MODULE *TLAPROOF12*

EXTENDS *Integers*, *TLC*, *TLAPS*

CONSTANTS $x0,\ y0,\ z0$

$pre \triangleq x0 = 10 \land z0 = 2 * x0 \land y0 = z0 + x0$
$L \triangleq \{\text{"l1"}, \text{"l2"}\}$

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

ASSUME *pre*

--algorithm *test* **{**
variables $x = x0,\ z = z0,\ y = y0$ **;**
{
$l1$: $y := z + x$ **;**
}
}

BEGIN TRANSLATION ($chksum(pcal) =$ "66c6fc76" $\land$ $chksum(tla) =$ "678ca025")

VARIABLES $x,\ z,\ y,\ pc$

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

$Init \triangleq$ Global variables
$\land x = x0$
$\land z = z0$
$\land y = y0$
$\land pc = \text{"l1"}$

$l1 \triangleq \land pc = \text{"l1"}$
$\land y' = z + x$
$\land pc' = \text{"Done"}$
$\land$ UNCHANGED $\langle x,\ z\rangle$

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

$Next \triangleq l1$
$\lor Terminating$

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

$Termination \triangleq \Diamond(pc = \text{"Done"})$

END TRANSLATION

ASSUME pre

$MAX \triangleq 32767$ 16 bits
$D \triangleq -32768 \,..\, 32767$
$x \leq 32760$

$DD(X) \triangleq (X \in D)$

$InductiveInvariant \triangleq$
$\quad \land pc \in \{\text{"l1"}, \text{"Done"}\}$
$\quad \land x \in Int \land y \in Int \land z \in Int$
$\quad \land pc = \text{"l1"} \Rightarrow x = 10 \land z = 2 * x \land y = z + x$
$\quad \land pc = \text{"Done"} \Rightarrow x = 10 \land y = x + 2 * 10$

$Inv \triangleq InductiveInvariant$
$Safety\_Partial\_Correctness \triangleq pc = \text{"Done"} \Rightarrow x = 10 \land y = x + 2 * 10$

$Safety\_rte \triangleq DD(x) \land DD(y) \land DD(z)$

$check \triangleq Inv \land Safety\_Partial\_Correctness \land Safety\_rte$

$prop \triangleq \Box(x = x0)$
$thepre \triangleq pre$

ASSUME $Assumption \triangleq pre$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$
$\langle 1 \rangle$ SUFFICES ASSUME $Init$
PROVE $InductiveInvariant$
OBVIOUS
$\langle 1 \rangle 1.$ $x = x0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 2.$ $y = y0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 3.$ $z = z0$BY $Assumption$ DEF $Init$
$\langle 1 \rangle 4.$ $pc = \text{"l1"}$ BY $Assumption$ DEF $Init$
$\langle 1 \rangle$.QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $\langle 1 \rangle 4$ DEF $InductiveInvariant$, $typeInt$, pre

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

LEMMA $truc \triangleq$
ASSUME $InductiveInvariant$, $l1$
PROVE $InductiveInvariant'$
BY DEFS $InductiveInvariant$, $l1$, $typeInt$

THEOREM $NextProperty \triangleq$
ASSUME $InductiveInvariant$, $[Next]_{\langle x \rangle}$
PROVE $InductiveInvariant'$

$\langle 1 \rangle$ SUFFICES ASSUME $InductiveInvariant \land [Next]_{\langle x \rangle}$
PROVE $InductiveInvariant'$
OBVIOUS
$\langle 1 \rangle 1.$ $x' \in 0 \,..\, x0 \land typeInt(x') \Rightarrow InductiveInvariant'$
BY PTL DEF $InductiveInvariant$
$\langle 1 \rangle 2.$
ASSUME $InductiveInvariant$, $l1$
PROVE $InductiveInvariant'$
BY $Zenon$, SMT, PTL DEF $InductiveInvariant$, $l1$, $typeInt$
$\langle 1 \rangle$.QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $Zenon$, SMT, PTL DEF $InductiveInvariant$, $typeInt$, $thepre$, pre

THEOREM $Correctness \triangleq Spec \Rightarrow \Box InductiveInvariant$
$\langle 1 \rangle 1.$ $Init \Rightarrow InductiveInvariant$
BY $Assumption$ DEF $Init$, $InductiveInvariant$, $typeInt$, $thepre$, pre
$\langle 1 \rangle 2.$ $InductiveInvariant \land [Next]_{vars} \Rightarrow InductiveInvariant'$
BY PTL DEF $InductiveInvariant$, $Next$, $typeInt$, $thepre$, $vars$,
$l1$
$\langle 1 \rangle$.QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, PTL DEF $Spec$