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*

$$
\begin{array}{l}
\mathit{TypeOK} \triangleq \\
\quad \forall\, i \in \text{DOMAIN } \mathit{transactions} : \\
\qquad \land\ \mathit{transactions}[i].\mathit{index} \in \mathit{Nat} \\
\qquad \land\ \mathit{transactions}[i].\mathit{phase} \in \{\mathit{Change},\ \mathit{Rollback}\} \\
\qquad \land\ \mathit{transactions}[i].\mathit{change}.\mathit{commit} \in \mathit{Status} \\
\qquad \land\ \mathit{transactions}[i].\mathit{change}.\mathit{apply} \in \mathit{Status} \\
\qquad \land\ \forall\, p \in \text{DOMAIN } \mathit{transactions}[i].\mathit{change}.\mathit{values} : \\
\qquad\quad \mathit{transactions}[i].\mathit{change}.\mathit{values}[p] \neq \mathit{Nil} \Rightarrow \\
\qquad\qquad \mathit{transactions}[i].\mathit{change}.\mathit{values}[p] \in \text{STRING} \\
\qquad \land\ \mathit{transactions}[i].\mathit{rollback}.\mathit{commit} \neq \mathit{Nil} \Rightarrow \\
\qquad\quad \mathit{transactions}[i].\mathit{rollback}.\mathit{commit} \in \mathit{Status} \\
\qquad \land\ \mathit{transactions}[i].\mathit{rollback}.\mathit{apply} \neq \mathit{Nil} \Rightarrow \\
\qquad\quad \mathit{transactions}[i].\mathit{rollback}.\mathit{apply} \in \mathit{Status} \\
\qquad \land\ \forall\, p \in \text{DOMAIN } \mathit{transactions}[i].\mathit{rollback}.\mathit{values} : \\
\qquad\quad \mathit{transactions}[i].\mathit{rollback}.\mathit{values}[p] \neq \mathit{Nil} \Rightarrow \\
\qquad\qquad \mathit{transactions}[i].\mathit{rollback}.\mathit{values}[p] \in \text{STRING}
\end{array}
$$

$$
\begin{array}{l}
\text{LOCAL } \mathit{State} \triangleq [\\
\quad \mathit{transactions} \mapsto \mathit{transactions}, \\
\quad \mathit{configuration} \mapsto \mathit{configuration}, \\
\quad \mathit{mastership} \mapsto \mathit{mastership}, \\
\quad \mathit{conn} \mapsto \mathit{conn}, \\
\quad \mathit{target} \mapsto \mathit{target}]
\end{array}
$$

$$
\begin{array}{l}
\text{LOCAL } \mathit{Transitions} \triangleq \\
\quad \text{LET} \\
\qquad \mathit{indexes} \triangleq \{i \in \text{DOMAIN } \mathit{transactions}' : \\
\qquad\qquad\qquad i \in \text{DOMAIN } \mathit{transactions} \Rightarrow \mathit{transactions}'[i] \neq \mathit{transactions}[i]\} \\
\quad \text{IN} \quad [\mathit{transactions} \mapsto [i \in \mathit{indexes} \mapsto \mathit{transactions}'[i]]]\ @@ \\
\qquad (\text{IF } \mathit{configuration}' \neq \mathit{configuration} \text{ THEN } [\mathit{configuration} \mapsto \mathit{configuration}'] \text{ ELSE } \mathit{Empty})\ @@ \\
\qquad (\text{IF } \mathit{target}' \neq \mathit{target} \text{ THEN } [\mathit{target} \mapsto \mathit{target}'] \text{ ELSE } \mathit{Empty})
\end{array}
$$

$$
\begin{array}{l}
\mathit{Test} \triangleq \text{INSTANCE } \mathit{Test} \text{ WITH} \\
\quad \mathit{File} \leftarrow \text{“Transaction.log”}
\end{array}
$$

