MODULE *AbstractBallotingWithPrepare*

This is a specification of *SCP*'s balloting protocol. We work at a high level of abstraction where we do not expliticely model messages. Instead, we track what statements are voted/accepted prepared and committed by each node. What we do model explicitely is how each node n votes and accepts statements based on its current ballot $ballot[n]$ and its highest confirmed-prepared ballot $h[n]$.

We also do not model *Byzantine* behavior explicitly. Instead, whenever a node checks that a set (a quorum or a blocking set) voted or accepted a statement, it only checks that the non-Byzantine members of the set did so. This soundly models what could happen under *Byzantine* behavior because *Byzantine* nodes, being unconstrained, could have voted or accepted whatever is needed to make the check pass.

We provide an inductive invariant that implies the agreement property, and we check its inductiveness exhaustively for small instances of the domain model.

An informal specification of *SCP* can be found at: https://datatracker.ietf.org/doc/html/draft-mazieres-dinrg-scp-05#section-3.5

EXTENDS *DomainModel*

VARIABLES
  $ballot$
, h
, $voteToPrepare$
, $acceptedPrepared$
, $voteToCommit$
, $acceptedCommitted$
, $externalized$
, byz the set of malicious nodes

$TypeOK \triangleq$
  $\land\ ballot \in [N \rightarrow BallotOrNull]$
  $\land\ h \in [N \rightarrow BallotOrNull]$
  $\land\ voteToPrepare \in [N \rightarrow \text{SUBSET } Ballot]$
  $\land\ acceptedPrepared \in [N \rightarrow \text{SUBSET } Ballot]$
  $\land\ voteToCommit \in [N \rightarrow \text{SUBSET } Ballot]$
  $\land\ acceptedCommitted \in [N \rightarrow \text{SUBSET } Ballot]$
  $\land\ externalized \in [N \rightarrow \text{SUBSET } Ballot]$
  $\land\ byz \in \text{SUBSET } N$

$Init \triangleq$
  $\land\ ballot = [n \in N \mapsto nullBallot]$ current ballot of each node
  $\land\ h = [n \in N \mapsto nullBallot]$ current highest confirmed-prepared ballot of each node
  $\land\ voteToPrepare = [n \in N \mapsto \{\}]$
  $\land\ acceptedPrepared = [n \in N \mapsto \{\}]$
  $\land\ voteToCommit = [n \in N \mapsto \{\}]$
  $\land\ acceptedCommitted = [n \in N \mapsto \{\}]$
  $\land\ externalized = [n \in N \mapsto \{\}]$
  $\land\ byz \in FailProneSet$ byz is initially set to an arbitrary fail-prone set

Node n enters a new ballot and votes to prepare it. Note that n votes to prepare its new ballot $ballot'[n]$ regardless of whether it has previously voted to commit an incompatible ballot b. The main subtlety of the protocol is that this is okay because:

1) We must have $b \prec h[n]$ because, when n votes to commit b (see *VoteToCommit*), it sets $h[n] = b$ if $h[n] \prec b$, and subsequently $h[n]$ can only grow, and

2) therefore, if $h[n].value \neq b.value$, then n confirmed $h[n]$ as prepared (by definition of how $h[n]$ is updated) and thus we know that, even though n voted to commit b, b can never gather a quorum of votes to commit.

Note how this reasoning appears in the inductive invariant below.

$$
\begin{array}{l}
IncreaseBallotCounter(n, c) \triangleq \\
\quad \land\ c > 0 \\
\quad \land\ c > ballot[n].counter \\
\quad \land\ h[n].counter \leq c \\
\quad \land\ \text{IF } h[n] \neq nullBallot \\
\qquad \text{THEN } ballot' = [ballot \text{ EXCEPT } ![n] = bal(c, h[n].value)] \\
\qquad \text{ELSE } \exists v \in V : ballot' = [ballot \text{ EXCEPT } ![n] = bal(c, v)] \\
\quad \land\ voteToPrepare' = [voteToPrepare \text{ EXCEPT } ![n] = @ \cup \{ballot[n]'\}] \\
\quad \land\ \text{UNCHANGED } \langle h, acceptedPrepared, voteToCommit, acceptedCommitted, externalized, byz \rangle
\end{array}
$$

Next we describe when a node accepts and confirms ballots prepared. Nothing surprising here.

