

```

1 |----- MODULE Clock -----|
2 | Hour Clock example from Lamport's book
4 EXTENDS Naturals, TLAPS
6 VARIABLES hr
8 HCInit  $\triangleq$   $hr \in 1 \dots 12$ 
9 HCNext  $\triangleq$   $hr' = \text{IF } hr \neq 12 \text{ THEN } hr + 1 \text{ ELSE } 1$ 
10
11 Specification.
12
14 Spec  $\triangleq$  HCInit  $\wedge$   $\Box[HCNext]_{hr}$ 
15
16 Spec for verify liveness
17 FSpec  $\triangleq$  HCInit  $\wedge$   $\Box[HCNext]_{hr}$ 
18
19
20 Liveness  $\triangleq$   $\Diamond(hr = 8)$ 
21 Safety  $\triangleq$   $(hr \in 1 \dots 12)$ 
22 BadSafety  $\triangleq$   $(hr \in 1 \dots 11)$ 
23
24 |-----|
25 | Thorem proving examples
26
27
29 | Lemma for progress of safety
30 LEMMA Progress  $\triangleq$  Safety  $\wedge$  HCNext  $\Rightarrow$  Safety'
31 <2> USE DEF Safety
32 <2>1.  $hr \neq 12 \vee hr = 12$ 
33     OBVIOUS
34 <2>2.CASE  $hr \neq 12$ 
35     BY DEF HCNext
36 <2>3.CASE  $hr = 12$ 
37     BY DEF HCNext
38 <2>4. QED
39     BY <2>1, <2>2, <2>3
40
41 THEOREM Spec  $\Rightarrow$   $\Box$  Safety
42 <1> USE DEF Safety
43 <1>1. HCInit  $\Rightarrow$  Safety We want to refer to non-temporal part of Safety!
44     BY DEF HCInit
45 <1>2. Safety  $\wedge$  HCNext  $\Rightarrow$  Safety'
46     BY Progress
47 <1>3. Safety  $\wedge$  UNCHANGED  $hr \Rightarrow$  Safety'
48     OBVIOUS
49 <1>4. QED
50     BY PTL, <1>1, <1>2, <1>3 DEF Spec
51
52 |-----|

```

53 When safety is already in temporal form

55 $SafetyFull \stackrel{\Delta}{=} \Box(hr \in 1 \dots 12)$

57 THEOREM $Spec \Rightarrow SafetyFull$

58 $\langle 1 \rangle 1. HCInit \Rightarrow SafetyFull!1$ We want to refer to non-temporal part of *Safety!*

59 BY DEF *HCInit*

60 $\langle 1 \rangle 2. SafetyFull!1 \wedge HCNext \Rightarrow SafetyFull!1'$

61 $\langle 2 \rangle 1. hr \neq 12 \vee hr = 12$

62 OBVIOUS

63 $\langle 2 \rangle 2. CASE \ hr \neq 12$

64 BY DEF *HCNext*

65 $\langle 2 \rangle 3. CASE \ hr = 12$

66 BY DEF *HCNext*

67 $\langle 2 \rangle 4. QED$

68 BY $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3$

69 $\langle 1 \rangle 3. SafetyFull!1 \wedge UNCHANGED \ hr \Rightarrow SafetyFull!1'$

70 OBVIOUS

71 $\langle 1 \rangle 4. Spec \Rightarrow \Box SafetyFull!1$

72 BY *PTL*, $\langle 1 \rangle 1, \langle 1 \rangle 2, \langle 1 \rangle 3$ DEF *Spec*

73 $\langle 1 \rangle 5. QED$

74 BY $\langle 1 \rangle 4$ DEF *SafetyFull*

76

\ * 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