Add a change for revision 'i' to the transaction log

$$
\begin{array}{l}
AppendChange(i) \triangleq \\
\quad \land Len(transactions) = i - 1 \\
\quad \land \exists\, p \in Path,\, v \in Value : \\
\qquad \text{LET } transaction \triangleq [\\
\qquad\qquad index \mapsto Len(transactions) + 1, \\
\qquad\qquad phase \mapsto Change, \\
\qquad\qquad change \mapsto [\\
\qquad\qquad\quad index \mapsto Len(transactions) + 1, \\
\qquad\qquad\quad ordinal \mapsto 0, \\
\qquad\qquad\quad values \mapsto (p :> v), \\
\qquad\qquad\quad commit \mapsto Pending, \\
\qquad\qquad\quad apply \mapsto Pending], \\
\qquad\qquad rollback \mapsto [\\
\qquad\qquad\quad index \mapsto 0, \\
\qquad\qquad\quad ordinal \mapsto 0, \\
\qquad\qquad\quad values \mapsto Empty, \\
\qquad\qquad\quad commit \mapsto Nil, \\
\qquad\qquad\quad apply \mapsto Nil]] \\
\qquad \text{IN} \quad \land transactions' = Append(transactions, transaction) \\
\quad \land \text{UNCHANGED } \langle configuration, mastership, conn, target, history \rangle
\end{array}
$$

Add a rollback of revision 'i' to the transaction log

$$
\begin{array}{l}
RollbackChange(i) \triangleq \\
\quad \land i \in \text{DOMAIN } transactions \\
\quad \land transactions[i].phase = Change \\
\quad \land transactions[i].change.commit = Complete \\
\quad \land transactions' = [transactions \text{ EXCEPT } ![i].phase = Rollback, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad ![i].rollback.commit = Pending, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad ![i].rollback.apply = Pending] \\
\quad \land \text{UNCHANGED } \langle configuration, mastership, conn, target, history \rangle
\end{array}
$$

$$
\begin{array}{l}
CommitChange(n, i) \triangleq \\
\quad \land \lor \land transactions[i].change.commit = Pending \\
\qquad\quad \land configuration.committed.change = i - 1 \\
\qquad\quad \land \lor \land configuration.committed.target \neq i \\
\qquad\qquad\quad \land configuration.committed.index = configuration.committed.target \\
\qquad\qquad\quad \land configuration.committed.index \in \text{DOMAIN } transactions \Rightarrow \\
\qquad\qquad\qquad\quad \lor \land configuration.committed.target = configuration.committed.index \\
\qquad\qquad\qquad\qquad\quad \land transactions[configuration.committed.index].change.commit \in Done \\
\qquad\qquad\qquad\quad \lor \land configuration.committed.target < configuration.committed.index \\
\qquad\qquad\qquad\qquad\quad \land transactions[configuration.committed.index].rollback.commit \in Done
\end{array}
$$

