

MODULE *FastPaxos*

This is a simplified specification of *Leslie Lamport's Fast Paxos* protocol. The following papers, *Fast Paxos* by *Leslie Lamport* and *Fast Paxos Made Easy: Theory and Implementation* by *Zhao Wenbing* was referenced in writing this specification.

This simplified specification was written by *Lim Ngian Xin Terry & Gaurav Gandhi*.

The following assumptions are made in this simplified specification.

1. There is a unique coordinator in the system. Therefore, Phase 1a and 1b can be omitted.
2. All agents in the system can communicate with one another.
3. Agents must have some stable storage that survives failure and restarts. An agent restores its state from stable storage when it restarts, so the failure of an agent is indistinguishable from its simply pausing. There is thus no need to model failures explicitly.

EXTENDS *TLC, Naturals, FiniteSets, Integers*

CONSTANTS *any, none, Replicas, Values, Ballots, Quorums*

CONSTANTS *FastQuorums, FastBallots*

VARIABLES *messages* Set of all messages sent.

VARIABLES *decision* Decided value of an acceptor.

VARIABLES *maxBallot* Maximum ballot an acceptor has seen.

VARIABLES *maxVBallot* Maximum ballot an acceptor has accepted.

VARIABLES *maxValue* Maximum value an acceptor has accepted.

VARIABLES *cValue* Value chosen by coordinator.

INSTANCE *Paxos*

ClassicBallots \triangleq *Ballots* \setminus *FastBallots* The set of ballots of classic rounds.

FastAssume \triangleq

$\wedge \forall q \in \text{FastQuorums} : q \subseteq \text{Replicas}$

$\wedge \forall q, r \in \text{FastQuorums} : q \cap r \neq \{\}$

$\wedge \forall q \in \text{FastQuorums} : (3 * \text{Cardinality}(\text{Replicas})) \div 4 \leq \text{Cardinality}(q)$

$\wedge \forall q \in \text{Quorums} : \forall r, s \in \text{FastQuorums} : q \cap r \cap s \neq \{\}$

ASSUME *PaxosAssume* \wedge *FastAssume*

IsMajorityValue(*M*, *v*) \triangleq $\text{Cardinality}(M) \div 2 < \text{Cardinality}(\{m \in M : m.\text{value} = v\})$

Phase 2a (Fast):

The coordinator starts a fast round by sending a *P2a* “Any” message, if no other values has been proposed before.

FastAny \triangleq

\wedge UNCHANGED $\langle \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, \text{cValue} \rangle$

$\wedge \exists f \in \text{FastBallots} :$

$\wedge \text{SendMessage}([type \mapsto \text{“P2a”},$
 $\text{ballot} \mapsto f,$
 $\text{value} \mapsto \text{any}])$

Phase 2b (Fast):

Acceptors can reply to a *P2a* “Any” message with a *P2b* message containing their proposed value.

$$\begin{aligned}
\text{FastPropose} &\triangleq \\
&\wedge \text{UNCHANGED } \langle \text{decision}, \text{cValue} \rangle \\
&\wedge \exists a \in \text{Replicas}, m \in \text{p2aMessages}, v \in \text{Values} : \\
&\quad \wedge m.\text{value} = \text{any} \\
&\quad \wedge \text{maxBallot}[a] \leq m.\text{ballot} \\
&\quad \wedge \text{maxValue}[a] = \text{none} \vee \text{maxValue}[a] = v \\
&\quad \wedge \text{maxBallot}' = [\text{maxBallot} \text{ EXCEPT } ![a] = m.\text{ballot}] \\
&\quad \wedge \text{maxVBallot}' = [\text{maxVBallot} \text{ EXCEPT } ![a] = m.\text{ballot}] \\
&\quad \wedge \text{maxValue}' = [\text{maxValue} \text{ EXCEPT } ![a] = v] \\
&\quad \wedge \forall n \in \text{p2bMessages} : \neg(n.\text{ballot} = m.\text{ballot} \wedge n.\text{acceptor} = a) \\
&\quad \wedge \text{SendMessage}([\text{type} \mapsto \text{“P2b”}, \\
&\quad \quad \quad \text{ballot} \mapsto m.\text{ballot}, \\
&\quad \quad \quad \text{acceptor} \mapsto a, \\
&\quad \quad \quad \text{value} \mapsto v])
\end{aligned}$$

A value is chosen if a fast quorum of acceptors proposed that value in a fast round.

