MODULE *DistributedCommit*

This is a high-level TLA+ specification of a distributed commit protocol. A set of nodes individually decide whether they wish to commit or abort a transaction. Second, the transaction will be committed iff every node wishes to commit.

CONSTANT $Node$ set of participating nodes

VARIABLE $nState$ state of each participant

Possible states of nodes.

$$NState \triangleq \{\text{“preparing”}, \text{“readyCommit”}, \text{“readyAbort”}, \text{“committed”}, \text{“aborted”}\}$$

Initially, every node is preparing the transaction.

$$Init \triangleq nState = [n \in Node \mapsto \text{“preparing”}]$$

A node decides whether it wishes to commit or abort.

$$\begin{array}{l} Decide(n) \triangleq \\ \quad \land\ nState[n] = \text{“preparing”} \\ \quad \land\ \lor\ nState' = [nState \text{ EXCEPT } ![n] = \text{“readyCommit”}] \\ \qquad \lor\ nState' = [nState \text{ EXCEPT } ![n] = \text{“readyAbort”}] \end{array}$$

A node may commit only if all nodes wish to do so.

$$\begin{array}{l} Commit(n) \triangleq \\ \quad \land \forall\, q \in Node : nState[q] \in \{\text{“readyCommit”}, \text{“committed”}\} \\ \quad \land\ nState' = [nState \text{ EXCEPT } ![n] = \text{“committed”}] \end{array}$$

A node aborts if some node requests an abort.

$$\begin{array}{l} Abort(n) \triangleq \\ \quad \land\ \ \exists\, q \in Node : nState[q] \in \{\text{“readyAbort”}, \text{“aborted”}\} \\ \quad \land\ \ nState' = [nState \text{ EXCEPT } ![n] = \text{“aborted”}] \end{array}$$

The next-state relation is the disjunction of the above actions.

$$Next \triangleq \exists\, n \in Node : Decide(n) \lor Commit(n) \lor Abort(n)$$

Overall specification.

$$Spec \triangleq Init \land \Box[Next]_{nState} \land \mathrm{WF}_{nState}(Next)$$

Check type correctness.

$$TypeOK \triangleq nState \in [Node \to NState]$$

Main safety property: nodes may commit only if all nodes agree.

$$\begin{array}{l} Safety \triangleq \\ \quad \forall\, n \in Node : nState[n] = \text{“committed”} \Rightarrow \\ \qquad \forall\, q \in Node : nState[n] \in \{\text{“readyCommit”}, \text{“committed”}\} \end{array}$$

Non-property: no node may ever commit.

$NeverCommit \triangleq \forall\, n \in Node : nState[n] \neq \text{“committed”}$

Liveness property: nodes will eventually commit or abort. (Requires fairness condition on next-state relation.)

$Liveness \triangleq \forall\, n \in Node : \Diamond(nState[n] \in \{\text{“committed”}, \text{“aborted”}\})$