$$
\begin{array}{l}
\quad \land\ configuration' = [configuration\ \text{EXCEPT}\ !.committed.target = i] \\
\quad \land\ history' = Append(history, [\\
\qquad\qquad type \mapsto Change, \\
\qquad\qquad phase \mapsto Commit, \\
\qquad\qquad index \mapsto i, \\
\qquad\qquad status \mapsto InProgress]) \\
\quad \land\ \text{UNCHANGED}\ \langle transactions \rangle \\
\lor\ \land\ configuration.committed.target = i \\
\quad \land\ transactions' = [transactions\ \text{EXCEPT}\ ![i].change.commit = InProgress, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ![i].rollback.index = configuration.committed.revisio \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ![i].rollback.values = [\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad p \in \text{DOMAIN}\ transactions[i].change.values \mapsto \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{IF}\ p \in \text{DOMAIN}\ configuration.committed.values\ \text{TH} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad configuration.committed.values[p] \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE}\ Nil]] \\
\quad \land\ \text{UNCHANGED}\ \langle configuration, history \rangle \\
\lor\ \land\ transactions[i].change.commit = InProgress \\
\quad \land\ \lor\ \land\ configuration.committed.index \neq i \\
\qquad \land\ \lor\ \land\ configuration' = [configuration\ \text{EXCEPT}\ !.committed.index = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad !.committed.change = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad !.committed.revision = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad !.committed.ordinal = configuration.committed. \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad !.committed.values = transactions[i].change.va \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad configuration.committ \\
\qquad\qquad \land\ history' = Append(history, [\\
\qquad\qquad\qquad\qquad type \mapsto Change, \\
\qquad\qquad\qquad\qquad phase \mapsto Commit, \\
\qquad\qquad\qquad\qquad index \mapsto i, \\
\qquad\qquad\qquad\qquad status \mapsto Complete]) \\
\qquad\quad \lor\ \land\ configuration' = [configuration\ \text{EXCEPT}\ !.committed.index = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad !.committed.change = i] \\
\qquad\qquad \land\ history' = Append(history, [\\
\qquad\qquad\qquad\qquad type \mapsto Change, \\
\qquad\qquad\qquad\qquad phase \mapsto Commit, \\
\qquad\qquad\qquad\qquad index \mapsto i, \\
\qquad\qquad\qquad\qquad status \mapsto Failed]) \\
\quad \land\ \text{UNCHANGED}\ \langle transactions \rangle \\
\lor\ \land\ configuration.committed.index = i \\
\quad \land\ \lor\ \land\ configuration.committed.revision = i \\
\qquad\quad \land\ transactions' = [transactions\ \text{EXCEPT}\ ![i].change.commit = Complete, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ![i].change.ordinal = configuration.committed.ord \\
\qquad\quad \lor\ \land\ configuration.committed.revision \neq i \\
\qquad\qquad \land\ transactions' = [transactions\ \text{EXCEPT}\ ![i].change.commit = Failed, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad ![i].change.apply = Canceled] \\
\quad \land\ \text{UNCHANGED}\ \langle configuration, history \rangle
\end{array}
$$

```
    ∧ UNCHANGED ⟨mastership, conn, target⟩

CommitRollback(n, i) ≜
    ∧ ∨ ∧ transactions[i].rollback.commit = Pending
        ∧ configuration.committed.revision = i
        ∧ ∨ ∧ configuration.committed.target = i
            ∧ configuration.committed.index = configuration.committed.target
            ∧ ∨ ∧ configuration.committed.index = i
                ∧ transactions[configuration.committed.index].change.commit = Complete
              ∨ ∧ configuration.committed.index > i
                ∧ transactions[configuration.committed.index].rollback.commit = Complete
            ∧ configuration' = [configuration EXCEPT !.committed.target = transactions[i].rollback.index]
            ∧ history' = Append(history, [
                                type   ↦ Rollback,
                                phase  ↦ Commit,
                                index  ↦ i,
                                status ↦ InProgress])
            ∧ UNCHANGED ⟨transactions⟩
          ∨ ∧ configuration.committed.revision = i
            ∧ configuration.committed.target = transactions[i].rollback.index
            ∧ transactions' = [transactions EXCEPT ![i].rollback.commit = InProgress]
            ∧ UNCHANGED ⟨configuration, history⟩
      ∨ ∧ transactions[i].rollback.commit = InProgress
        ∧ ∨ ∧ configuration.committed.revision = i
            ∧ configuration' = [configuration EXCEPT !.committed.index    = i,
                                                     !.committed.ordinal  = configuration.committed.ordin
                                                     !.committed.revision = transactions[i].rollback.index,
                                                     !.committed.values   = transactions[i].rollback.values
                                                                            configuration.committed.va
            ∧ history' = Append(history, [
                                type   ↦ Rollback,
                                phase  ↦ Commit,
                                index  ↦ i,
                                status ↦ Complete])
            ∧ UNCHANGED ⟨transactions⟩
          ∨ ∧ configuration.committed.revision = transactions[i].rollback.index
            ∧ transactions' = [transactions EXCEPT ![i].rollback.commit  = Complete,
                                                   ![i].rollback.ordinal = configuration.committed.ordinal
            ∧ UNCHANGED ⟨configuration, history⟩
    ∧ UNCHANGED ⟨mastership, conn, target⟩

ApplyChange(n, i) ≜
    ∧ transactions[i].change.commit = Complete
    ∧ ∨ ∧ transactions[i].change.apply = Pending
        ∧ ∨ ∧ configuration.applied.ordinal = transactions[i].change.ordinal − 1
```

