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

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

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

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

$$Next \triangleq \lor LIFOInterface!INext \lor BufRcv \lor BufSend$$

$$Liveness1 \triangleq \exists msg \in Message : \mathrm{WF}_{\langle in,\, out,\, lifoq\rangle}(LIFOInterface!Send(msg) \lor BufRcv)$$
$$Liveness2 \triangleq \mathrm{SF}_{\langle in,\, out,\, lifoq\rangle}(lifoq \neq \langle\rangle \lor BufSend)$$
$$Liveness3 \triangleq \mathrm{WF}_{\langle in,\, out,\, lifoq\rangle}(BufSend \lor LIFOInterface!Rcv)$$

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

THEOREM $Spec \Rightarrow \Box LIFOInterface!TypeInvariant$