

---

MODULE *Transaction*

---

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

INSTANCE *TLC*

---

An empty constant

CONSTANT *Nil*

Transaction phase constants

CONSTANTS

*Change,*

*Rollback*

Transaction phase constants

CONSTANTS

*Commit,*

*Apply*

Status constants

CONSTANTS

*Pending,*

*InProgress,*

*Complete,*

*Aborted,*

*Canceled,*

*Failed*

$Status \triangleq \{Pending, InProgress, Complete, Aborted, Canceled, Failed\}$

$Done \triangleq \{Complete, Aborted, Canceled, Failed\}$

The set of all nodes

CONSTANT *Node*

The set of possible paths and values

CONSTANT *Path, Value*

$Empty \triangleq [p \in \{\} \mapsto Nil]$

---

Variables defined by other modules.

VARIABLES

*configuration*,  
*mastership*,  
*conn*,  
*target*

A transaction log. Transactions may either request a set of changes to a set of targets or rollback a prior change.

VARIABLE *transactions*

A history of transaction change/rollback commit/apply events used for model checking.

VARIABLE *history*

*TypeOK*  $\triangleq$

$\forall i \in \text{DOMAIN } transactions :$   
 $\wedge transactions[i].index \in Nat$   
 $\wedge transactions[i].phase \in \{Change, Rollback\}$   
 $\wedge transactions[i].change.commit \in Status$   
 $\wedge transactions[i].change.apply \in Status$   
 $\wedge \forall p \in \text{DOMAIN } transactions[i].change.values :$   
 $\quad transactions[i].change.values[p] \neq Nil \Rightarrow$   
 $\quad \quad transactions[i].change.values[p] \in STRING$   
 $\wedge transactions[i].rollback.commit \neq Nil \Rightarrow$   
 $\quad transactions[i].rollback.commit \in Status$   
 $\wedge transactions[i].rollback.apply \neq Nil \Rightarrow$   
 $\quad transactions[i].rollback.apply \in Status$   
 $\wedge \forall p \in \text{DOMAIN } transactions[i].rollback.values :$   
 $\quad transactions[i].rollback.values[p] \neq Nil \Rightarrow$   
 $\quad \quad transactions[i].rollback.values[p] \in STRING$

LOCAL *State*  $\triangleq$  [  
   *transactions*  $\mapsto transactions$ ,  
   *configuration*  $\mapsto configuration$ ,  
   *mastership*  $\mapsto mastership$ ,  
   *conn*  $\mapsto conn$ ,  
   *target*  $\mapsto target$ ]

LOCAL *Transitions*  $\triangleq$

LET  
   *indexes*  $\triangleq \{i \in \text{DOMAIN } transactions' : i \in \text{DOMAIN } transactions \Rightarrow transactions'[i] \neq transactions[i]\}$   
 IN [*transactions*  $\mapsto [i \in indexes \mapsto transactions'[i]]$ ] @@  
   (IF *configuration'*  $\neq configuration$  THEN [*configuration*  $\mapsto configuration'$ ] ELSE *Empty*) @@  
   (IF *target'*  $\neq target$  THEN [*target*  $\mapsto target'$ ] ELSE *Empty*)

*Test*  $\triangleq$  INSTANCE *Test* WITH  
   *File*  $\leftarrow$  "Transaction.log"



