
MODULE *Config*

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

INSTANCE *TLC*

GenerateTestCases \triangleq FALSE

Nil \triangleq "<nil>"

Change \triangleq "Change"

Rollback \triangleq "Rollback"

Commit \triangleq "Commit"

Apply \triangleq "Apply"

Pending \triangleq "Pending"

InProgress \triangleq "InProgress"

Complete \triangleq "Complete"

Aborted \triangleq "Aborted"

Failed \triangleq "Failed"

Done \triangleq { *Complete*, *Aborted*, *Failed* }

Node \triangleq { "node1" }

NumTransactions \triangleq 4

NumTerms \triangleq 2

NumConns \triangleq 2

NumStarts \triangleq 2

Path \triangleq { "path1" }

Value \triangleq { "value1", "value2" }

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

VARIABLE *transaction*

A record of per-target proposals

VARIABLE *proposal*

A record of per-target configurations

VARIABLE *configuration*

A record of target masterships
VARIABLE *mastership*

A record of node connections to the target
VARIABLE *conn*

The target state
VARIABLE *target*

A sequence of state changes used for model checking.
VARIABLE *history*

$\text{vars} \triangleq \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{conn}, \text{target}, \text{history} \rangle$

LOCAL *Transaction* \triangleq INSTANCE *Transaction*

LOCAL *Proposal* \triangleq INSTANCE *Proposal*

LOCAL *Configuration* \triangleq INSTANCE *Configuration*

LOCAL *Mastership* \triangleq INSTANCE *Mastership*

LOCAL *Target* \triangleq INSTANCE *Target*

$\text{RequestChange}(p, v) \triangleq$
 $\wedge \text{Transaction!RequestChange}(p, v)$
 $\wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn}, \text{target}, \text{history} \rangle$

$\text{RequestRollback}(i) \triangleq$
 $\wedge \text{Transaction!RequestRollback}(i)$
 $\wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn}, \text{target}, \text{history} \rangle$

$\text{ReconcileTransaction}(n, i) \triangleq$
 $\wedge i \in \text{DOMAIN } \text{transaction}$
 $\wedge \text{Transaction!ReconcileTransaction}(n, i)$
 $\wedge \text{UNCHANGED } \langle \text{mastership}, \text{conn}, \text{target}, \text{history} \rangle$
 $\wedge \text{GenerateTestCases} \Rightarrow \text{Transaction!Test!Log}([node \mapsto n, index \mapsto i])$

$\text{ReconcileProposal}(n, i) \triangleq$
 $\wedge i \in \text{DOMAIN } \text{proposal}$
 $\wedge \text{Proposal!ReconcileProposal}(n, i)$
 $\wedge \text{UNCHANGED } \langle \text{transaction} \rangle$
 $\wedge \text{GenerateTestCases} \Rightarrow \text{Proposal!Test!Log}([node \mapsto n, index \mapsto i])$

$\text{ReconcileConfiguration}(n) \triangleq$
 $\wedge \text{Configuration!ReconcileConfiguration}(n)$

$$\begin{aligned}
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{history} \rangle \\
& \wedge \text{GenerateTestCases} \Rightarrow \text{Configuration!Test!Log}([node \mapsto n]) \\
\text{ReconcileMastership}(n) & \triangleq \\
& \wedge \text{Mastership!ReconcileMastership}(n) \\
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{target}, \text{history} \rangle \\
& \wedge \text{GenerateTestCases} \Rightarrow \text{Mastership!Test!Log}([node \mapsto n]) \\
\text{ConnectNode}(n) & \triangleq \\
& \wedge \text{Target!Connect}(n) \\
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{history} \rangle \\
\text{DisconnectNode}(n) & \triangleq \\
& \wedge \text{Target!Disconnect}(n) \\
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{history} \rangle \\
\text{StartTarget} & \triangleq \\
& \wedge \text{Target!Start} \\
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{history} \rangle \\
\text{StopTarget} & \triangleq \\
& \wedge \text{Target!Stop} \\
& \wedge \text{UNCHANGED } \langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{history} \rangle
\end{aligned}$$

Formal specification, constraints, and theorems.

