MODULE $TLAPROOF5$

EXTENDS $Naturals$, $Integers$, TLC, $TLAPS$

CONSTANTS $x0$, $y0$, $z0$

VARIABLES x, y, z, pc

Auxiliary definitions

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

$pre(u, v, w) \triangleq \land u \in Int \land v \in Int \land w \in Int$

$\quad\quad \land u = 3 \land v = w + u \land w = 2 * u$

$\quad\quad L \triangleq \{\text{"l1"}, \text{"l2"}\}$

Interpretation: we assume that the precondition can hold and we have to find possible values for $x0$,$y0$, $z0$ to validate or not

ASSUME $pre(x0, y0, z0)$

Action for transition of the algorithm

$al1l2 \triangleq$

$\quad \land pc = \text{"l1"}$

$\quad \land pc' = \text{"l2"}$

$\quad \land y' = z + x$

$\quad \land z' = z \land x' = x$

Computations

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

$Next \triangleq al1l2 \lor \text{UNCHANGED } vars$

$Init \triangleq pc = \text{"l0"} \land x = x0 \land y = y0 \land z = z0 \land pre(x0, y0, z0)$

Checking the annotation by checking the invariant i derived from the annotation

$i \triangleq$

$\quad \land typeInt(x) \land typeInt(y) \quad \land typeInt(z)$

$\quad \land pc = \text{"l1"} \Rightarrow x = x0 \land y = y0 \land z = z0 \land pre(x0, y0, z0)$

$\quad \land pc = \text{"l2"} \Rightarrow x = 3 \land y = x + 6 \land pre(x0, y0, z0)$

$Safe \triangleq i$

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

$InductiveInvariant \triangleq$

$\quad \land typeInt(x) \land typeInt(y) \quad \land typeInt(z)$

$\quad \land pc = \text{"l1"} \Rightarrow x = x0 \land y = y0 \land z = z0 \land pre(x0, y0, z0)$

$\quad \land pc = \text{"l2"} \Rightarrow x = 3 \land y = x + 6 \land pre(x0, y0, z0)$

$thepre \triangleq pre(x0, y0, z0)$

ASSUME $Assumption \triangleq thepre$

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*
$\langle 1 \rangle 4.\ pc =$ "l0" BY *Assumption* DEF *Init*
$\langle 1 \rangle 5.$ *thepre* BY *Assumption* DEF *Init*
$\langle 1 \rangle 7.$ QED
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $\langle 1 \rangle 4$, $\langle 1 \rangle 5$ DEF *InductiveInvariant*,
sm: added *typeInt*, *L*, *thepre*, *pre*

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

THEOREM $NextProperty \triangleq InductiveInvariant \land [Next]_{\langle x,\, y,\, z,\, pc \rangle} \Rightarrow InductiveInvariant'$

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