MODULE $ABProtocol2$

EXTENDS $Integers$, $Sequences$

CONSTANT $Data$, The set of all possible data objects.
Bad The bad message (to model broken/lost messages).

Bad must be different from any of the legal messages.

ASSUME $Bad \notin (Data \times \{0, 1\}) \cup \{0, 1\}$

VARIABLES $AVar$, The last $\langle value, bit \rangle$ pair A decided to send.
$BVar$, The last $\langle value, bit \rangle$ pair B received.
$AtoB$, Sequence of DATA messages in transit from sender to receiver.
$BtoA$ Sequence of ACK messages in transit from receiver to sender.

$$\begin{aligned} TypeOK \triangleq\ & \land AVar \in Data \times \{0, 1\} \\ & \land BVar \in Data \times \{0, 1\} \\ & \land AtoB \in Seq(Data \times \{0, 1\} \cup \{Bad\}) \\ & \land BtoA \in Seq(\{0, 1, Bad\}) \end{aligned}$$

$vars \triangleq \langle AVar, BVar, AtoB, BtoA \rangle$ All variables.

$$\begin{aligned} Init \triangleq\ & \land AVar \in Data \times \{1\} \\ & \land BVar = AVar \\ & \land AtoB = \langle\rangle \\ & \land BtoA = \langle\rangle \end{aligned}$$

A sending a data message to B by putting the same message in the channel until an ACK is received.

$$\begin{aligned} ASnd \triangleq\ & \land AtoB' = Append(AtoB, AVar) \\ & \land \text{UNCHANGED } \langle AVar, BtoA, BVar \rangle \end{aligned}$$

B receiving a data message from A.

$$\begin{aligned} BRcv \triangleq\ & \land AtoB \neq \langle\rangle \quad \text{There is at least one message in the channel.} \\ & \land \text{IF } (Head(AtoB) \neq Bad) \land (Head(AtoB)[2] \neq BVar[2]) \\ & \quad \text{THEN } BVar' = Head(AtoB) \quad \text{Accept the message if } ACK \text{ bit is the alternate bit.} \\ & \quad \text{ELSE } BVar' = BVar \quad \text{Ignore the message and keep the same local state.} \\ & \land AtoB' = Tail(AtoB) \quad \text{Remove the received message from the channel.} \\ & \land \text{UNCHANGED } \langle AVar, BtoA \rangle \end{aligned}$$

B sending an ACK for the last data value received.

$$\begin{aligned} BSnd \triangleq\ & \land BtoA' = Append(BtoA, BVar[2]) \\ & \land \text{UNCHANGED } \langle AVar, BVar, AtoB \rangle \end{aligned}$$

A receiving an ACK from B.

$$\begin{aligned} ARcv \triangleq\ & \land BtoA \neq \langle\rangle \quad \text{There is at least one message in the channel.} \\ & \land \text{IF } Head(BtoA) = AVar[2] \quad \text{Check the } ACK \text{ bit.} \\ & \quad \text{THEN } \exists\, d \in Data : AVar' = \langle d, 1 - AVar[2] \rangle \quad \text{Alternate bit and send another message.} \\ & \quad \text{ELSE } AVar' = AVar \quad \text{Keep sending } AVar \text{ if } ACK \text{ bit doesn't match.} \end{aligned}$$

$\land\ BtoA' = Tail(BtoA)$ Remove received message from the channel.
$\land$ UNCHANGED $\langle AtoB,\ BVar\rangle$

Corrupt a message in one of the channels.
$CorruptMsg \triangleq \land \lor$ Corrupt a data message.
$\land \exists\, i \in 1\,..\,Len(AtoB) :$
$AtoB' = [AtoB$ EXCEPT $![i] = Bad]$
$\land\ BtoA' = BtoA$
$\lor$ Corrupt an ACK message.
$\land \exists\, i \in 1\,..\,Len(BtoA) :$
$BtoA = [BtoA$ EXCEPT $![i] = Bad]$
$\land\ AtoB' = AtoB$
$\land$ UNCHANGED $\langle AVar,\ BVar\rangle$

$Next \triangleq \lor\ ASnd$
$\lor\ BRcv$
$\lor\ BSnd$
$\lor\ ARcv$
$\lor\ CorruptMsg$

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

$ABS \triangleq$ INSTANCE $ABSpec$

THEOREM $Live \triangleq Spec \Rightarrow ABS!Spec$

$FairSpec \triangleq Spec \land \mathrm{SF}_{vars}(ARcv) \land \mathrm{SF}_{vars}(BRcv)$
$\land\ \mathrm{WF}_{vars}(ASnd) \land \mathrm{WF}_{vars}(ASnd)$

NOTE(*philix*): This doesn't hold (see the last lectures for the fixes)
THEOREM $Live2 \triangleq FairSpec \Rightarrow ABS!FairSpec$
