

EXTENDS

*Northbound*,  
*Transaction*,  
*Proposal*,  
*Configuration*,  
*Southbound*

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

LOCAL INSTANCE *TLC*

*vars*  $\triangleq$   $\langle \textit{transaction}, \textit{proposal}, \textit{configuration}, \textit{mastership}, \textit{target} \rangle$

---

Formal specification, constraints, and theorems.

*Init*  $\triangleq$

$\wedge$  *InitTransaction*  
 $\wedge$  *InitProposal*  
 $\wedge$  *InitConfiguration*  
 $\wedge$  *InitNorthbound*  
 $\wedge$  *InitSouthbound*

*Next*  $\triangleq$

$\vee \wedge$  *NextTransaction*  
 $\wedge$  UNCHANGED  $\langle \textit{configuration}, \textit{target}, \textit{mastership} \rangle$   
 $\vee \wedge$  *NextProposal*  
 $\wedge$  UNCHANGED  $\langle \textit{transaction} \rangle$   
 $\vee \wedge$  *NextConfiguration*  
 $\wedge$  UNCHANGED  $\langle \textit{transaction}, \textit{proposal} \rangle$   
 $\vee \wedge$  *NextNorthbound*  
 $\wedge$  UNCHANGED  $\langle \textit{proposal}, \textit{configuration}, \textit{target}, \textit{mastership} \rangle$   
 $\vee \wedge$  *NextSouthbound*  
 $\wedge$  UNCHANGED  $\langle \textit{transaction}, \textit{proposal}, \textit{configuration} \rangle$

*Spec*  $\triangleq$  *Init*  $\wedge$   $\Box[\textit{Next}]_{\textit{vars}} \wedge \text{WF}_{\textit{vars}}(\textit{Next})$

*Order*  $\triangleq$

$\forall t \in \text{DOMAIN } \textit{proposal} :$   
 $\forall i \in \text{DOMAIN } \textit{proposal}[t] :$   
 $\wedge \wedge \textit{proposal}[t][i].\textit{phase} = \textit{ProposalCommit}$   
 $\wedge \textit{proposal}[t][i].\textit{state} = \textit{ProposalInProgress}$

$$\begin{aligned}
&\Rightarrow \neg \exists j \in \text{DOMAIN } \text{proposal}[t] : \\
&\quad \wedge j > i \\
&\quad \wedge \text{proposal}[t][j].\text{phase} = \text{ProposalCommit} \\
&\quad \wedge \text{proposal}[t][j].\text{state} = \text{ProposalComplete} \\
&\wedge \wedge \text{proposal}[t][i].\text{phase} = \text{ProposalApply} \\
&\quad \wedge \text{proposal}[t][i].\text{state} = \text{ProposalInProgress} \\
&\Rightarrow \neg \exists j \in \text{DOMAIN } \text{proposal}[t] : \\
&\quad \wedge j > i \\
&\quad \wedge \text{proposal}[t][j].\text{phase} = \text{ProposalApply} \\
&\quad \wedge \text{proposal}[t][j].\text{state} = \text{ProposalComplete}
\end{aligned}$$

*Consistency*  $\triangleq$

$\forall t \in \text{DOMAIN } \text{target} :$

LET

Compute the transaction indexes that have been applied to the target

$$\begin{aligned}
\text{targetIndexes} &\triangleq \{i \in \text{DOMAIN } \text{transaction} : \\
&\quad \wedge i \in \text{DOMAIN } \text{proposal}[t] \\
&\quad \wedge \text{proposal}[t][i].\text{phase} = \text{ProposalApply} \\
&\quad \wedge \text{proposal}[t][i].\text{state} = \text{ProposalComplete} \\
&\quad \wedge t \in \text{transaction}[i].\text{targets} \\
&\quad \wedge \neg \exists j \in \text{DOMAIN } \text{transaction} : \\
&\quad \quad \wedge j > i \\
&\quad \quad \wedge \text{transaction}[j].\text{type} = \text{TransactionRollback} \\
&\quad \quad \wedge \text{transaction}[j].\text{rollback} = i \\
&\quad \quad \wedge \text{transaction}[j].\text{phase} = \text{TransactionApply} \\
&\quad \quad \wedge \text{transaction}[j].\text{state} = \text{TransactionComplete}\}
\end{aligned}$$

Compute the set of paths in the target that have been updated by transactions

$$\text{appliedPaths} \triangleq \text{UNION } \{\text{DOMAIN } \text{proposal}[t][i].\text{change.values} : i \in \text{targetIndexes}\}$$

Compute the highest index applied to the target for each path

$$\begin{aligned}
\text{pathIndexes} &\triangleq [p \in \text{appliedPaths} \mapsto \text{CHOOSE } i \in \text{targetIndexes} : \\
&\quad \forall j \in \text{targetIndexes} : \\
&\quad \quad \wedge i \geq j \\
&\quad \quad \wedge p \in \text{DOMAIN } \text{proposal}[t][i].\text{change.values}]
\end{aligned}$$

Compute the expected target configuration based on the last indexes applied to the target for each path.

$$\text{expectedConfig} \triangleq [p \in \text{DOMAIN } \text{pathIndexes} \mapsto \text{proposal}[t][\text{pathIndexes}[p]].\text{change.values}[p]]$$

IN

$$\text{target}[t] = \text{expectedConfig}$$

*Isolation*  $\triangleq$

$\forall i \in \text{DOMAIN } \text{transaction} :$

$$\begin{aligned}
&\wedge \wedge \text{transaction}[i].\text{phase} = \text{TransactionCommit} \\
&\quad \wedge \text{transaction}[i].\text{state} = \text{TransactionInProgress} \\
&\quad \wedge \text{transaction}[i].\text{isolation} = \text{Serializable} \\
&\Rightarrow \neg \exists j \in \text{DOMAIN } \text{transaction} :
\end{aligned}$$

$$\begin{aligned}
& \wedge j > i \\
& \wedge \text{transaction}[j].\text{targets} \cap \text{transaction}[i].\text{targets} \neq \{\} \\
& \wedge \text{transaction}[j].\text{phase} = \text{TransactionCommit} \\
& \wedge \wedge \text{transaction}[i].\text{phase} = \text{TransactionApply} \\
& \wedge \text{transaction}[i].\text{state} = \text{TransactionInProgress} \\
& \wedge \text{transaction}[i].\text{isolation} = \text{Serializable} \\
& \Rightarrow \neg \exists j \in \text{DOMAIN } \text{transaction} : \\
& \quad \wedge j > i \\
& \quad \wedge \text{transaction}[j].\text{targets} \cap \text{transaction}[i].\text{targets} \neq \{\} \\
& \quad \wedge \text{transaction}[j].\text{phase} = \text{TransactionApply}
\end{aligned}$$

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

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

$$\begin{aligned}
\text{Terminated}(i) & \triangleq \\
& \wedge i \in \text{DOMAIN } \text{transaction} \\
& \wedge \text{transaction}[i].\text{phase} \in \{\text{TransactionApply}, \text{TransactionAbort}\} \\
& \wedge \text{transaction}[i].\text{state} = \text{TransactionComplete}
\end{aligned}$$

$$\begin{aligned}
\text{Termination} & \triangleq \\
& \forall i \in 1 \dots \text{Len}(\text{transaction}) : \text{Terminated}(i)
\end{aligned}$$

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

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

---

\ \* Modification History  
\ \* Last modified Sun Feb 20 09:10:53 PST 2022 by jordanhalterman  
\ \* Created Wed Sep 22 13:22:32 PDT 2021 by jordanhalterman