MODULE *Consensus*

EXTENDS *Integers*

CONSTANTS PCS The set of all processes

VARIABLES
- $states$, states of each process in PCS
- $proposals$, proposals of each process in PCS
- $pset$, set of all proposals
- $decisions$ decision of each process in PCS

$$
\begin{aligned}
typeOK \triangleq\ & \land states \in [PCS \to \{\text{“working”}, \text{“proposed”}, \text{“decided”}\}] \\
& \land proposals \in [PCS \to \{0, 1\}] \\
& \land pset \subseteq \{0, 1\} \\
& \land decisions \in [PCS \to \{-1, 0, 1\}]
\end{aligned}
$$

$$
\begin{aligned}
init \triangleq\ & \land states = [p \in PCS \mapsto \text{“working”}] \\
& \land proposals \in [PCS \to \{0, 1\}] \\
& \land pset = \{\} \\
& \land decisions = [p \in PCS \mapsto -1]
\end{aligned}
$$

$$
\begin{aligned}
propose(p) \triangleq\ & \land states[p] = \text{“working”} \\
& \land states' = [states \text{ EXCEPT } ![p] = \text{“proposed”}] \\
& \land pset' = pset \cup \{proposals[p]\} \\
& \land \text{UNCHANGED } \langle proposals, decisions \rangle
\end{aligned}
$$

$$
\begin{aligned}
decide(p) \triangleq\ & \land \neg \exists\, q \in PCS : states[q] = \text{“working”} \\
& \land states[p] = \text{“proposed”} \\
& \land states' = [states \text{ EXCEPT } ![p] = \text{“decided”}] \\
& \land decisions[p] = -1 \\
& \land decisions' = [decisions \text{ EXCEPT } ![p] = \text{CHOOSE } x \in pset : \text{TRUE}] \\
& \land \text{UNCHANGED } \langle proposals, pset \rangle
\end{aligned}
$$

$$
next \triangleq \exists\, p \in PCS : propose(p) \lor decide(p)
$$

$$
\begin{aligned}
validity \triangleq\ & \exists\, v \in \{0, 1\} : (\forall\, p \in PCS : proposals[p] = v) \\
& \Rightarrow \forall\, q \in PCS : (states[q] = \text{“decided”} \\
& \quad \Rightarrow decisions[q] = v)
\end{aligned}
$$

$$
\begin{aligned}
agreement \triangleq\ & \forall\, p1, p2 \in PCS : \neg \land decisions[p1] = 0 \\
& \qquad\qquad\qquad\qquad \land decisions[p2] = 1
\end{aligned}
$$

$$
\begin{aligned}
integrity \triangleq\ & \forall\, p \in PCS : \\
& (states[p] = \text{“decided”} \\
& \Rightarrow \exists\, r \in PCS : proposals[r] = decisions[p])
\end{aligned}
$$

$$
\begin{aligned}
specOK \triangleq\ & \land validity \\
& \land agreement
\end{aligned}
$$

$\wedge$ *integrity*

* Modification History
* Last modified Sun *Jan* 21 04:06:32 *JST* 2018 by *Zhang*
* Created *Thu Jan* 18 15:52:38 *SRET* 2018 by *Zhang*