$$
\begin{array}{l}
\land \lor \land \mathit{configuration.applied.target} \neq i \\
\quad \land \mathit{configuration.applied.index} \in \text{DOMAIN } \mathit{transactions} \Rightarrow \\
\qquad \lor \land \mathit{configuration.applied.target} = \mathit{configuration.applied.index} \\
\qquad\quad \land \mathit{transactions}[\mathit{configuration.applied.index}].\mathit{change.apply} \in \mathit{Done} \\
\qquad \lor \land \mathit{configuration.applied.target} < \mathit{configuration.applied.index} \\
\qquad\quad \land \mathit{transactions}[\mathit{configuration.applied.index}].\mathit{rollback.apply} \in \mathit{Done} \\
\quad \land \lor \land \mathit{configuration.applied.revision} = \mathit{transactions}[i].\mathit{rollback.index} \\
\qquad \land \mathit{configuration}' = [\mathit{configuration} \text{ EXCEPT } !.\mathit{applied.target} = i] \\
\qquad \land \mathit{history}' = \mathit{Append}(\mathit{history}, [\\
\qquad\qquad\qquad\qquad \mathit{type} \mapsto \mathit{Change}, \\
\qquad\qquad\qquad\qquad \mathit{phase} \mapsto \mathit{Apply}, \\
\qquad\qquad\qquad\qquad \mathit{index} \mapsto i, \\
\qquad\qquad\qquad\qquad \mathit{status} \mapsto \mathit{InProgress}]) \\
\quad\ \lor \land \lor \mathit{transactions}[i].\mathit{phase} = \mathit{Rollback} \\
\qquad\quad \lor \mathit{configuration.applied.revision} < \mathit{transactions}[i].\mathit{rollback.index} \\
\qquad \land \mathit{configuration}' = [\mathit{configuration} \text{ EXCEPT } !.\mathit{applied.target} = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad !.\mathit{applied.index} = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad !.\mathit{applied.ordinal} = \mathit{transactions}[i].\mathit{change.or} \\
\qquad \land \mathit{history}' = \mathit{Append}(\mathit{history}, [\\
\qquad\qquad\qquad\qquad \mathit{type} \mapsto \mathit{Change}, \\
\qquad\qquad\qquad\qquad \mathit{phase} \mapsto \mathit{Apply}, \\
\qquad\qquad\qquad\qquad \mathit{index} \mapsto i, \\
\qquad\qquad\qquad\qquad \mathit{status} \mapsto \mathit{Aborted}]) \\
\quad\ \land \text{UNCHANGED } \langle \mathit{transactions} \rangle \\
\quad\ \lor \land \mathit{configuration.applied.target} = i \\
\qquad \land \mathit{transactions}' = [\mathit{transactions} \text{ EXCEPT } ![i].\mathit{change.apply} = \mathit{InProgress}] \\
\qquad \land \text{UNCHANGED } \langle \mathit{configuration}, \mathit{history} \rangle \\
\ \lor \land \mathit{configuration.applied.ordinal} = \mathit{transactions}[i].\mathit{change.ordinal} \\
\quad\ \land \mathit{transactions}' = [\mathit{transactions} \text{ EXCEPT } ![i].\mathit{change.apply} = \mathit{Aborted}] \\
\quad\ \land \text{UNCHANGED } \langle \mathit{configuration}, \mathit{history} \rangle \\
\land \text{UNCHANGED } \langle \mathit{target} \rangle \\
\lor \land \mathit{transactions}[i].\mathit{change.apply} = \mathit{InProgress}
\end{array}
$$

If the change has not yet been applied, attempt to apply it.

$$
\begin{array}{l}
\land \lor \land \mathit{configuration.applied.ordinal} \neq \mathit{transactions}[i].\mathit{change.ordinal} \\
\quad \land \lor \land \mathit{transactions}[i].\mathit{phase} = \mathit{Change} \\
\qquad \land \mathit{configuration.state} = \mathit{Complete} \\
\qquad \land \mathit{configuration.term} = \mathit{mastership.term} \\
\qquad \land \mathit{conn}[n].\mathit{id} = \mathit{mastership.conn} \\
\qquad \land \mathit{conn}[n].\mathit{connected} \\
\qquad \land \mathit{target.running} \\
\qquad \land \lor \land \mathit{target}' = [\mathit{target} \text{ EXCEPT } !.\mathit{values} = \mathit{transactions}[i].\mathit{change.values} \mathbin{@@} \mathit{target.values}] \\
\qquad\quad \land \mathit{configuration}' = [\mathit{configuration} \text{ EXCEPT } !.\mathit{applied.index} = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad !.\mathit{applied.ordinal} = \mathit{transactions}[i].\mathit{change.} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad !.\mathit{applied.revision} = i, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad !.\mathit{applied.values} = \mathit{transactions}[i].\mathit{change.}
\end{array}
$$

$configuration.applied$

$\land\ history' = Append(history, [$
$type \mapsto Change,$
$phase \mapsto Apply,$
$index \mapsto i,$
$status \mapsto Complete])$

$\lor\ \land\ configuration' = [configuration \text{ EXCEPT } !.applied.index = i,$
$!.applied.ordinal = transactions[i].change.o$
$\land\ history' = Append(history, [$
$type \mapsto Change,$
$phase \mapsto Apply,$
$index \mapsto i,$
$status \mapsto Failed])$
$\land \text{ UNCHANGED } \langle target \rangle$

