## MODULE *TCommit*

CONSTANT $RM$

The set of participating resource managers

VARIABLE $rmState$

$rmState[rm]$ is the state of resource manager $r$.

---

$TCTypeOK \triangleq$

The type-correctness invariant

$$rmState \in [RM \rightarrow \{\text{“working”}, \text{“prepared”}, \text{“committed”}, \text{“aborted”}\}]$$

$$TCInit \triangleq \quad rmState = [r \in RM \mapsto \text{“working”}]$$

The initial predicate.

$$canCommit \triangleq \forall r \in RM : rmState[r] \in \{\text{“prepared”}, \text{“committed”}\}$$

True iff all $RMs$ are in the “prepared” or “committed” state.

$$notCommitted \triangleq \forall r \in RM : rmState[r] \neq \text{“committed”}$$

True iff no resource manager has decided to commit.

---

We now define the actions that may be performed by the $RMs$, and then define the complete next-state action of the specification to be the disjunction of the possible $RM$ actions.

$$
\begin{array}{lll}
Prepare(r) & \triangleq & \land\ rmState[r] = \text{“working”} \\
 & & \land\ rmState' = [rmState\ \text{EXCEPT}\ ![r] = \text{“prepared”}]
\end{array}
$$

$$
\begin{array}{llll}
Decide(r) & \triangleq & \lor & \land\ rmState[r] = \text{“prepared”} \\
 & & & \land\ canCommit \\
 & & & \land\ rmState' = [rmState\ \text{EXCEPT}\ ![r] = \text{“committed”}] \\
 & & \lor & \land\ rmState[r] \in \{\text{“working”}, \text{“prepared”}\} \\
 & & & \land\ notCommitted \\
 & & & \land\ rmState' = [rmState\ \text{EXCEPT}\ ![r] = \text{“aborted”}]
\end{array}
$$

$$TCNext \triangleq \exists r \in RM : Prepare(r) \lor Decide(r)$$

The next-state action.

---

$$TCSpec \triangleq TCInit \land \Box[TCNext]_{rmState}$$

The complete specification of the protocol.

---

We now assert invariance properties of the specification.

$TCConsistent \triangleq$

A state predicate asserting that two $RMs$ have not arrived at conflicting decisions.

$$
\begin{array}{ll}
\forall r1, r2 \in RM : \neg & \land\ rmState[r1] = \text{“aborted”} \\
 & \land\ rmState[r2] = \text{“committed”}
\end{array}
$$

THEOREM $TCSpec \Rightarrow \Box(TCTypeOK \land TCConsistent)$

Asserts that $TCTypeOK$ and $TCInvariant$ are invariants of the protocol.