$\overline{\qquad\qquad\qquad\qquad\qquad \text{MODULE } FastPaxos \qquad\qquad\qquad\qquad\qquad}$

EXTENDS $TLC,\ Naturals,\ FiniteSets,\ Integers$

$MaxValue(A) \;\triangleq\; \text{CHOOSE } a \in A : \forall\, b \in A : b \le a$

CONSTANT $Values$ Set of all the values.
CONSTANT $Replicas$ Set of all replicas.
CONSTANT $FastRoundNumber$ Set of Fast Rounds.

As there is only one coordinator thereofore, Explicitly specify the name of the coordinator. We are here also considering that the only coordinator is also the leader.

CONSTANT $Coordinator$

$RoundNumber \;\triangleq\; Nat \setminus \{0\}$ set of positive round numbers

ASSUME $IsFiniteSet(Replicas)$ Set of $Replicas$ should be a Finite set.
ASSUME $Coordinator \in Replicas$ Assumption related to coordinator that it should be a member of $Replicas$ set.
ASSUME $FastRoundNumber \subseteq RoundNumber$

It is a set of all subsets of replicas which contains count of members which is more than half of the size of set $Replicas$
$FastPaxosQuorums \;\triangleq\; \{q \in \text{SUBSET } Replicas : (Cardinality(Replicas) \div 2) < Cardinality(q)\}$
$QuorumAssume \;\triangleq\; \wedge \forall\, q \in FastPaxosQuorums : q \subseteq Replicas$
$\qquad\qquad\qquad\qquad \wedge \forall\, q,\, r \in FastPaxosQuorums : q \cap r \ne \{\}$
ASSUME $QuorumAssume$

All round numbers which are not fast rounds will be classic rounds
$ClassicRoundRoundNumber \;\triangleq\; RoundNumber \setminus FastRoundNumber$

Definition of any value and none values.
$AnyValue \;\triangleq\; \text{CHOOSE } val : val \notin Values$
$NoneValue \;\triangleq\; \text{CHOOSE } nval : nval \notin (Values \cup \{AnyValue\})$

$P1aMessage \;\triangleq\; [type : \{\text{``P1a''}\},$
$\qquad\qquad\qquad round : RoundNumber]$ round is in set round.

$P1bMessage \;\triangleq\; [type : \{\text{``P1b''}\},$
$\qquad\qquad\qquad round : RoundNumber,$ round is in set round.
$\qquad\qquad\qquad valueRound : RoundNumber \cup \{0\},$ round in which value is chosen
$\qquad\qquad\qquad acceptor : Replicas,$ Acceptor is in set $Replicas$.
$\qquad\qquad\qquad value : Values \cup \{AnyValue\}]$

$P2aMessage \;\triangleq\; [type\ \ : \{\text{``P2a''}\},$
$\qquad\qquad\qquad round : RoundNumber,$ round value is in set round.
$\qquad\qquad\qquad value\ \ : Values]$ Value is in set $Values$.

$P2bMessage \;\triangleq\; [type : \{\text{``P2b''}\},$
$\qquad\qquad\qquad round : RoundNumber,$ round is in set round.
$\qquad\qquad\qquad acceptor : Replicas,$ Acceptor is in set $Replicas$.

1

$$value : Values]$$ Value is in set *Values*.

$$P3Message \triangleq [type : \{\text{``P3''}\},$$
$$round : RoundNumber,$$ round value is in set round.
$$value : Values]$$ Value is in set *Values*.

Message is the union of $P1aMessage$, $P1bMessage$, $P2aMessage$, $P2bMessage$ and $P3Message$.
$$Message \triangleq P1aMessage \cup P1bMessage \cup P2aMessage \cup P2bMessage \cup P3Message$$

round of participation for an acceptor. 0 means has not participated in any round
VARIABLE *rounds*

Highest numbered round in which an acceptor has casted a vote. Initially 0. $valueRound \leq round$, as acceptor can participate in rounds after casting vote.
VARIABLE *valueRounds*