Note that we could check that nothing less-and-incompatible is accepted committed. That would simplify the agreement proof but complicate the liveness proof. In any case, it is an invariant that nothing less-and-incompatible is accepted committed at this point (see *AcceptNeverContradictory*).

$$
\begin{array}{l}
AcceptPrepared(n, b) \triangleq \\
\quad \land\ \lor \exists Q \in Quorum : \forall n2 \in Q \setminus byz : b \in voteToPrepare[n2] \cup acceptedPrepared[n2] \\
\qquad \lor \exists Bl \in BlockingSet : \forall n2 \in Bl \setminus byz : b \in acceptedPrepared[n2] \\
\quad \land\ acceptedPrepared' = [acceptedPrepared \text{ EXCEPT } ![n] = @ \cup \{b\}] \\
\quad \land\ \text{UNCHANGED } \langle ballot, h, voteToPrepare, voteToCommit, acceptedCommitted, externalized, byz \rangle
\end{array}
$$

$$
\begin{array}{l}
ConfirmPrepared(n, b) \triangleq \\
\quad \land\ b.counter > -1 \\
\quad \land\ h[n] \prec b \\
\quad \land\ \exists Q \in Quorum : \forall n2 \in Q \setminus byz : b \in acceptedPrepared[n2] \\
\quad \land\ h' = [h \text{ EXCEPT } ![n] = b] \\
\quad \land\ \text{UNCHANGED } \langle ballot, voteToPrepare, acceptedPrepared, voteToCommit, acceptedCommitted, externalize
\end{array}
$$

When a node votes to commit a ballot, it must check that it has not already voted or accepted to abort it. This is crucial to avoid externalizing two different values in two different ballots. We also update $h[n]$ if needed to reflect the new highest-confirmed prepared ballot.

$$
\begin{array}{l}
VoteToCommit(n, b) \triangleq \\
\quad \land\ b.counter > 0 \\
\quad \land\ b = ballot[n] \\
\quad \land\ \forall b2 \in Ballot : LessThanAndIncompatible(b, b2) \Rightarrow \\
\qquad\quad b2 \notin voteToPrepare[n] \cup acceptedPrepared[n]
\end{array}
$$

$$
\begin{array}{l}
\quad \land\ b \prec h[n] \Rightarrow b.value \quad = h[n].value \\
\quad \land\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in acceptedPrepared[n2] \\
\quad \land\ voteToCommit' = [voteToCommit\ \text{EXCEPT}\ ![n] = @ \cup \{b\}] \\
\quad \land\ \text{IF}\ h[n] \quad \preceq b \\
\qquad\ \ \text{THEN}\ h' = [h\ \text{EXCEPT}\ ![n] = b] \\
\qquad\ \ \text{ELSE}\ \ \text{UNCHANGED}\ h \\
\quad \land\ \text{UNCHANGED}\ \langle ballot,\ voteToPrepare,\ acceptedPrepared,\ acceptedCommitted,\ externalized,\ byz \rangle
\end{array}
$$

Next we describe when a node accepts and confirms ballots committed. Nothing surprising here.

$$
\begin{array}{l}
AcceptCommitted(n,\ b)\ \triangleq \\
\quad \land\ b = ballot[n] \\
\quad \land\ \lor\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in voteToCommit[n2] \\
\qquad\ \lor\ \exists\, Bl \in BlockingSet : \forall\, n2 \in Bl \setminus byz : b \in acceptedCommitted[n2] \\
\quad \land\ acceptedCommitted' = [acceptedCommitted\ \text{EXCEPT}\ ![n] = @ \cup \{b\}] \\
\quad \land\ \text{UNCHANGED}\ \langle ballot,\ h,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ externalized,\ byz \rangle
\end{array}
$$

$$
\begin{array}{l}
Externalize(n,\ b)\ \triangleq \\
\quad \land\ b = ballot[n] \\
\quad \land\ \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b \in acceptedCommitted[n2] \\
\quad \land\ externalized' = [externalized\ \text{EXCEPT}\ ![n] = @ \cup \{b\}] \\
\quad \land\ \text{UNCHANGED}\ \langle ballot,\ h,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ acceptedCommitted,\ byz \rangle
\end{array}
$$