Because the quorum size of a fast round and classic round is different, we assume that the acceptor distinguishes a fast round and classic round based on the *P2a* message it receives. If the *P2a* message contains the special value “any”, it is a fast round. Else it is a classic round.

$$\begin{aligned}
\text{FastDecide} &\triangleq \\
&\wedge \text{UNCHANGED } \langle \text{messages}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, \text{cValue} \rangle \\
&\wedge \exists b \in \text{FastBallots}, q \in \text{FastQuorums} : \\
&\quad \text{LET } M \triangleq \{m \in \text{p2bMessages} : m.\text{ballot} = b \wedge m.\text{acceptor} \in q\} \\
&\quad \quad V \triangleq \{w \in \text{Values} : \exists m \in M : w = m.\text{value}\} \\
&\quad \text{IN } \wedge \forall a \in q : \exists m \in M : m.\text{acceptor} = a \\
&\quad \wedge 1 = \text{Cardinality}(V) \\
&\quad \wedge \exists m \in M : \text{decision}' = m.\text{value}
\end{aligned}$$

Phase 2a (Classic)

If more than one value has been proposed, the collision is resolved using the following rules:

1. If the proposals contain different values, a value must be selected if the majority of acceptors in the fast quorum have casted a vote for that value.
2. Otherwise, the coordinator is free to select any value.

$$\begin{aligned}
\text{ClassicAccept} &\triangleq \\
&\wedge \text{UNCHANGED } \langle \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue} \rangle \\
&\wedge \exists b \in \text{ClassicBallots}, f \in \text{FastBallots}, q \in \text{FastQuorums}, v \in \text{Values} : \\
&\quad \wedge f < b \text{ There was a fast round before this classic round.} \\
&\quad \wedge \text{cValue} = \text{none} \vee \text{cValue} = v \\
&\quad \wedge \text{cValue}' = v \\
&\quad \wedge \forall m \in \text{p2aMessages} : m.\text{ballot} \neq b \\
&\quad \wedge \text{LET } M \triangleq \{m \in \text{p2bMessages} : m.\text{ballot} = f \wedge m.\text{acceptor} \in q\}
\end{aligned}$$

$$\begin{aligned}
& V \triangleq \{w \in \text{Values} : \exists m \in M : w = m.\text{value}\} \\
\text{IN } & \wedge \forall a \in q : \exists m \in M : m.\text{acceptor} = a \\
& \wedge 1 < \text{Cardinality}(V) \text{ Collision occurred.} \\
& \wedge \text{IF } \exists w \in V : \text{IsMajorityValue}(M, w) \\
& \quad \text{THEN } \text{IsMajorityValue}(M, v) \text{ Choose majority in quorum.} \\
& \quad \text{ELSE } v \in V \text{ Choose any.} \\
& \wedge \text{SendMessage}([type \mapsto \text{"P2a"}, \\
& \quad \quad \quad ballot \mapsto b, \\
& \quad \quad \quad value \mapsto v])
\end{aligned}$$

Phase 2b (Classic)

Same as in *Paxos*.

$$\begin{aligned}
\text{ClassicAccepted} & \triangleq \\
& \wedge \text{UNCHANGED } \langle cValue \rangle \\
& \wedge \text{PaxosAccepted}
\end{aligned}$$

Same as in *Paxos*.

$$\begin{aligned}
\text{ClassicDecide} & \triangleq \\
& \wedge \text{UNCHANGED } \langle \text{messages}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, cValue \rangle \\
& \wedge \exists b \in \text{ClassicBallots}, q \in \text{Quorums} : \\
& \quad \text{LET } M \triangleq \{m \in p2bMessages : m.\text{ballot} = b \wedge m.\text{acceptor} \in q\} \\
& \quad \text{IN } \wedge \forall a \in q : \exists m \in M : m.\text{acceptor} = a \\
& \quad \wedge \exists m \in M : \text{decision}' = m.\text{value}
\end{aligned}$$

$$\begin{aligned}
\text{FastTypeOK} & \triangleq \wedge \text{PaxosTypeOK} \\
& \wedge cValue \in \text{Values} \cup \{none\}
\end{aligned}$$

$$\begin{aligned}
\text{FastInit} & \triangleq \wedge \text{PaxosInit} \\
& \wedge cValue = none
\end{aligned}$$

$$\begin{aligned}
\text{FastNext} & \triangleq \vee \text{FastAny} \\
& \vee \text{FastPropose} \\
& \vee \text{FastDecide} \\
& \vee \text{ClassicAccept} \\
& \vee \text{ClassicAccepted} \\
& \vee \text{ClassicDecide}
\end{aligned}$$

$$\begin{aligned}
\text{FastSpec} & \triangleq \wedge \text{FastInit} \\
& \wedge \Box[\text{FastNext}]_{\langle \text{messages}, \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, cValue \rangle} \\
& \wedge \text{SF}_{\langle \text{messages}, \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, cValue \rangle}(\text{FastDecide}) \\
& \wedge \text{SF}_{\langle \text{messages}, \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, cValue \rangle}(\text{ClassicDecide})
\end{aligned}$$

Only proposed values can be learnt.

$$\begin{aligned}
\text{FastNontriviality} & \triangleq \vee \text{decision} = none \\
& \vee \exists m \in p2bMessages : m.\text{value} = \text{decision} \wedge m.\text{ballot} \in \text{FastBallots}
\end{aligned}$$

$$\text{FastSafetyProperty} \triangleq \wedge \Box[\text{FastNontriviality}]_{\langle \text{messages}, \text{decision}, \text{maxBallot}, \text{maxVBallot}, \text{maxValue}, cValue \rangle}$$

$$\wedge \square [PaxosConsistency]_{\langle messages, decision, maxBallot, maxVBallot, maxValue, cValue \rangle}$$

$$FastSymmetry \triangleq PaxosSymmetry$$

THEOREM $FastSpec \Rightarrow PaxosSpec$
