MODULE *TCommitJonRo*

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.

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

Can commit iff all RMs are in the “prepared” or “committed” state.

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

Can abort iff no RM 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.

$$Prepare(r) \triangleq \land\ rmState[r] = \text{“working”}$$

Any RM in the working state can go to the prepared state

$$\land\ rmState' = [rmState \text{ EXCEPT } ![r] = \text{“prepared”}]$$

$$Commit(r) \triangleq \land\ rmState[r] = \text{“prepared”}$$

$\land\ canCommit$ Only allowed to commit from prepared if we can commit

$$\land\ rmState' = [rmState \text{ EXCEPT } ![r] = \text{“committed”}]$$

$$Abort(r) \triangleq \land\ rmState[r] \in \{\text{“working”}, \text{“prepared”}\}$$

$\land\ canAbort$ Only allowed to abort from working or prepared if we can abort

$$\land\ rmState' = [rmState \text{ EXCEPT } ![r] = \text{“aborted”}]$$

$$TCNext \triangleq \exists\, r \in RM : Prepare(r) \lor Commit(r) \lor Abort(r)$$

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.

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

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

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