$\lor\ \land\ transactions[i].phase = Rollback$
$\land\ configuration' = [configuration \text{ EXCEPT } !.applied.index = i,$
$!.applied.ordinal = transactions[i].change.ordina$
$\land\ history' = Append(history, [$
$type \mapsto Change,$
$phase \mapsto Apply,$
$index \mapsto i,$
$status \mapsto Failed])$
$\land \text{ UNCHANGED } \langle target \rangle$

$\land \text{ UNCHANGED } \langle transactions \rangle$

If the change has been applied, update the transaction status.

$\lor\ \land\ configuration.applied.ordinal = transactions[i].change.ordinal$
$\land\ \lor\ \land\ configuration.applied.revision = i$
$\land\ transactions' = [transactions \text{ EXCEPT } ![i].change.apply = Complete]$
$\lor\ \land\ configuration.applied.revision = transactions[i].rollback.index$
$\land\ transactions' = [transactions \text{ EXCEPT } ![i].change.apply = Failed]$
$\land \text{ UNCHANGED } \langle configuration, target, history \rangle$

$\land \text{ UNCHANGED } \langle mastership, conn \rangle$

$ApplyRollback(n, i) \triangleq$
$\land\ transactions[i].rollback.commit = Complete$
$\land\ \lor\ \land\ transactions[i].rollback.apply = Pending$
$\land\ \lor\ \land\ configuration.applied.ordinal = transactions[i].rollback.ordinal - 1$
$\land\ \lor\ \land\ configuration.applied.target \neq transactions[i].rollback.index$
$\land\ \lor\ \land\ configuration.applied.index = i$
$\land\ transactions[configuration.applied.index].change.apply \in Done$
$\lor\ \land\ configuration.applied.index > i$
$\land\ transactions[configuration.applied.index].rollback.apply \in Done$
$\land\ configuration' = [configuration \text{ EXCEPT } !.applied.target = transactions[i].rollback.index]$
$\land\ history' = Append(history, [$
$type \mapsto Rollback,$

```
                                    phase ↦ Apply,
                                    index ↦ i,
                                    status ↦ InProgress])
                    ∧ UNCHANGED ⟨transactions⟩
                ∨ ∧ configuration.applied.target = transactions[i].rollback.index
                  ∧ transactions′ = [transactions EXCEPT ![i].rollback.apply = InProgress]
                  ∧ UNCHANGED ⟨configuration, history⟩
        ∧ UNCHANGED ⟨target⟩
    ∨ ∧ transactions[i].rollback.apply = InProgress
      If this transaction has not yet been applied, attempt to apply it.
      ∧ ∨ ∧ configuration.applied.ordinal ≠ transactions[i].rollback.ordinal
          ∧ configuration.state = Complete
          ∧ configuration.term = mastership.term
          ∧ conn[n].id = mastership.conn
          ∧ conn[n].connected
          ∧ target.running
          ∧ target′ = [target EXCEPT !.values = transactions[i].rollback.values @@ target.values]
          ∧ configuration′ = [configuration EXCEPT !.applied.index    = i,
                                                   !.applied.ordinal  = transactions[i].rollback.ordinal,
                                                   !.applied.revision = transactions[i].rollback.index,
                                                   !.applied.values   = transactions[i].rollback.values @@
                                                                        configuration.applied.values]
          ∧ history′ = Append(history, [
                              type   ↦ Rollback,
                              phase  ↦ Apply,
                              index  ↦ i,
                              status ↦ Complete])
          ∧ UNCHANGED ⟨transactions⟩
        If the change has been applied, update the transaction status.
        ∨ ∧ configuration.applied.ordinal = transactions[i].rollback.ordinal
          ∧ configuration.applied.revision = transactions[i].rollback.index
          ∧ transactions′ = [transactions EXCEPT ![i].rollback.apply = Complete]
          ∧ UNCHANGED ⟨configuration, target, history⟩
    ∧ UNCHANGED ⟨mastership, conn⟩

ReconcileTransaction(n, i) ≜
    ∧ i ∈ DOMAIN transactions
    ∧ mastership.master = n
    ∧ ∨ CommitChange(n, i)
      ∨ ApplyChange(n, i)
      ∨ CommitRollback(n, i)
      ∨ ApplyRollback(n, i)
```