$$\begin{aligned}
\text{Init} & \triangleq \\
& \wedge \text{transaction} = [\\
& \quad i \in \{\} \mapsto [\\
& \quad \quad \text{type} \mapsto \text{Change}, \\
& \quad \quad \text{proposal} \mapsto 0, \\
& \quad \quad \text{values} \mapsto [p \in \{\} \mapsto \text{Nil}], \\
& \quad \quad \text{commit} \mapsto \text{Pending}, \\
& \quad \quad \text{apply} \mapsto \text{Pending}] \\
& \wedge \text{proposal} = [\\
& \quad i \in \{\} \mapsto [\\
& \quad \quad \text{phase} \mapsto \text{Nil}, \\
& \quad \quad \text{change} \mapsto [\\
& \quad \quad \quad \text{commit} \mapsto \text{Nil}, \\
& \quad \quad \quad \text{apply} \mapsto \text{Nil}, \\
& \quad \quad \quad \text{values} \mapsto [\\
& \quad \quad \quad \quad p \in \{\} \mapsto [\\
& \quad \quad \quad \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \quad \quad \quad \text{value} \mapsto \text{Nil}]]], \\
& \quad \text{rollback} \mapsto [\\
& \quad \quad \text{commit} \mapsto \text{Nil},
\end{aligned}$$

$$\begin{aligned}
& \text{apply} \mapsto \text{Nil}, \\
& \text{values} \mapsto [\\
& \quad p \in \{\} \mapsto [\\
& \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \text{value} \mapsto \text{Nil}]]]] \\
\wedge \text{configuration} = [\\
& \quad \text{state} \mapsto \text{InProgress}, \\
& \quad \text{term} \mapsto 0, \\
& \quad \text{committed} \mapsto [\\
& \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \text{revision} \mapsto 0, \\
& \quad \quad \text{values} \mapsto [\\
& \quad \quad \quad p \in \{\} \mapsto [\\
& \quad \quad \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \quad \quad \text{value} \mapsto \text{Nil}]], \\
& \quad \text{applied} \mapsto [\\
& \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \text{revision} \mapsto 0, \\
& \quad \quad \text{target} \mapsto 0, \\
& \quad \quad \text{values} \mapsto [\\
& \quad \quad \quad p \in \{\} \mapsto [\\
& \quad \quad \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \quad \quad \text{value} \mapsto \text{Nil}]]]] \\
\wedge \text{target} = [\\
& \quad \text{id} \mapsto 1, \\
& \quad \text{running} \mapsto \text{TRUE}, \\
& \quad \text{values} \mapsto [\\
& \quad \quad p \in \{\} \mapsto [\\
& \quad \quad \quad \text{index} \mapsto 0, \\
& \quad \quad \quad \text{value} \mapsto \text{Nil}]] \\
\wedge \text{mastership} = [\\
& \quad \text{master} \mapsto \text{CHOOSE } n \in \text{Node} : \text{TRUE}, \\
& \quad \text{term} \mapsto 1, \\
& \quad \text{conn} \mapsto 1] \\
\wedge \text{conn} = [\\
& \quad n \in \text{Node} \mapsto [\\
& \quad \quad \text{id} \mapsto 1, \\
& \quad \quad \text{connected} \mapsto \text{TRUE}] \\
\wedge \text{history} = \langle \rangle \\
\text{Next} \triangleq \\
& \vee \exists p \in \text{Path}, v \in \text{Value} : \\
& \quad \text{RequestChange}(p, v) \\
& \vee \exists i \in \text{DOMAIN transaction} : \\
& \quad \text{RequestRollback}(i)
\end{aligned}$$

