MODULE *exemple*

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

CONSTANTS $x0$, $y0$, $z0$, *min*, *max*, *undef*

precondition

ASSUME $x0 = y0 + 3 * z0$

```
--algorithm ex{
  variables x = x0,
            y = y0,
            z = z0 ;

{
l0: assert x = y + 3 * z ∧ ∧ y = y0 ∧ z = z0 ;
    x := y + 3 * z ;
l1: assert x = y0 + 3 * z0 ∧ y = y0 ∧ z = z0 ;
 }
 }
```

BEGIN TRANSLATION ($chksum(pcal) =$ "$d40e24$" $\land$ $chksum(tla) =$ "$b11fc418$")

VARIABLES x, y, z, pc

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

$Init \triangleq$ Global variables
$\land x = x0$
$\land y = y0$
$\land z = z0$
$\land pc =$ "l0"

$l0 \triangleq \land pc =$ "l0"
$\land Assert(x = y + 3 * z \land \land y = y0 \land z = z0,$
"Failure of assertion at line 15, column 5.")
$\land x' = y + 3 * z$
$\land pc' =$ "l1"
$\land$ UNCHANGED $\langle y, z \rangle$

$l1 \triangleq \land pc =$ "l1"
$\land Assert(x = y0 + 3 * z0 \land y = y0 \land z = z0,$
"Failure of assertion at line 17, column 5.")
$\land pc' =$ "Done"
$\land$ UNCHANGED $\langle x, y, z \rangle$

Allow infinite stuttering to prevent deadlock on termination.

$Terminating \triangleq pc =$ "Done" $\land$ UNCHANGED $vars$

$Next \triangleq l0 \lor l1$
$\lor Terminating$

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

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

END TRANSLATION

$ISDEF(X,\ Y) \triangleq X \neq undef \Rightarrow X \in Y$
$DD(X) \triangleq X \neq undef \Rightarrow X \in min\ ..\ max$

$i \triangleq$
$\quad \wedge\ pc \in \{\text{“l0”},\ \text{“l1”},\ \text{“Done”}\}$
$\quad \wedge\ ISDEF(x,\ Int)\ \wedge ISDEF(x,\ Int) \wedge ISDEF(z,\ Int)$
$\quad \wedge\ pc = \text{“l0”} \Rightarrow x = y + 3 * z$
$\quad \wedge\ pc = \text{“l1”} \Rightarrow x + y + z \geq y$
$post \triangleq \quad x = y0 + 3 * z0 \wedge y = y0 \wedge z = z0$

$safetyrte \triangleq DD(x) \wedge DD(y) \wedge DD(z)$
$safetypc \triangleq pc = \text{“Done”} \Rightarrow post$
