MODULE $ACP\_NB\_WRONG\_TLC$

Erroneous Non blocking Atomic *Committment* Protocol (ACP-NB)
The mistake is to deliver a broacast message locally *before* it has been
forwarded to other participants.
This protocol does not satisfy the consistency property $AC1$

EXTENDS ACP_SB

Participants type is extended with a "forward" variable.
Coordinator type is unchanged.

$$
\begin{array}{l}
TypeInvParticipantNB \triangleq participant \in [\\
\quad participants \to [\\
\quad\quad vote : \{yes, no\},\\
\quad\quad alive : \text{BOOLEAN},\\
\quad\quad decision : \{undecided, commit, abort\},\\
\quad\quad faulty : \text{BOOLEAN},\\
\quad\quad voteSent : \text{BOOLEAN},\\
\quad\quad forward : [participants \to \{notsent, commit, abort\}]\\
\quad]\\
]
\end{array}
$$

$$TypeInvNB \triangleq TypeInvParticipantNB \land TypeInvCoordinator$$

Initially, participants have not forwarded anything yet

$$
\begin{array}{l}
InitParticipantNB \triangleq participant \in [\\
\quad participants \to [\\
\quad\quad vote : \{yes, no\},\\
\quad\quad alive : \{\text{TRUE}\},\\
\quad\quad decision : \{undecided\},\\
\quad\quad faulty : \{\text{FALSE}\},\\
\quad\quad voteSent : \{\text{FALSE}\},\\
\quad\quad forward : [participants \to \{notsent\}]\\
\quad]\\
]
\end{array}
$$

$$InitNB \triangleq InitParticipantNB \land InitCoordinator$$

Participant statements that realize a better broadcast

$forward(i, j)$: forwarding of the predecision from participant i to participant j
IF
particpant i is alive
participant i has received a decision and has decided (it shouldn't have decided yet)
participant i has not yet forwarded this decision to participant j
THEN
participant i forwards the decision to participant j

$$
\begin{array}{l}
forward(i, j) \triangleq \land\ i \neq j\\
\quad \land\ participant[i].alive\\
\quad \land\ participant[i].decision \neq notsent\\
\quad \land\ participant[i].forward[j] = notsent\\
\quad \land\ participant' = [participant \text{ EXCEPT } ![i] =\\
\quad\quad [@ \text{ EXCEPT } !.forward =\\
\quad\quad\quad [@ \text{ EXCEPT } ![j] = participant[i].decision]\\
\quad\quad]\\
\quad]
\end{array}
$$

$\wedge$ UNCHANGED $\langle coordinator \rangle$

decideOnForward(i, j): participant i receives decision from participant j
IF
participant i is alive
participant i has yet to receive a decision
participant j has forwarded its decision to participant i
THEN
participant i decides in accordance with participant j's decision (it should only predecide)

$$
\begin{aligned}
decideOnForward(i, j) \triangleq\ & \wedge i \neq j \\
& \wedge participant[i].alive \\
& \wedge participant[i].decision = undecided \\
& \wedge participant[j].forward[i] \neq notsent \\
& \wedge participant' = [participant \text{ EXCEPT } ![i] = \\
& \qquad [@ \text{ EXCEPT } !.decision = participant[j].forward[i]] \\
& \quad] \\
& \wedge \text{UNCHANGED } \langle coordinator \rangle
\end{aligned}
$$

abortOnTimeout(i): conditions for a timeout are simulated
IF
participant is alive and undecided and coordinator is not alive
coordinator died before sending decision to all participants who are alive
all dead participants died before forwarding decision to a participant who is alive
THEN
decide abort

$$
\begin{aligned}
abortOnTimeout(i) \triangleq\ & \wedge participant[i].alive \\
& \wedge participant[i].decision = undecided \\
& \wedge \neg coordinator.alive \\
& \wedge \forall j \in participants : participant[j].alive \Rightarrow coordinator.broadcast[j] = notsent \\
& \wedge \forall j, k \in participants : \neg participant[j].alive \wedge participant[k].alive \Rightarrow participant[j].forward[k] = notsent \\
& \wedge participant' = [participant \text{ EXCEPT } ![i] = [@ \text{ EXCEPT } !.decision = abort]] \\
& \wedge \text{UNCHANGED } \langle coordinator \rangle
\end{aligned}
$$

FOR N PARTICIPANTS

$$
\begin{aligned}
parProgNB(i, j) \triangleq\ & \vee parProg(i) \\
& \vee forward(i, j) \\
& \vee decideOnForward(i, j) \\
& \vee abortOnTimeout(i)
\end{aligned}
$$

$$parProgNNB \triangleq \exists i, j \in participants : parDie(i) \vee parProgNB(i, j)$$

$$progNNB \triangleq parProgNNB \vee coordProgN$$

$$
\begin{aligned}
fairnessNB \triangleq\ & \wedge \forall i \in participants : \mathrm{WF}_{\langle coordinator, participant \rangle}(\exists j \in participants : parProgNB(i, j)) \\
& \wedge \mathrm{WF}_{\langle coordinator, participant \rangle}(coordProgB)
\end{aligned}
$$

$$SpecNB \triangleq InitNB \wedge \Box[progNNB]_{\langle coordinator, participant \rangle} \wedge fairnessNB$$
