

MODULE *ICen2*

The first part of this module defines the TLA+ representation of the abstract program *ICen2* of Figure 7.5 of the book “A Science of Computer Programs” by *Leslie Lamport*. The second part defines a program *ICen2.s* by adding a prophecy variable *s* to *ICen2* as in Section 7.3.2, and it asserts that *ICen2.s* implements *ICen1* under a suitable refinement mapping. For that purpose, it instantiates module *ICen1* that defines program *ICen1*. That second part is commented out (by ending the module before it) when this module is instantiated by *ICen1*, which is done when *ICen1* is the root module.

EXTENDS *Integers, Sequences*

CONSTANT *Art, NotArt*

VARIABLES *inp, aw, disp*
 $vars \triangleq \langle inp, aw, disp \rangle$

$TypeOK \triangleq \wedge inp \in Art \cup \{NotArt\}$
 $\wedge disp \in Art \times \{0, 1\}$
 $\wedge aw \in Seq(Art)$

$Init \triangleq \wedge inp = NotArt$
 $\wedge aw = \langle \rangle$
 $\wedge disp \in Art \times \{0, 1\}$

$InputOrNot \triangleq \wedge (inp = NotArt) \wedge (aw = \langle \rangle)$
 $\wedge inp' \in Art$
 $\wedge \vee aw' = \langle inp' \rangle$
 $\vee aw' = aw$
 $\wedge disp' = disp$

$Ack \triangleq \wedge (inp \in Art) \wedge (aw = \langle \rangle)$
 $\wedge inp' = NotArt$
 $\wedge UNCHANGED \langle aw, disp \rangle$

$Display \triangleq \wedge aw \neq \langle \rangle$
 $\wedge disp' = \langle aw[1], 1 - disp[2] \rangle$
 $\wedge aw' = \langle \rangle$
 $\wedge UNCHANGED inp$

$Next2 \triangleq InputOrNot \vee Ack \vee Display$

Although not done in the book, we now define a fairness requirement for the *ICen2* program. It is weak fairness of all the actions except the *InputOrNot* action, since we don't want to require that the artist keep submitting works of art.

$Fairness2 \triangleq WF_{vars}(Ack \vee Display)$

$ICen2 \triangleq Init \wedge \Box[Next2]_{vars} \wedge Fairness2$

When *ICen2* is the root module, comment out the following line that ends the module at this point.

Adding a stuttering variable s to show $ICen2 \Rightarrow \exists aw : ICen1$

VARIABLE s

$Init_s \triangleq Init \quad \wedge (s = 0)$

$Ack_s \triangleq (s = 0) \wedge Ack \wedge (s' = 0)$

$exp \triangleq \text{IF } aw' = \langle \rangle \text{ THEN } 1 \text{ ELSE } 0$

$InputOrNot_s \triangleq \begin{aligned} &\vee (s = 0) \wedge InputOrNot \wedge (s' = exp) \\ &\vee (s > 0) \wedge (s' = s - 1) \wedge \text{UNCHANGED } vars \end{aligned}$

$Display_s \triangleq (s = 0) \wedge Display \wedge (s' = 0)$

$Next2_s \triangleq InputOrNot_s \vee Ack_s \vee Display_s$

$ICen2_s \triangleq Init_s \wedge \Box[Next2_s]_{\langle vars, s \rangle} \wedge Fairness2$

$awBar \triangleq \text{IF } s = 0 \text{ THEN } aw \text{ ELSE } \langle inp \rangle$

$I \triangleq \text{INSTANCE } ICen1 \text{ WITH } aw \leftarrow awBar$

\ * Modification History

\ * Last modified *Wed Oct 16 16:02:05 CEST 2024* by *lamport*

\ * Created *Wed Nov 22 18:05:34 PST 2023* by *lamport*