Finally we put everything together:

$$
\begin{array}{l}
Next\ \triangleq \\
\quad \lor\ \exists\, n \in N \setminus byz,\ c \in BallotNumber,\ v \in V : \\
\qquad \text{LET}\ b\ \triangleq\ bal(c,\ v)\ \text{IN} \\
\qquad\qquad \lor\ IncreaseBallotCounter(n,\ c) \\
\qquad\qquad \lor\ AcceptPrepared(n,\ b) \\
\qquad\qquad \lor\ ConfirmPrepared(n,\ b) \\
\qquad\qquad \lor\ VoteToCommit(n,\ b) \\
\qquad\qquad \lor\ AcceptCommitted(n,\ b) \\
\qquad\qquad \lor\ Externalize(n,\ b)
\end{array}
$$

$$
vars\ \triangleq\ \langle ballot,\ h,\ voteToPrepare,\ acceptedPrepared,\ voteToCommit,\ acceptedCommitted,\ externalized,\ byz \rangle
$$

$$
Spec\ \triangleq\ Init \land \Box[Next]_{vars}
$$

$$
\begin{array}{l}
Agreement\ \triangleq \\
\quad \forall\, n1,\ n2 \in N \setminus byz : \forall\, b1,\ b2 \in Ballot : \\
\qquad b1 \in externalized[n1] \land b2 \in externalized[n2] \Rightarrow b1.value = b2.value
\end{array}
$$

Here is an inductive invariant that implies agreement:

$InductiveInvariant\ \triangleq$

First, the boring stuff:

$\quad \land\ TypeOK$

$\land \; byz \in \mathit{FailProneSet}$

$\land \; \forall\, n \in N \setminus byz,\ c1,\ c2 \in \mathit{BallotNumber},\ v1,\ v2 \in V :$

$\quad \text{LET } b1 \triangleq bal(c1, v1) b2 \triangleq bal(c2, v2) \text{IN}$

$\quad \land \; ballot[n].counter > -1 \Rightarrow ballot[n].counter > 0$

$\quad \land \; b1 \in voteToPrepare[n] \lor b1 \in voteToCommit[n] \Rightarrow b1.counter > 0 \land b1.counter \leq ballot[n].counte$

$\quad \land \; b1 \in acceptedPrepared[n] \Rightarrow \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b1 \in voteToPrepare[n2]$

$\quad \land \; b1 \in acceptedCommitted[n] \Rightarrow \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b1 \in voteToCommit[n2]$

$\quad \land \; h[n].counter > 0 \Rightarrow \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : h[n] \in acceptedPrepared[n2]$

$\quad \land \; b1 \in externalized[n] \Rightarrow \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b1 \in acceptedCommitted[n2]$

$\quad \land \; b1 \in voteToPrepare[n] \lor b1 \in voteToCommit[n] \Rightarrow$

$\qquad \land \; b1.counter \leq ballot[n].counter$

$\qquad \land \; b1.counter = ballot[n].counter \Rightarrow b1.value = ballot[n].value$

$\quad \land \; bal(c1, v1) \in voteToPrepare[n] \land bal(c1, v2) \in voteToPrepare[n] \Rightarrow v1 = v2$

$\quad \land \; bal(c1, v1) \in voteToCommit[n] \land bal(c1, v2) \in voteToCommit[n] \Rightarrow v1 = v2$

$\quad \land \; b1 \in voteToCommit[n] \Rightarrow$

$\qquad\quad \land \; \exists\, Q \in Quorum : \forall\, n2 \in Q \setminus byz : b1 \in acceptedPrepared[n2]$

$\qquad\quad \land \; b1 \preceq h[n]$ note this is important

Next, the crux of the matter:

(in short, a node overrides "commit v" only if it is sure that "commit v" cannot reach quorum threshold)

$\quad \land \; \land \; b1 \in voteToCommit[n]$

$\qquad \land \; LessThanAndIncompatible(b1, b2)$

$\qquad \land \; b2 \in voteToPrepare[n]$

$\qquad \Rightarrow \forall\, Q \in Quorum : \exists\, n2 \in Q \setminus byz :$

$\qquad\qquad b1 \notin voteToCommit[n2] \land ballot[n2].counter > b1.counter$

Finally, our goal:

$\land \; Agreement$

An additional property implies by the inductive invariant:

$AcceptNeverContradictory \triangleq \forall\, b1,\ b2 \in Ballot,\ n1,\ n2 \in N \setminus byz :$

$\quad \land \; b1 \in acceptedCommitted[n1]$

$\quad \land \; b2 \in acceptedPrepared[n2]$

$\quad \land \; b1 \prec b2$

$\quad \Rightarrow b1.value = b2.value$