MODULE *TrafficLight*

EXTENDS *Integers*

VARIABLE *light*   Single traffic light state

$vars \triangleq \langle light \rangle$
$Colors \triangleq \{\text{“red”}, \text{“yellow”}, \text{“green”}\}$

$TypeOK \triangleq light \in Colors$

$Init \triangleq light = \text{“red”}$

Simple state transitions: *red* → *green* → *yellow* → *red*

$$\begin{array}{l}
Next \triangleq \\
\quad \lor \land light = \text{“red”} \\
\quad \land light' = \text{“green”} \\
\quad \lor \land light = \text{“green”} \\
\quad \land light' = \text{“yellow”} \\
\quad \lor \land light = \text{“yellow”} \\
\quad \land light' = \text{“red”}
\end{array}$$

Safety as a state predicate (for invariant checking)

$$\begin{array}{l}
SafetyInvariant \triangleq \\
\quad light \in Colors
\end{array}$$

Only valid colors are allowed

Safety as a temporal property (for theorem proving)

$$\begin{array}{l}
Safety \triangleq \\
\quad \Box[\\
\quad\quad \land (light = \text{“red”} \Rightarrow light' \in \{\text{“red”}, \text{“green”}\}) \\
\quad\quad \land (light = \text{“green”} \Rightarrow light' \in \{\text{“green”}, \text{“yellow”}\}) \\
\quad\quad \land (light = \text{“yellow”} \Rightarrow light' \in \{\text{“yellow”}, \text{“red”}\}) \\
\quad]_{vars}
\end{array}$$

Liveness: The light must change colors eventually

$$\begin{array}{l}
Liveness \triangleq \\
\quad \land \Box\Diamond(light = \text{“red”}) \\
\quad \land \Box\Diamond(light = \text{“yellow”}) \\
\quad \land \Box\Diamond(light = \text{“green”})
\end{array}$$

The complete specification

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

Theorems

THEOREM $Spec \Rightarrow \Box TypeOK$
THEOREM $Spec \Rightarrow Safety$