MODULE *TLASAFETY*

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

CONSTANTS $n0$

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

ASSUME $n0 \in Nat$

VARIABLES x, y

$a \triangleq x \geq 0 \land x' = x + 1 \land y' = y$

$bplus \triangleq y < n0 \land y' = y + 1 \land x' = x$

$bminus \triangleq 0 < y \land y' = y - 1 \land x' = x$

$Init \triangleq x = -1 \land y = 0$

$Next \triangleq a \lor bplus \lor bminus$

$Spec \triangleq Init \land \Box[Next]_{\langle x, y \rangle}$

$Typing \triangleq x \in Int \land y \in Int$

$Safe1 \triangleq x = -1$

$Safe2 \triangleq x \leq 0$

$Safe3 \triangleq 0 \leq y \land y \leq n0$

$InductiveInvariant \triangleq Typing \land Safe1 \land Safe2 \land Safe3$

ASSUME $Assumption \triangleq n0 \in Nat$

THEOREM $InitProperty \triangleq Init \Rightarrow InductiveInvariant$

$\langle 1 \rangle$ SUFFICES ASSUME $Init$

PROVE $InductiveInvariant$

OBVIOUS

$\langle 1 \rangle 1.$ $pre(n0)$ BY $Assumption$ DEF $Init$, pre

$\langle 1 \rangle 2.$ $x = -1$BY DEF $Init$

$\langle 1 \rangle 3.$ $y = 0$BY DEF $Init$

$\langle 1 \rangle 4.$ QED

BY $1 > 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$ DEFS $InductiveInvariant$, $Init$, pre

THEOREM $Invariance \triangleq Spec \Rightarrow \Box InductiveInvariant$

THEOREM $Correctness \triangleq Spec \Rightarrow \Box Safe2$