$$\begin{aligned}
& \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{committed.target} = i] \\
& \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \text{type} \mapsto \text{Change}, \\
& \quad \text{phase} \mapsto \text{Commit}, \\
& \quad \text{index} \mapsto i, \\
& \quad \text{status} \mapsto \text{InProgress}]) \\
& \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
\vee & \wedge \text{configuration.committed.target} = i \\
& \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{change.commit} = \text{InProgress}, \\
& \quad ![i].\text{rollback.index} = \text{configuration.committed.revision}, \\
& \quad ![i].\text{rollback.values} = [ \\
& \quad \quad p \in \text{DOMAIN } \text{transactions}[i].\text{change.values} \mapsto \\
& \quad \quad \text{IF } p \in \text{DOMAIN } \text{configuration.committed.values} \text{ THEN } \\
& \quad \quad \quad \text{configuration.committed.values}[p] \\
& \quad \quad \text{ELSE } \text{Nil}]] \\
& \wedge \text{UNCHANGED } \langle \text{configuration}, \text{history} \rangle \\
\vee & \wedge \text{transactions}[i].\text{change.commit} = \text{InProgress} \\
& \wedge \vee \wedge \text{configuration.committed.index} \neq i \\
& \quad \wedge \vee \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{committed.transaction} = i, \\
& \quad \quad !.\text{committed.index} = i, \\
& \quad \quad !.\text{committed.change} = i, \\
& \quad \quad !.\text{committed.revision} = i, \\
& \quad \quad !.\text{committed.ordinal} = \text{configuration.committed.ordinal}, \\
& \quad \quad !.\text{committed.values} = \text{transactions}[i].\text{change.values}, \\
& \quad \quad \text{configuration.committed.values} = \text{configuration.committed.values} \text{ EXCEPT } i] \\
& \quad \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \quad \text{type} \mapsto \text{Change}, \\
& \quad \quad \text{phase} \mapsto \text{Commit}, \\
& \quad \quad \text{index} \mapsto i, \\
& \quad \quad \text{status} \mapsto \text{Complete}]) \\
& \quad \vee \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{committed.transaction} = i, \\
& \quad \quad !.\text{committed.index} = i, \\
& \quad \quad !.\text{committed.change} = i] \\
& \quad \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \quad \text{type} \mapsto \text{Change}, \\
& \quad \quad \text{phase} \mapsto \text{Commit}, \\
& \quad \quad \text{index} \mapsto i, \\
& \quad \quad \text{status} \mapsto \text{Failed}]) \\
& \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
\vee & \wedge \text{configuration.committed.index} = i \\
& \wedge \vee \wedge \text{configuration.committed.revision} = i \\
& \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{change.commit} = \text{Complete}, \\
& \quad \quad ![i].\text{change.ordinal} = \text{configuration.committed.ordinal}, \\
& \quad \quad \text{configuration.committed.revision} = \text{configuration.committed.revision} \text{ EXCEPT } i] \\
& \quad \vee \wedge \text{configuration.committed.revision} \neq i \\
& \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{change.commit} = \text{Failed},
\end{aligned}$$

$$\begin{aligned}
& \wedge \text{UNCHANGED } \langle \text{configuration}, \text{history} \rangle \\
& \wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn}, \text{target} \rangle \\
& \text{CommitRollback}(n, i) \triangleq \\
& \quad \wedge \vee \wedge \text{transactions}[i].\text{rollback.commit} = \text{Pending} \\
& \quad \wedge \text{configuration.committed.revision} = i \\
& \quad \wedge \vee \wedge \text{configuration.committed.target} = i \\
& \quad \quad \wedge \text{configuration.committed.index} = \text{configuration.committed.target} \\
& \quad \wedge \vee \wedge \text{configuration.committed.transaction} = i \\
& \quad \quad \wedge \text{transactions}[\text{configuration.committed.transaction}].\text{change.commit} = \text{Complete} \\
& \quad \quad \vee \wedge \text{configuration.committed.transaction} > i \\
& \quad \quad \quad \wedge \text{transactions}[\text{configuration.committed.transaction}].\text{rollback.commit} = \text{Complete} \\
& \quad \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{committed.target} = \text{transactions}[i].\text{rollback.index}] \\
& \quad \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \quad \quad \text{type} \mapsto \text{Rollback}, \\
& \quad \quad \quad \text{phase} \mapsto \text{Commit}, \\
& \quad \quad \quad \text{index} \mapsto i, \\
& \quad \quad \quad \text{status} \mapsto \text{InProgress}]) \\
& \quad \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
& \quad \vee \wedge \text{configuration.committed.revision} = i \\
& \quad \quad \wedge \text{configuration.committed.target} = \text{transactions}[i].\text{rollback.index} \\
& \quad \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{rollback.commit} = \text{InProgress}] \\
& \quad \quad \wedge \text{UNCHANGED } \langle \text{configuration}, \text{history} \rangle \\
& \quad \vee \wedge \text{transactions}[i].\text{rollback.commit} = \text{InProgress} \\
& \quad \quad \wedge \vee \wedge \text{configuration.committed.revision} = i \\
& \quad \quad \quad \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{committed.transaction} = i, \\
& \quad \quad \quad \quad \quad \quad \quad !.\text{committed.index} = i, \\
& \quad \quad \quad \quad \quad \quad \quad !.\text{committed.ordinal} = \text{configuration.committed.ordinal}, \\
& \quad \quad \quad \quad \quad \quad \quad !.\text{committed.revision} = \text{transactions}[i].\text{rollback.index}, \\
& \quad \quad \quad \quad \quad \quad \quad !.\text{committed.values} = \text{transactions}[i].\text{rollback.values}, \\
& \quad \quad \quad \quad \quad \quad \quad \text{configuration.committed.target} = \text{configuration.committed.target}] \\
& \quad \quad \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \quad \quad \text{type} \mapsto \text{Rollback}, \\
& \quad \quad \quad \text{phase} \mapsto \text{Commit}, \\
& \quad \quad \quad \text{index} \mapsto i, \\
& \quad \quad \quad \text{status} \mapsto \text{Complete}]) \\
& \quad \quad \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
& \quad \vee \wedge \text{configuration.committed.revision} = \text{transactions}[i].\text{rollback.index} \\
& \quad \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{rollback.commit} = \text{Complete}, \\
& \quad \quad \quad \quad \quad \quad \quad ![i].\text{rollback.ordinal} = \text{configuration.committed.ordinal}] \\
& \quad \quad \wedge \text{UNCHANGED } \langle \text{configuration}, \text{history} \rangle \\
& \quad \wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn}, \text{target} \rangle \\
& \text{ApplyChange}(n, i) \triangleq
\end{aligned}$$



