MODULE $AB2$

EXTENDS *Integers*, *Sequences*

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

VARIABLES $AVar$, $BVar$, $AtoB2$, $BtoA2$
$vars \triangleq \langle AVar, BVar, AtoB2, BtoA2 \rangle$

$$
\begin{aligned}
TypeOK \triangleq\ & \land AVar \in Data \times \{0, 1\} \\
& \land BVar \in Data \times \{0, 1\} \\
& \land AtoB2 \in Seq((Data \times \{0, 1\}) \cup \{Bad\}) \\
& \land BtoA2 \in Seq(\{0, 1, Bad\})
\end{aligned}
$$

$$
\begin{aligned}
Init \triangleq\ & \land AVar \in Data \times \{1\} \\
& \land BVar = AVar \\
& \land AtoB2 = \langle\rangle \\
& \land BtoA2 = \langle\rangle
\end{aligned}
$$

$$
\begin{aligned}
ASnd \triangleq\ & \land AtoB2' = Append(AtoB2, AVar) \\
& \land \text{UNCHANGED } \langle AVar, BtoA2, BVar \rangle \\
BSnd \triangleq\ & \land BtoA2' = Append(BtoA2, BVar[2]) \\
& \land \text{UNCHANGED } \langle AVar, AtoB2, BVar \rangle
\end{aligned}
$$

$$
\begin{aligned}
ARcv \triangleq\ & \land BtoA2 \neq \langle\rangle \\
& \land \text{IF } Head(BtoA2) = AVar[2] \\
& \quad \text{THEN } \exists\, d \in Data : \\
& \qquad AVar' = \langle d, 1 - AVar[2] \rangle \\
& \quad \text{ELSE UNCHANGED } AVar \\
& \land BtoA2' = Tail(BtoA2) \\
& \land \text{UNCHANGED } \langle BVar, AtoB2 \rangle
\end{aligned}
$$

$$
\begin{aligned}
BRcv \triangleq\ & \land AtoB2 \neq \langle\rangle \\
& \land \text{IF } (Head(AtoB2) \neq Bad) \land (Head(AtoB2)[2] \neq BVar[2]) \\
& \quad \text{THEN } BVar' = Head(AtoB2) \\
& \quad \text{ELSE UNCHANGED } BVar \\
& \land AtoB2' = Tail(AtoB2) \\
& \land \text{UNCHANGED } \langle AVar, BtoA2 \rangle
\end{aligned}
$$

$$
\begin{aligned}
CorruptMsg \triangleq\ & \land \lor \land \exists\, i \in 1 \,..\, Len(AtoB2) : \\
& \qquad\qquad AtoB2' = [AtoB2 \text{ EXCEPT } ![i] = Bad] \\
& \qquad \land \text{UNCHANGED } BtoA2 \\
& \quad \lor \land \exists\, i \in 1 \,..\, Len(BtoA2) : \\
& \qquad\qquad BtoA2' = [BtoA2 \text{ EXCEPT } ![i] = Bad] \\
& \qquad \land \text{UNCHANGED } AtoB2 \\
& \land \text{UNCHANGED } \langle AVar, BVar \rangle
\end{aligned}
$$

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

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

---

$ABS \triangleq$ INSTANCE $ABSpec$
THEOREM $Spec \Rightarrow ABS!Spec$

---

RECURSIVE $RemoveBad(\_)$
$RemoveBad(seq) \triangleq$
IF $seq = \langle\rangle$
THEN $\langle\rangle$
ELSE IF $Head(seq) = Bad$
THEN $RemoveBad(Tail(seq))$
ELSE $\langle Head(seq)\rangle \circ RemoveBad(Tail(seq))$

$AB \triangleq$ INSTANCE $AB$ WITH $AtoB \leftarrow -RemoveBad(AtoB2)$, $BtoA \leftarrow -RemoveBad(BtoA2)$
THEOREM $Spec \Rightarrow AB!Spec$

---

* Modification History
* Last modified Sun *Nov* 17 22:22:04 *CET* 2019 by *martin*
* Created Sun *Nov* 17 19:29:22 *CET* 2019 by *martin*