MODULE *tcommit*

This specification is explained in "Transaction Commit", Lecture 5 of the TLA+ Video Course.

CONSTANT RM The set of participating resource managers

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

$TCTypeOK \triangleq$

The type-correctness invariant

$rmState \in [RM \to \{\text{"working"}, \text{"prepared"}, \text{"committed"}, \text{"aborted"}\}]$

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

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.

$$\begin{aligned} Prepare(r) \triangleq\ & \land\ rmState[r] = \text{"working"} \\ & \land\ rmState' = [rmState \text{ EXCEPT } ![r] = \text{"prepared"}] \end{aligned}$$

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

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

The next-state action.

$TCConsistent \triangleq$

A state predicate asserting that two RMs have not arrived at conflicting decisions. It is an invariant of the specification.

$$\begin{aligned} \forall\, r1, r2 \in RM : \neg\ & \land\ rmState[r1] = \text{"aborted"} \\ & \land\ rmState[r2] = \text{"committed"} \end{aligned}$$

The following part of the spec is not discussed in Video Lecture 5. It will be explained in Video Lecture 8.

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

The complete specification of the protocol written as a temporal formula.

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

This theorem asserts the truth of the temporal formula whose meaning is that the state predicate $TCTypeOK \land TCInvariant$ is an invariant of the specification $TCSpec$. Invariance of this conjunction is equivalent to invariance of both of the formulas $TCTypeOK$ and $TCConsistent$.