MODULE *Clock*

Hour *Clock* example from *Lamport*'s book

EXTENDS *Naturals*, *TLAPS*

VARIABLES *hr*

$HCInit \triangleq hr \in 1 \,..\, 12$
$HCNext \triangleq hr' = \text{IF } hr \neq 12 \text{ THEN } hr + 1 \text{ ELSE } 1$

Specification.

$Spec \triangleq HCInit \wedge \Box[HCNext]_{hr}$

Spec for verify liveness

$FSpec \triangleq HCInit \wedge \Box[HCNext]_{hr}$

$Liveness \triangleq \Diamond(hr = 8)$
$Safety \triangleq (hr \in 1 \,..\, 12)$
$BadSafety \triangleq (hr \in 1 \,..\, 11)$

Thorem proving examples

Lemma for progress of safety

LEMMA $Progress \triangleq Safety \wedge HCNext \Rightarrow Safety'$
$\langle 2 \rangle$ USE DEF *Safety*
$\langle 2 \rangle 1$. $hr \neq 12 \vee hr = 12$
OBVIOUS
$\langle 2 \rangle 2$.CASE $hr \neq 12$
BY DEF *HCNext*
$\langle 2 \rangle 3$.CASE $hr = 12$
BY DEF *HCNext*
$\langle 2 \rangle 4$. QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$

THEOREM $Spec \Rightarrow \Box Safety$
$\langle 1 \rangle$ USE DEF *Safety*
$\langle 1 \rangle 1$. $HCInit \Rightarrow Safety$ We want to refer to non-temporal part of *Safety*!
BY DEF *HCInit*
$\langle 1 \rangle 2$. $Safety \wedge HCNext \Rightarrow Safety'$
BY *Progress*
$\langle 1 \rangle 3$. $Safety \wedge$ UNCHANGED $hr \Rightarrow Safety'$
OBVIOUS
$\langle 1 \rangle 4$. QED
BY *PTL*, $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$ DEF *Spec*

When safety is already in temporal form

$SafetyFull \triangleq \Box(hr \in 1 \,..\, 12)$

THEOREM $Spec \Rightarrow SafetyFull$
$\langle 1 \rangle 1.$ $HCInit \Rightarrow SafetyFull!1$ We want to refer to non-temporal part of *Safety*!
BY DEF $HCInit$
$\langle 1 \rangle 2.$ $SafetyFull!1 \land HCNext \Rightarrow SafetyFull!1'$
$\langle 2 \rangle 1.$ $hr \neq 12 \lor hr = 12$
OBVIOUS
$\langle 2 \rangle 2.$CASE $hr \neq 12$
BY DEF $HCNext$
$\langle 2 \rangle 3.$CASE $hr = 12$
BY DEF $HCNext$
$\langle 2 \rangle 4.$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$
$\langle 1 \rangle 3.$ $SafetyFull!1 \land$ UNCHANGED $hr \Rightarrow SafetyFull!1'$
OBVIOUS
$\langle 1 \rangle 4.$ $Spec \Rightarrow \Box SafetyFull!1$
BY PTL, $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$ DEF $Spec$
$\langle 1 \rangle 5.$ QED
BY $\langle 1 \rangle 4$ DEF $SafetyFull$

* Modification History
* Last modified *Wed Jul* 03 14:22:07 *JST* 2019 by *shinsa*
* Created *Wed Jul* 03 14:11:59 *JST* 2019 by *shinsa*