Value for which an acceptor casted a vote.
VARIABLE *values*

Highest numbered round a coordinator has begun.
VARIABLE *coordinatorRound*

This value is either none, if coordinator has not picked any value, or is equal to the value picked by the coordinator in round *coordinatorRound*.
VARIABLE *coordinatorValue*
VARIABLE *messages*
VARIABLE *proposedValue*
VARIABLE *learnedValue*
VARIABLE *goodSet*

grouping all the variables together.
group of variables related to acceptor.
$$AcceptorVariables \triangleq \langle rounds, valueRounds, values \rangle$$

group of variables related to coordinator.
$$CoordinatorVariables \triangleq \langle coordinatorRound, coordinatorValue \rangle$$

group of all other variables
$$OtherVariables \triangleq \langle proposedValue, learnedValue, goodSet \rangle$$

group containing all variables.
$$AllVarialbes \triangleq \langle AcceptorVariables, CoordinatorVariables, OtherVariables, messages \rangle$$

Invariant for all the variables declared.
$$FastPaxosTypeOK \triangleq \wedge rounds \in [Replicas \to Nat]$$
$$\wedge valueRounds \in [Replicas \to Nat]$$
$$\wedge values \in [Replicas \to Val \cup \{AnyValue\}]$$
$$\wedge coordinatorRound \in Nat$$

2

$$\wedge\ coordinatorValue\ \in\ Values \cup \{AnyValue,\ NoneValue\}$$
$$\wedge\ messages \in \text{SUBSET}\ Message$$
$$\wedge\ proposedValue \in \text{SUBSET}\ \ Values$$
$$\wedge\ learnedValue \in \text{SUBSET}\ \ Values$$
$$\wedge\ goodSet \subseteq Replicas$$

$FastPaxosInit\ \triangleq\ \wedge\ rounds = [Replicas \mapsto 0]$
$\qquad\qquad\qquad \wedge\ valueRounds = [Replicas \mapsto 0]$
$\qquad\qquad\qquad \wedge\ values\ = [Replicas \mapsto AnyValue]$
$\qquad\qquad\qquad \wedge\ rounds = [Replicas \mapsto 0]$
$\qquad\qquad\qquad \wedge\ coordinatorRound = 0$
$\qquad\qquad\qquad \wedge\ coordinatorValue\ = NoneValue$
$\qquad\qquad\qquad \wedge\ messages = \{\}$
$\qquad\qquad\qquad \wedge\ proposedValue = \{\}$
$\qquad\qquad\qquad \wedge\ learnedValue = \{\}$
$\qquad\qquad\qquad \wedge\ goodSet\qquad \in \text{SUBSET}\ Replicas$

$SendMessage(m)\ \triangleq\ messages' = messages \cup \{m\}$

Implementing Phase $1a$ for round i
$FastPaxosPrepare(i)\ \triangleq\ \wedge\ coordinatorRound < i \qquad\qquad$ coordinator's round number is less than the current rou
$\qquad\qquad\qquad\quad \wedge\ \vee\ coordinatorRound = 0 \qquad\quad$ if coordinator has not participated in any of the rounds
$\qquad\qquad\qquad\qquad \vee \exists\, msg \in messages : \wedge\ coordinatorRound < msg.round$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \wedge\ msg.round < i$
$\qquad\qquad\qquad\qquad \vee\ \wedge\ coordinatorRound \in FastRoundNumber \qquad$ coordinator previouslt particip
$\qquad\qquad\qquad\qquad\qquad \wedge\ i \in ClassicRoundRoundNumber \qquad\qquad$ but the current round is a class
$\qquad\qquad\qquad\quad \wedge\ coordinatorRound' = i$
$\qquad\qquad\qquad\quad \wedge\ coordinatorValue = NoneValue$
$\qquad\qquad\qquad\quad \wedge\ SendMessage([type \mapsto \text{``P1a''},\ round \mapsto i])$
$\qquad\qquad\qquad\quad \wedge\ \text{UNCHANGED}\ \langle AcceptorVariables,\ OtherVariables \rangle$

returns the set of all the messages for a particular phase and round and from acceptors of a particular quorum
$FilterMessagesForQuorumRoundAndPhase(quorum,\ round,\ phase)\ \triangleq\ \{m \in messages : (m.type = phase)$

$msgs$ are $p1b$ messages sent in the round by all the acceptors of quorum.
$IsValueInQuorum(quorum,\ round,\ msgs,\ val)\ \triangleq\ \text{LET}\ AcceptorRound(a)\ \triangleq\ (\text{CHOOSE}\ msg \in msgs : msg.$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad AcceptorValue(a)\ \triangleq\ (\text{CHOOSE}\ msg \in msgs : msg.$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad HighestRound\ \triangleq\ MaxValue(\{AcceptorRound(accep$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad HighestRoundValue\ \triangleq\ \{AcceptorValue(acceptor) :$

3