Next*
PROVE $i0'$

BY $w1po0$, $w2po0$, $w3po0$, $Terminatingpo0$ DEFS *Next*, *InductiveInvariant*, $i0$, $w1$, $w2$, $w3$, *Terminating*, *ty*

$i0$

$i00$

LEMMA $w1po00 \triangleq$
ASSUME $InductiveInvariant$, $w1$
PROVE $i00'$

$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i00$, $i1$, $i0$, $w1$, $typeInt$, pre

$\langle 1 \rangle 1$ $(i \neq n) \lor (i = n)$
OBVIOUS

$\langle 1 \rangle$aCASE $i \neq n$
$\langle 2 \rangle 1$ $pc' =$ "w2" $\land$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$a, SMT
$\langle 2 \rangle 2$ $i1'$
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $U1$, $U2$, SMT
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$a, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMT
$\langle 1 \rangle$bCASE $i = n$
$\langle 2 \rangle 1$ $pc =$ "w1" $\land i = n \land cu' = u[i'] \land cu' = cu \land i' = i \land pc' =$ "w3" $\land$ UNCHANGED $\langle n, v, i, cu, r \rangle$
BY $\langle 1 \rangle$b, $U1$, $U2$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 2 \rangle 2$ $i00'$
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, $U1$, $U2$, SMT DEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 2 \rangle$ QED
BY $\langle 1 \rangle$b, $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, SMTDEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre
$\langle 1 \rangle 2$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle$a, $\langle 1 \rangle$b, $U1$, $U2$, SMTDEFS $InductiveInvariant$, $i1$, $i0$, $i00$, $w1$, $typeInt$, pre

LEMMA $w3po00 \triangleq$
ASSUME $InductiveInvariant$, $w3$
PROVE $i00'$
$\langle 1 \rangle$ USE DEF $InductiveInvariant$, $i0$, $i1$, $i00$, $w3$, $typeInt$, pre
$\langle 1 \rangle 1$ $pc =$ "w3" $\land r' = cu \land pc' =$ "Done" $\land$ UNCHANGED $\langle n, v, i, cu \rangle$
BY $U1$, $U2$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w3$, $typeInt$, pre
$\langle 1 \rangle 2$ $i = n \land cu = u[n]$ BY $U1$, $U2$, SMT DEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w3$, $typeInt$, pre
$\langle 1 \rangle 3$ $i00'$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $U1$, $U2$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w3$, $typeInt$, pre
$\langle 1 \rangle 4$ QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $U1$, $U2$, SMTDEFS $InductiveInvariant$, $i0$, $i1$, $i00$, $w3$, $typeInt$, pre

LEMMA $w2po00 \triangleq$

ASSUME *InductiveInvariant*, $w2$
PROVE $i00'$
⟨1⟩ USE DEF *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩1 $pc =$ "w2" $\land$ UNCHANGED $\langle n, v, r \rangle$
BY *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩2 $v = v0 \land n = n0$
BY *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩3 $v' = v0$ BY ⟨1⟩1, ⟨1⟩2, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩4 $n' = n0$ BY ⟨1⟩1, ⟨1⟩2, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩5 $cu = u[i]$BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*, u
⟨1⟩6 $cu' = cu + v0[i+1]$BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*,
⟨1⟩7 $i' = i + 1$
BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *Isa*, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*, u
⟨1⟩8 $u[i'] = u[i+1] \land i \in 0 \,..\, n0 - 1$
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩4, ⟨1⟩5, $U1$, $U2$, *Isa*, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*, u
⟨1⟩9 $u[i+1] = u[i] + v0[i+1]$
BY $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*, u
⟨1⟩10 $cu' = u[i'] \land u[i'] = u[i+1] \land u[i+1] = u[i] + v0[i+1]$
BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *Isa*, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*
⟨1⟩11 $(pc =$ "w1" $\Rightarrow i \leq n) \land i \leq n \land (pc' =$ "w1" $\Rightarrow i' \leq n') \land i' \leq n'$
BY ⟨1⟩1, ⟨1⟩2, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*, $U1$, $U2$
⟨1⟩12 $(pc =$ "w2" $\Rightarrow i < n) \land (pc' =$ "w2" $\Rightarrow i' < n')$
BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*

