MODULE AB

EXTENDS $Integers$, $Sequences$

CONSTANT $Data$

$$Remove(i,\, seq) \triangleq [j \in 1 \,..\, (Len(seq) - 1) \mapsto \text{IF } j < i \text{ THEN } seq[j] \text{ ELSE } seq[j+1]]$$

VARIABLES $AVar$, $BVar$, $AtoB$, $BtoA$

$$vars \triangleq \langle AVar,\, BVar,\, AtoB,\, BtoA \rangle$$

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

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

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

$$\begin{aligned} ARcv \triangleq\ & \land BtoA \neq \langle\rangle \\ & \land \text{IF } Head(BtoA) = AVar[2] \\ & \quad \text{THEN } \exists\, d \in Data : \\ & \qquad AVar' = \langle d,\, 1 - AVar[2] \rangle \\ & \quad \text{ELSE UNCHANGED } AVar \\ & \land BtoA' = Tail(BtoA) \\ & \land \text{UNCHANGED } \langle BVar,\, AtoB \rangle \end{aligned}$$

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

$$\begin{aligned} BRcv \triangleq\ & \land AtoB \neq \langle\rangle \\ & \land \text{IF } Head(AtoB)[2] \neq BVar[2] \\ & \quad \text{THEN } BVar' = Head(AtoB) \\ & \quad \text{ELSE } BVar' = BVar \\ & \land AtoB' = Tail(AtoB) \\ & \land \text{UNCHANGED } \langle AVar,\, BtoA \rangle \end{aligned}$$

$$\begin{aligned} LoseMsg \triangleq\ & \land \lor \land \exists\, i \in 1 \,..\, Len(AtoB) : AtoB' = Remove(i,\, AtoB) \\ & \qquad \land BtoA' = BtoA \\ & \quad \lor \land \exists\, i \in 1 \,..\, Len(BtoA) : BtoA' = Remove(i,\, BtoA) \\ & \qquad \land AtoB' = AtoB \end{aligned}$$

$\land$ UNCHANGED $\langle AVar,\ BVar\rangle$

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

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

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

$ABS \triangleq$ INSTANCE $ABSpec$

THEOREM $Spec \Rightarrow ABS!Spec$
THEOREM $FairSpec \Rightarrow ABS!FairSpec$

---

* Modification History
* Last modified Sat *Nov* 16 22:37:11 *CET* 2019 by *martin*
* Created Sat *Nov* 16 21:47:38 *CET* 2019 by *martin*