$$\begin{aligned}
& \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{applied.transaction} = i, \\
& \qquad \qquad \qquad !.\text{applied.ordinal} = \text{transactions}[i].\text{change.ordinal}, \\
& \qquad \qquad \qquad !.\text{applied.revision} = i, \\
& \qquad \qquad \qquad !.\text{applied.values} = \text{transactions}[i].\text{change.values}, \\
& \qquad \qquad \qquad \text{configuration.applied.transaction} = i] \\
& \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \qquad \text{type} \mapsto \text{Change}, \\
& \qquad \text{phase} \mapsto \text{Apply}, \\
& \qquad \text{index} \mapsto i, \\
& \qquad \text{status} \mapsto \text{Complete}]) \\
& \vee \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{applied.transaction} = i, \\
& \qquad \qquad \qquad !.\text{applied.ordinal} = \text{transactions}[i].\text{change.ordinal}, \\
& \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \qquad \text{type} \mapsto \text{Change}, \\
& \qquad \text{phase} \mapsto \text{Apply}, \\
& \qquad \text{index} \mapsto i, \\
& \qquad \text{status} \mapsto \text{Failed}]) \\
& \wedge \text{UNCHANGED } \langle \text{target} \rangle \\
& \vee \wedge \text{transactions}[i].\text{phase} = \text{Rollback} \\
& \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{applied.transaction} = i, \\
& \qquad \qquad \qquad !.\text{applied.ordinal} = \text{transactions}[i].\text{change.ordinal}, \\
& \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \qquad \text{type} \mapsto \text{Change}, \\
& \qquad \text{phase} \mapsto \text{Apply}, \\
& \qquad \text{index} \mapsto i, \\
& \qquad \text{status} \mapsto \text{Failed}]) \\
& \wedge \text{UNCHANGED } \langle \text{target} \rangle \\
& \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
& \text{If the change has been applied, update the transaction status.} \\
& \vee \wedge \text{configuration.applied.ordinal} = \text{transactions}[i].\text{change.ordinal} \\
& \wedge \vee \wedge \text{configuration.applied.revision} = i \\
& \qquad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{change.apply} = \text{Complete}] \\
& \qquad \vee \wedge \text{configuration.applied.revision} = \text{transactions}[i].\text{rollback.index} \\
& \qquad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{change.apply} = \text{Failed}] \\
& \wedge \text{UNCHANGED } \langle \text{configuration}, \text{target}, \text{history} \rangle \\
& \wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn} \rangle \\
& \text{ApplyRollback}(n, i) \triangleq \\
& \wedge \text{transactions}[i].\text{rollback.commit} = \text{Complete} \\
& \wedge \vee \wedge \text{transactions}[i].\text{rollback.apply} = \text{Pending} \\
& \wedge \vee \wedge \text{configuration.applied.ordinal} = \text{transactions}[i].\text{rollback.ordinal} - 1 \\
& \wedge \vee \wedge \text{configuration.applied.target} \neq \text{transactions}[i].\text{rollback.index} \\
& \wedge \vee \wedge \text{configuration.applied.transaction} = i \\
& \qquad \wedge \text{transactions}[\text{configuration.applied.transaction}].\text{change.apply} \in \text{Done} \\
& \vee \wedge \text{configuration.applied.transaction} > i
\end{aligned}$$

