MODULE *ABSpec*

EXTENDS *Integers*

CONSTANT *Data* The set of all possible data values.

VARIABLES *AVar*, The last $\langle value, bit \rangle$ pair A decided to send.
BVar The last $\langle value, bit \rangle$ pair B received.

Type correctness means that *AVar* and *BVar* are tuples $\langle d, i \rangle$ where $d \in Data$ and $i \in \{0, 1\}$.

$$TypeOK \triangleq \land AVar \in Data \times \{0, 1\} \\ \qquad\qquad \land BVar \in Data \times \{0, 1\}$$

It's useful to define *vars* to be the tuple of all variables, for example so we can write [*Next*]_*vars* instead of [*Next*]_$\langle \ldots \rangle$

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

Initially *AVar* can equal $\langle d, 1 \rangle$ for any *Data* value d, and *BVar* equals *AVar*.

$$Init \triangleq \land AVar \in Data \times \{1\} \\ \qquad \land BVar = AVar$$

When $AVar = BVar$, the sender can "send" an arbitrary data d item by setting $AVar[1]$ to d and complementing $AVar[2]$. It then waits until the receiver "receives" the message by setting *BVar* to *AVar* before it can send its next message. Sending is described by action A and receiving by action B.

$$A \triangleq \land AVar = BVar \\ \quad \land \exists d \in Data : AVar' = \langle d, 1 - AVar[2] \rangle \\ \quad \land BVar' = BVar$$

$$B \triangleq \land AVar \neq BVar \\ \quad \land BVar' = AVar \\ \quad \land AVar' = AVar$$

$$Next \triangleq A \lor B$$

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

For understanding the spec, it's useful to define formulas that should be invariants and check that they are invariant. The following invariant *Inv* asserts that, if *AVar* and *BVar* have equal second components, then they are equal (which by the invariance of *TypeOK* implies that they have equal first components).

$$Inv \triangleq (AVar[2] = BVar[2]) \Rightarrow (AVar = BVar)$$

FairSpec is *Spec* with the addition requirement that it keeps taking steps.

$$FairSpec \triangleq Spec \land \mathrm{WF}_{vars}(Next)$$

\* Modification History

\* Last modified Sat *Apr* 13 16:25:42 *CEST* 2019 by *Naxxo*
\* Created Sat *Apr* 13 16:25:28 *CEST* 2019 by *Naxxo*