⟨1⟩13 $(pc =$ "w3" $\Rightarrow i = n) \land (pc' =$ "w3" $\Rightarrow i' = n')$
BY ⟨1⟩1, ⟨1⟩2, $U1$, $U2$, *SMT* DEFS *InductiveInvariant*, $i00$, $i0$, $i1$, $w2$, *typeInt*, *pre*

⟨1⟩14 $i00'$
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, ⟨1⟩4, ⟨1⟩5, ⟨1⟩6, ⟨1⟩7, ⟨1⟩8, ⟨1⟩9, ⟨1⟩10, ⟨1⟩11, $U1$, $U2$, *SMT* DEFS *InductiveInvarian*
⟨1⟩15 QED
BY ⟨1⟩1, ⟨1⟩2, ⟨1⟩3, ⟨1⟩4, ⟨1⟩5, ⟨1⟩6, ⟨1⟩7, ⟨1⟩8, ⟨1⟩9, ⟨1⟩10, ⟨1⟩11, ⟨1⟩12, *SMT* DEFS *InductiveInvariant*,

LEMMA *Terminatingpo00* $\triangleq$
ASSUME *InductiveInvariant*, *Terminating*
PROVE $i00'$
⟨1⟩ USE DEF *InductiveInvariant*, $i00$, $w3$, *typeInt*, *pre*, *vars*
⟨1⟩1 $pc =$ "Done" $\land$ UNCHANGED *vars*
BY *SMT* DEF *Terminating*
⟨1⟩2 $i00'$
BY *SMT* DEF *Terminating*
⟨1⟩3 QED
BY ⟨1⟩1, ⟨1⟩2, *SMT*

LEMMA *stutteringpo*00 $\triangleq$
ASSUME *InductiveInvariant*, *stut*
PROVE $i00'$
$\langle 1\rangle 1$ $i00'$
BY *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $i00$, *stut*, *typeInt*, *pre*, *vars*
$\langle 1\rangle 2$ QED
BY $\langle 1\rangle 1$, *SMT* DEFS *InductiveInvariant*, $i1$, $i0$, $i00$, *stut*, *typeInt*, *pre*, *vars*

LEMMA *NextP*00 $\triangleq$
ASSUME *InductiveInvariant*, *Next*
PROVE $i00'$

BY $w1po00$, $w2po00$, $w3po00$, *Terminatingpo*00 DEFS *Next*, *InductiveInvariant*, $i0$, $w1$, $w2$, $w3$, *Terminating*

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

BY $U1$, $U2$, *NextP*1, *NextP*0, *NextP*00, *SMT* DEFS *Next*, *InductiveInvariant*, $i1$, $i0$, $i00$, $w1$, $w2$, $w3$, *Termi*

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

BY *NextP*, *stutteringpo*1, *stutteringpo*0, *stutteringpo*00, *PTL*, *SMT* DEFS *Next*, *InductiveInvariant*, $i1$, $i0$, $i00$

THEOREM *INV* $\triangleq$ $InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY *NNextInvariant* DEFS *InductiveInvariant*, $i1$, $w1$, $w2$, $w3$, *Terminating*, *typeInt*, *pre*, *vars*

THEOREM *Invariance* $\triangleq$ $Spec \Rightarrow \Box InductiveInvariant$
$\langle 1\rangle 1$ $InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY *INV* DEF *InductiveInvariant*, $i1$, $w1$, $w2$, $w3$, *Terminating*, *typeInt*, *pre*, *vars*
$\langle 1\rangle 2$ $Init \Rightarrow InductiveInvariant$
BY *InitProperty* DEF *InductiveInvariant*, $i1$, $w1$, $w2$, $w3$, *Terminating*, *typeInt*, *pre*, *vars*
$\langle 1\rangle 3$ $Spec \Rightarrow \Box InductiveInvariant$
BY *PTL*, *InitProperty*, *NextP*, $\langle 1\rangle 1$ DEF *Spec*, *InductiveInvariant*, $i1$, $w1$, $w2$, $w3$, *Terminating*, *typeInt*, *p*
$\langle 1\rangle$ QED
BY *PTL*, $\langle 1\rangle 2$, $\langle 1\rangle 3$