Non blocking Atomic Commitment Protocol (ACP-NB)

The non blocking property AC5 is obtained by using a reliable broadcast implemented as follows:
- upon reception of a broadcast message, this message is forwarded to all participants before it’s delivered to the local site;
- since participant \(i\) does not forward to itself, \(\text{forward}[i]\) is used to store the decision before it’s delivered (and becomes “decision”)

EXTENDS ACP SB

Participants type is extended with a “forward” variable.
Coordinator type is unchanged.

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

\[
\text{TypeInvNB} \triangleq \text{TypeInvParticipantNB} \land \text{TypeInvCoordinator}
\]

Initially, participants have not forwarded anything yet

\[
\text{InitParticipantNB} \triangleq \text{participant} \in \left[ \begin{array}{l}
\text{participants} \rightarrow \left[ \\
\text{vote} : \{\text{yes, no}\}, \\
\text{alive} : \{\text{true}\}, \\
\text{decision} : \{\text{undecided}\}, \\
\text{faulty} : \{\text{false}\}, \\
\text{voteSent} : \{\text{false}\}, \\
\text{forward} : \left[ \text{participants} \rightarrow \{\text{notsent}\} \right]
\end{array} \right]
\right]
\]

\[
\text{InitNB} \triangleq \text{InitParticipantNB} \land \text{InitCoordinator}
\]

Participant statements that realize a better broadcast

\[
\text{forward}(i, j) : \text{forwarding of the predecision from participant } i \text{ to participant } j
\]

\[
\text{if}
\text{ participant } i \text{ is alive}
\text{ participant } i \text{ has received a decision (stored in } \text{forward}[i])
\text{ participant } i \text{ has not yet forwarded this decision to participant } j
\text{ then}
\text{ participant } i \text{ forwards the decision to participant } j
\]

\[
\text{forward}(i, j) \triangleq \land i \neq j
\land \text{participant}[i].\text{alive}
\land \text{participant}[i].\text{forward}[i] \neq \text{notsent}
\land \text{participant}[i].\text{forward}[j] = \text{notsent}
\land \text{participant}' = \left[ \text{participant} \text{ EXCEPT } ![i] \right]
\]
\[ \text{preDecideOnForward}(i, j): \text{participant } i \text{ receives decision from participant } j \]

\[
\text{IF} \quad \begin{align*}
\text{participant } i \text{ is alive} \\
\text{participant } i \text{ has yet to receive a decision} \\
\text{participant } j \text{ has forwarded its decision to participant } i
\end{align*}
\text{THEN} \quad \text{participant } i \text{ (pre)decides in accordance with participant } j \text{'s decision}
\]

\[ \text{preDecideOnForward}(i, j) \triangleq \begin{align*}
&\land \ i \neq j \\
&\land \ \text{participant}[i].\text{alive} \\
&\land \ \text{participant}[i].\text{forward}[i] = \text{notsent} \\
&\land \ \text{participant}[j].\text{forward}[i] \neq \text{notsent} \\
&\land \ \text{participant}' = [\text{participant} \ \text{EXCEPT} \ ![i] = \\
&\quad [\text{EXCEPT} \ ![i] = \text{participant}[j].\text{forward}[i]] \\
&\quad ] \\
&\land \ \text{UNCHANGED } \langle \text{coordinator} \rangle
\]

\[ \text{preDecide}(i): \text{participant } i \text{ receives decision from coordinator} \]

\[
\text{IF} \quad \begin{align*}
\text{participant } i \text{ is alive} \\
\text{participant } i \text{ has yet to receive a decision} \\
\text{coordinator has sent its decision to participant } i
\end{align*}
\text{THEN} \quad \text{participant } i \text{ (pre)decides in accordance with coordinator's decision}
\]

\[ \text{preDecide}(i) \triangleq \begin{align*}
&\land \ \text{participant}[i].\text{alive} \\
&\land \ \text{participant}[i].\text{forward}[i] = \text{notsent} \\
&\land \ \text{coordinator}.\text{broadcast}[i] \neq \text{notsent} \\
&\land \ \text{participant}' = [\text{participant} \ \text{EXCEPT} \ ![i] = \\
&\quad [\text{EXCEPT} \ ![i] = \text{coordinator}.\text{broadcast}[i]] \\
&\quad ] \\
&\land \ \text{UNCHANGED } \langle \text{coordinator} \rangle
\]

\[ \text{decideNB}(i): \text{Actual decision, after predecision has been forwarded} \]

\[
\text{IF} \quad \begin{align*}
\text{participant } i \text{ is alive} \\
\text{participant } i \text{ has forwarded its (pre)decision to all other participants}
\end{align*}
\text{THEN} \quad \text{participant } i \text{ decides in accordance with it's predecision}
\]

\[ \text{decideNB}(i) \triangleq \begin{align*}
&\land \ \text{participant}[i].\text{alive} \\
&\land \ \forall j \in \text{participants} : \text{participant}[i].\text{forward}[j] \neq \text{notsent} \\
&\land \ \text{participant}' = [\text{participant} \ \text{EXCEPT} \ ![i] = \\
&\quad [\text{EXCEPT} \ ![i] = \text{participant}[i].\text{forward}[i]] \\
&\quad ] \\
&\land \ \text{UNCHANGED } \langle \text{coordinator} \rangle
\]

\[ \text{abortOnTimeout}(i): \text{conditions for a timeout are simulated} \]

\[
\text{IF} \quad \begin{align*}
\text{participant is alive and undecided and coordinator is not alive}
\end{align*}
\]

\[ 2 \]
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

abortOnTimeout(i) ≡ \∧ participant[i].alive
∧ participant[i].decision = undecided
∧ \¬ coordinator.alive
∧ ∀ j ∈ participants : participant[j].alive ⇒ coordinator.broadcast[j] = notsent
∧ ∀ j, k ∈ participants : \¬ participant[j].alive ∧ participant[k].alive ⇒ participant[j].forward[k] = notsent
∧ participant' = [participant EXCEPT ![i] = [\@ EXCEPT ![decision = abort]]
∧ UNCHANGED ⟨coordinator⟩

FOR N PARTICIPANTS

parProgNB(i, j) ≡ \∨ sendVote(i)
\∨ abortOnVote(i)
\∨ abortOnTimeoutRequest(i)
\∨ forward(i, j)
\∨ preDecideOnForward(i, j)
\∨ abortOnTimeout(i)
\∨ preDecide(i)
\∨ decideTimeout(i)

parProgNNB ≡ \∃ i, j ∈ participants : parDie(i) \lor parProgNB(i, j)

progNNB ≡ parProgNNB \lor coordProgN

fairnessNB ≡ \∧ ∀ i ∈ participants : WF_{(coordinator, participant)}(\exists j ∈ participants : parProgNB(i, j))
∧ WF_{(coordinator, participant)}(coordProgB)

SpecNB ≡ InitNB \land \Box[progNNB]_{(coordinator, participant)} \land fairnessNB

(SOME) INVALID PROPERTIES

AllCommit ≡ \forall i ∈ participants : \Box(participant[i].decision = commit \lor participant[i].faulty)

AllAbort ≡ \forall i ∈ participants : \Box(participant[i].decision = abort \lor participant[i].faulty)

AllCommitYesVotes ≡ \forall i ∈ participants :
\forall j ∈ participants : participant[j].vote = yes
\lor participant[i].decision = commit \lor participant[i].faulty \lor coordinator.faulty