$$\begin{aligned}
& \vee \exists n \in \text{Node} : \\
& \quad \exists i \in \text{DOMAIN } \text{transaction} : \\
& \quad \quad \text{ReconcileTransaction}(n, i) \\
& \vee \exists n \in \text{Node} : \\
& \quad \exists i \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \text{ReconcileProposal}(n, i) \\
& \vee \exists n \in \text{Node} : \\
& \quad \text{ReconcileConfiguration}(n) \\
& \vee \exists n \in \text{Node} : \\
& \quad \text{ReconcileMastership}(n) \\
& \vee \exists n \in \text{Node} : \\
& \quad \vee \text{ConnectNode}(n) \\
& \quad \vee \text{DisconnectNode}(n) \\
& \vee \text{StartTarget} \\
& \vee \text{StopTarget} \\
\text{Spec} & \triangleq \\
& \wedge \text{Init} \\
& \wedge \square[\text{Next}]_{\text{vars}} \\
& \wedge \forall p \in \text{Path}, v \in \text{Value} : \\
& \quad \text{WF}_{\langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{target} \rangle}(\text{Transaction!RequestChange}(p, v)) \\
& \wedge \forall i \in 1 \dots \text{NumTransactions} : i \in \text{DOMAIN } \text{transaction} \Rightarrow \\
& \quad \text{WF}_{\langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{target} \rangle}(\text{Transaction!RequestRollback}(i)) \\
& \wedge \forall n \in \text{Node}, i \in 1 \dots \text{NumTransactions} : \\
& \quad \text{WF}_{\langle \text{transaction}, \text{proposal}, \text{configuration}, \text{mastership}, \text{target} \rangle}(\text{Transaction!ReconcileTransaction}(n, i)) \\
& \wedge \forall n \in \text{Node}, i \in 1 \dots \text{NumTransactions} : \\
& \quad \text{WF}_{\langle \text{proposal}, \text{configuration}, \text{mastership}, \text{conn}, \text{target}, \text{history} \rangle}(\text{Proposal!ReconcileProposal}(n, i)) \\
& \wedge \forall n \in \text{Node} : \\
& \quad \text{WF}_{\langle \text{configuration}, \text{mastership}, \text{conn}, \text{target} \rangle}(\text{Configuration!ReconcileConfiguration}(n)) \\
& \wedge \forall n \in \text{Node} : \\
& \quad \text{WF}_{\langle \text{mastership}, \text{conn} \rangle}(\text{Mastership!ReconcileMastership}(n)) \\
& \wedge \forall n \in \text{Node} : \\
& \quad \text{WF}_{\langle \text{conn}, \text{target} \rangle}(\text{Target!Connect}(n) \vee \text{Target!Disconnect}(n)) \\
& \wedge \text{WF}_{\langle \text{conn}, \text{target} \rangle}(\text{Target!Start} \vee \text{Target!Stop})
\end{aligned}$$

$$\text{LimitTransactions} \triangleq \text{Len}(\text{transaction}) \leq \text{NumTransactions}$$

$$\begin{aligned}
\text{LimitTerms} & \triangleq \\
& \vee \text{mastership.term} < \text{NumTerms} \\
& \vee \wedge \text{mastership.term} = \text{NumTerms} \\
& \wedge \text{mastership.master} \neq \text{Nil}
\end{aligned}$$

$$\begin{aligned}
\text{LimitConns} & \triangleq \\
& \forall n \in \text{DOMAIN } \text{conn} :
\end{aligned}$$

$$\begin{aligned}
& \vee \text{conn}[n].id < \text{NumConns} \\
& \vee \wedge \text{conn}[n].id = \text{NumConns} \\
& \wedge \text{conn}[n].connected
\end{aligned}$$

$$\begin{aligned}
\text{LimitStarts} & \triangleq \\
& \vee \text{target}.id < 2 \\
& \vee \wedge \text{target}.id = 2 \\
& \wedge \text{target}.running
\end{aligned}$$

$$\begin{aligned}
\text{TypeOK} & \triangleq \\
& \wedge \text{Transaction! TypeOK} \\
& \wedge \text{Proposal! TypeOK} \\
& \wedge \text{Configuration! TypeOK} \\
& \wedge \text{Mastership! TypeOK}
\end{aligned}$$

$$\begin{aligned}
\text{LOCAL } \text{IsOrderedChange}(p, i) & \triangleq \\
& \wedge \text{history}[i].type = \text{Change} \\
& \wedge \text{history}[i].phase = p \\
& \wedge \neg \exists j \in \text{DOMAIN } \text{history} : \\
& \quad \wedge j < i \\
& \quad \wedge \text{history}[j].type = \text{Change} \\
& \quad \wedge \text{history}[j].phase = p \\
& \quad \wedge \text{history}[j].index \geq \text{history}[i].index
\end{aligned}$$

$$\begin{aligned}
\text{LOCAL } \text{IsOrderedRollback}(p, i) & \triangleq \\
& \wedge \text{history}[i].type = \text{Rollback} \\
& \wedge \text{history}[i].phase = p \\
& \wedge \neg \exists j \in \text{DOMAIN } \text{history} : \\
& \quad \wedge j < i \\
& \quad \wedge \text{history}[j].type = \text{Change} \\
& \quad \wedge \text{history}[j].phase = p \\
& \quad \wedge \text{history}[j].index > \text{history}[i].index \\
& \wedge \neg \exists k \in \text{DOMAIN } \text{history} : \\
& \quad \wedge k > j \\
& \quad \wedge k < i \\
& \quad \wedge \text{history}[k].type = \text{Rollback} \\
& \quad \wedge \text{history}[k].phase = p \\
& \quad \wedge \text{history}[k].index = \text{history}[j].index
\end{aligned}$$

