MODULE *LIFO*

EXTENDS *Naturals*, *Sequences*
CONSTANT *Message*, *QueueSize*
VARIABLES *in*, *out*, *lifoq*

$LIFOInterface \triangleq$ INSTANCE *LIFO_Interface* WITH $q \leftarrow lifoq$

Receive message from channel *in* . change the queue to contain a concatination of the new value from the in channel and the original queue

$$\begin{aligned} BufRcv \triangleq\ & \land LIFOInterface!InChan!Rcv \\ & \land lifoq' = \langle in.val \rangle \circ lifoq \\ & \land \text{UNCHANGED } out \end{aligned}$$

$$\begin{aligned} BufSend \triangleq\ & \land lifoq \neq \langle\rangle \\ & \land LIFOInterface!OutChan!Send(Head(lifoq)) \\ & \land lifoq' = Tail(lifoq) \\ & \land \text{UNCHANGED } in \end{aligned}$$

Enabled only if q is nonempty. Send $Tail(q)$ on channel *out* and remove it from q.

$$\begin{aligned} Next \triangleq\ & \lor LIFOInterface!INext \\ & \lor BufRcv \\ & \lor BufSend \end{aligned}$$

BufRcv should eventually be called if $LIFOInterface!Send(msg)$ has been enabled

$$Liveness1 \triangleq \exists\, msg \in Message : \mathrm{WF}_{\langle in,\, out,\, lifoq \rangle}(LIFOInterface!Send(msg) \lor BufRcv)$$

While the *lifoq* is NOT empty *BufSend* is enabled

$$Liveness2 \triangleq \mathrm{SF}_{\langle in,\, out,\, lifoq \rangle}(lifoq \neq \langle\rangle \lor BufSend)$$

$LIFOInterface!Rcv$ should eventually be called if *BufSend* has been enabled

$$Liveness3 \triangleq \mathrm{WF}_{\langle in,\, out,\, lifoq \rangle}(BufSend \lor LIFOInterface!Rcv)$$

$$\begin{aligned} Spec \triangleq\ & \land LIFOInterface!Init \\ & \land \Box[Next]_{\langle in,\, out,\, lifoq \rangle} \\ & \land LIFOInterface!Liveness \\ & \land Liveness1 \\ & \land Liveness2 \\ & \land Liveness3 \end{aligned}$$

THEOREM $Spec \Rightarrow \Box LIFOInterface!TypeInvariant$