

---

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

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

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

The initial predicate.

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

True iff all *RM*s 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 *RM*s, and then define the complete next-state action of the specification to be the disjunction of the possible *RM* actions.

*Prepare*(*r*)  $\triangleq$   $\wedge rmState[r] = \text{“working”}$   
 $\wedge rmState' = [rmState \text{ EXCEPT } ![r] = \text{“prepared”}]$

*Decide*(*r*)  $\triangleq$   $\vee \wedge rmState[r] = \text{“prepared”}$   
 $\wedge canCommit$   
 $\wedge rmState' = [rmState \text{ EXCEPT } ![r] = \text{“committed”}]$   
 $\vee \wedge rmState[r] \in \{\text{“working”}, \text{“prepared”}\}$   
 $\wedge notCommitted$   
 $\wedge rmState' = [rmState \text{ EXCEPT } ![r] = \text{“aborted”}]$

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

The next-state action.

---

*TConsistent*  $\triangleq$

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

$\forall r1, r2 \in RM : \neg \wedge rmState[r1] = \text{“aborted”}$   
 $\wedge rmState[r2] = \text{“committed”}$

---

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

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

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

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

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

---

\ \* Modification History  
\ \* Last modified *Mon Jan 01 22:09:06 CET 2024* by *Alexander*  
\ \* Created *Mon Jan 01 22:08:38 CET 2024* by *Alexander*