$$\begin{aligned}
& \wedge \text{transactions}[\text{configuration.applied.transaction}].\text{rollback.apply} \in \text{Done} \\
& \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{applied.target} = \text{transactions}[i].\text{rollback.index}] \\
& \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \text{type} \mapsto \text{Rollback}, \\
& \quad \text{phase} \mapsto \text{Apply}, \\
& \quad \text{index} \mapsto i, \\
& \quad \text{status} \mapsto \text{InProgress}]) \\
& \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
& \vee \wedge \text{configuration.applied.target} = \text{transactions}[i].\text{rollback.index} \\
& \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{rollback.apply} = \text{InProgress}] \\
& \quad \wedge \text{UNCHANGED } \langle \text{configuration}, \text{history} \rangle \\
& \wedge \text{UNCHANGED } \langle \text{target} \rangle \\
& \vee \wedge \text{transactions}[i].\text{rollback.apply} = \text{InProgress} \\
& \quad \text{If this transaction has not yet been applied, attempt to apply it.} \\
& \quad \wedge \vee \wedge \text{configuration.applied.ordinal} \neq \text{transactions}[i].\text{rollback.ordinal} \\
& \quad \quad \wedge \text{configuration.state} = \text{Complete} \\
& \quad \quad \wedge \text{configuration.term} = \text{mastership.term} \\
& \quad \quad \wedge \text{conn}[n].\text{id} = \text{mastership.conn} \\
& \quad \quad \wedge \text{conn}[n].\text{connected} \\
& \quad \quad \wedge \text{target.running} \\
& \quad \quad \wedge \text{target}' = [\text{target} \text{ EXCEPT } !.\text{values} = \text{transactions}[i].\text{rollback.values} @@ \text{target.values}] \\
& \quad \quad \wedge \text{configuration}' = [\text{configuration} \text{ EXCEPT } !.\text{applied.transaction} = i, \\
& \quad \quad \quad !.\text{applied.ordinal} = \text{transactions}[i].\text{rollback.ordinal}, \\
& \quad \quad \quad !.\text{applied.revision} = \text{transactions}[i].\text{rollback.index}, \\
& \quad \quad \quad !.\text{applied.values} = \text{transactions}[i].\text{rollback.values} \\
& \quad \quad \quad \text{configuration.applied.values}] \\
& \quad \wedge \text{history}' = \text{Append}(\text{history}, [ \\
& \quad \quad \text{type} \mapsto \text{Rollback}, \\
& \quad \quad \text{phase} \mapsto \text{Apply}, \\
& \quad \quad \text{index} \mapsto i, \\
& \quad \quad \text{status} \mapsto \text{Complete}]) \\
& \quad \wedge \text{UNCHANGED } \langle \text{transactions} \rangle \\
& \quad \text{If the change has been applied, update the transaction status.} \\
& \quad \vee \wedge \text{configuration.applied.ordinal} = \text{transactions}[i].\text{rollback.ordinal} \\
& \quad \quad \wedge \text{configuration.applied.revision} = \text{transactions}[i].\text{rollback.index} \\
& \quad \quad \wedge \text{transactions}' = [\text{transactions} \text{ EXCEPT } ![i].\text{rollback.apply} = \text{Complete}] \\
& \quad \quad \wedge \text{UNCHANGED } \langle \text{configuration}, \text{target}, \text{history} \rangle \\
& \wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn} \rangle \\
& \text{ReconcileTransaction}(n, i) \triangleq \\
& \quad \wedge i \in \text{DOMAIN } \text{transactions} \\
& \quad \wedge \text{mastership.master} = n \\
& \quad \wedge \vee \text{CommitChange}(n, i) \\
& \quad \quad \vee \text{ApplyChange}(n, i) \\
& \quad \quad \vee \text{CommitRollback}(n, i)
\end{aligned}$$



$\vee \textit{ApplyRollback}(n, i)$

\_\_\_\_\_