$$\begin{aligned}
\text{Order} & \triangleq \\
& \wedge \forall i \in \text{DOMAIN } \text{history} : \\
& \quad \vee \text{IsOrderedChange}(\text{Commit}, i) \\
& \quad \vee \text{IsOrderedChange}(\text{Apply}, i) \\
& \quad \vee \text{IsOrderedRollback}(\text{Commit}, i) \\
& \quad \vee \text{IsOrderedRollback}(\text{Apply}, i)
\end{aligned}$$

$$\begin{aligned}
& \wedge \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \wedge \text{proposal}[i].\text{change.apply} = \text{Failed} \\
& \quad \wedge \text{proposal}[i].\text{rollback.apply} \neq \text{Complete} \\
& \quad \Rightarrow \forall j \in \text{DOMAIN } \text{proposal} : (j > i \Rightarrow \\
& \quad \quad (\text{proposal}[j].\text{change.apply} \in \{\text{Pending}, \text{Aborted}\}))
\end{aligned}$$

Consistency \triangleq

$$\begin{aligned}
& \wedge \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \vee \text{configuration.committed.index} < i \\
& \quad \vee \text{configuration.committed.revision} < i \\
& \quad \Rightarrow \neg \exists p \in \text{DOMAIN } \text{configuration.committed.values} : \\
& \quad \quad \text{configuration.committed.values}[p].\text{index} = i \\
& \wedge \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \vee \text{configuration.applied.index} < i \\
& \quad \vee \text{configuration.applied.revision} < i \\
& \quad \Rightarrow \wedge \neg \exists p \in \text{DOMAIN } \text{configuration.applied.values} : \\
& \quad \quad \text{configuration.applied.values}[p].\text{index} = i \\
& \quad \wedge \neg \exists p \in \text{DOMAIN } \text{target.values} : \\
& \quad \quad \text{target.values}[p].\text{index} = i \\
& \wedge \wedge \text{target.running} \\
& \wedge \text{configuration.applied.target} = \text{target.id} \\
& \wedge \text{configuration.state} = \text{Complete} \\
& \Rightarrow \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \wedge \text{configuration.applied.index} \geq i \\
& \quad \wedge \text{configuration.applied.revision} \geq i \\
& \quad \Rightarrow \forall p \in \text{DOMAIN } \text{proposal}[i].\text{change.values} : \\
& \quad \quad \wedge \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j > i \\
& \quad \quad \quad \wedge \text{configuration.applied.index} \geq j \\
& \quad \quad \quad \wedge \text{configuration.applied.revision} \geq j \\
& \quad \Rightarrow \wedge p \in \text{DOMAIN } \text{target.values} \\
& \quad \quad \wedge \text{target.values}[p].\text{value} = \text{proposal}[i].\text{change.values}[p].\text{value} \\
& \quad \quad \wedge \text{target.values}[p].\text{index} = \text{proposal}[i].\text{change.values}[p].\text{index}
\end{aligned}$$

Safety $\triangleq \Box(\text{Order} \wedge \text{Consistency})$

THEOREM $\text{Spec} \Rightarrow \text{Safety}$

Terminates(*i*) \triangleq

$$\begin{aligned}
& \wedge i \in \text{DOMAIN } \text{transaction} \\
& \wedge \text{transaction}[i].\text{commit} \in \text{Done} \\
& \wedge \text{transaction}[i].\text{apply} \in \text{Done} \\
& \wedge \text{transaction}[i].\text{index} \in \text{DOMAIN } \text{proposal} \\
& \wedge \vee \wedge \text{transaction}[i].\text{type} = \text{Change} \\
& \quad \wedge \vee \text{proposal}[\text{transaction}[i].\text{index}].\text{change.commit} \in \{\text{Aborted}, \text{Failed}\} \\
& \quad \vee \text{proposal}[\text{transaction}[i].\text{index}].\text{change.apply} \in \text{Done}
\end{aligned}$$

$$\begin{aligned}
& \vee \wedge \text{transaction}[i].\text{type} = \text{Rollback} \\
& \wedge \vee \text{proposal}[\text{transaction}[i].\text{index}].\text{rollback.commit} \in \{\text{Aborted}, \text{Failed}\} \\
& \vee \text{proposal}[\text{transaction}[i].\text{index}].\text{rollback.apply} \in \text{Done}
\end{aligned}$$

$$\begin{aligned}
\text{Termination} & \triangleq \\
& \forall i \in 1 \dots \text{NumTransactions} : \Diamond \text{Terminates}(i)
\end{aligned}$$

$$\text{Liveness} \triangleq \text{Termination}$$

THEOREM $\text{Spec} \Rightarrow \text{Liveness}$