MODULE *Channel*

Taken from “Specifying systems”

EXTENDS *Naturals*

CONSTANT *Data*

VARIABLE *chan*

$$TypeInvariant \triangleq chan \in [val : Data,\ ready : \{0, 1\},\ ack : \{0, 1\}]$$

In the begining, the *ack* and ready flags are the same.

$$Init \triangleq \begin{array}{l} \land TypeInvariant \\ \land chan.ack = chan.ready \end{array}$$

When the flags are the same, you can send the message.

$$Send(d) \triangleq \begin{array}{ll} \land chan.ready & = chan.ack \\ \land chan' & = [chan \text{ EXCEPT } !.val = d,\ !.ready = 1 - chan.ready] \end{array}$$

When the flags are not the same, you can confirm the message.

$$Receive \triangleq \begin{array}{ll} \land chan.ready & \neq chan.ack \\ \land chan' & = [chan \text{ EXCEPT } !.ready = 1 - chan.ready] \end{array}$$

$$Next \triangleq (\exists\, d \in Data : Send(d)) \land Receive$$

$$Spec \triangleq Init \land \Box[Next]_{chan}$$

THEOREM $Spec \Rightarrow \Box\, TypeInvariant$