MODULE *skeenAlgorithm*

EXTENDS TLC, $Naturals$, $FiniteSets$, $Sequences$

CONSTANTS $NPROCESS$, $MESSAGES$

VARIABLES pc, $sent$, $pending$, $received$, lc, $messages$

ASSUME $(NPROCESS \in Nat) \land (MESSAGES \neq \{\})$
ASSUME $(NPROCESS \geq 2)$

$vars \triangleq \langle pc, sent, pending, received, lc, messages \rangle$

$Processes \triangleq 1 \,..\, NPROCESS$

$Init \triangleq$
$\land\ messages = [i \in Processes \mapsto MESSAGES]$
$\land\ pending = [i \in Processes \mapsto \{\}]$
$\land\ received = [i \in Processes \mapsto \{\}]$
$\land\ sent = [i \in Processes \mapsto [bc \mapsto \{\},\ ts \mapsto \{\},\ sn \mapsto \{\}]]$
$\land\ pc \in [Processes \to \{\text{“BCAST”},\ \text{“”}\}]$
$\land\ lc\ = [i \in Processes \mapsto 0]$

$Broadcast(message) \triangleq$
$[i \in Processes \mapsto [sent[i]$ EXCEPT $!.bc = sent[i].bc \cup \{message\}]]$

$UpponBCAST(self) \triangleq$
$\land\ (pc[self] = \text{“BCAST”}) \land (messages[self] \neq \{\})$
$\land$ LET $currentMessage \triangleq$ CHOOSE $x \in messages[self] :$ TRUE
IN $\land\ sent' = Broadcast(\langle self,\ currentMessage \rangle)$
$\land\ messages' = [messages$ EXCEPT $![self] = messages[self] \setminus \{currentMessage\}]$
$\land$ UNCHANGED $\langle lc, pending, pc, received \rangle$

$\langle TYPE, SOURCE, DESTINATION, MESSAGE\_BODY, TIMESTAMP \rangle$
$ReceivedMessage(self) \triangleq$
$\land\ \exists\, msg \in sent[self].bc :$
$\land\ msg \notin pending[self]$
$\land\ pending' = [pending$ EXCEPT $![self] = pending[self] \cup \{msg\}]$
$\land\ sent' = [sent$ EXCEPT $![msg[1]].ts = sent[msg[1]].ts \cup \{\langle self,\ msg[2],\ lc[self] \rangle\}]$
$\land$ UNCHANGED $\langle received, pc, messages, lc \rangle$

$MaxTSAllProcess(S) \triangleq$ (CHOOSE $t \in S : \forall\, s \in S : s[3] \leq t[3])[3]$

$SN(message) \triangleq$
$[i \in Processes \mapsto [sent[i]$ EXCEPT $!.sn = sent[i].sn \cup \{message\}]]$

$ReceivedTSFromAll(self) \triangleq$
$\land$ LET $msgs \triangleq \{m1 \in sent[self].ts : \forall\, m2 \in sent[self].ts : m1[2] = m2[2]\}$
IN $\land\ Cardinality(msgs) \quad = NPROCESS$
$\land$ LET $m \triangleq$ CHOOSE $x \in msgs :$ TRUE

$$\begin{array}{ll} \text{IN} & \land\ sent' = SN(\langle self,\ m[2],\ MaxTSAllProcess(msgs)\rangle) \\ & \land\ \text{UNCHANGED}\ \langle received,\ pending,\ lc,\ messages,\ pc\rangle \end{array}$$

$$\begin{array}{l} ReceivedSN(self)\ \triangleq \\ \quad \land \exists\, msg \in sent[self].sn : \\ \qquad \land \langle msg[1],\ msg[2]\rangle \notin received[self] \\ \qquad \land received' = [received\ \text{EXCEPT}\ ![self] = received[self] \cup \{\langle msg[1],\ msg[2]\rangle\}] \\ \qquad \land\ \text{UNCHANGED}\ \langle sent,\ pending,\ lc,\ messages,\ pc\rangle \end{array}$$

FIX RECEIVED

$$\begin{array}{l} Accept(self)\ \triangleq \\ \quad \land\ Cardinality(Processes \times MESSAGES) = Cardinality(received[self]) \\ \quad \land\ pc' = [pc\ \text{EXCEPT}\ ![self] = \text{“AC”}] \\ \quad \land\ \text{UNCHANGED}\ \ \langle sent,\ pending,\ lc,\ messages,\ received\rangle \end{array}$$

$$\begin{array}{l} Steps(self)\ \triangleq \\ \quad \lor\ UpponBCAST(self) \\ \quad \lor\ ReceivedMessage(self) \\ \quad \lor\ ReceivedTSFromAll(self) \\ \quad \lor\ ReceivedSN(self) \\ \quad \lor\ Accept(self) \\ \quad \lor\ \text{UNCHANGED}\ vars \end{array}$$

$$Next\ \triangleq\ (\exists\, self \in Processes : Steps(self))$$

$$Fairness\ \triangleq\ \text{WF}_{vars}(Next)$$

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

$$\begin{array}{l} TypeOK\ \triangleq \\ \quad \land\quad pc \in [Processes \to \{\text{“BCAST”},\ \text{“SN”},\ \text{“AC”},\ \text{“”}\}] \end{array}$$

Properties

$$Agreement\ \triangleq\ \Box((\exists\, self \in Processes : pc[self] = \text{“AC”}) \Rightarrow \Diamond\Box(\forall\, self \in Processes : pc[self] = \text{“AC”}))$$

$$SelectedMessage\ \triangleq\ \text{CHOOSE}\ m \in (Processes \times MESSAGES) : \text{TRUE}$$

$$Validity\ \triangleq\ \Box((\exists\, self \in Processes : SelectedMessage \in sent[self].bc) \Rightarrow \Diamond\Box(\forall\, p \in Processes : SelectedMess$$

$$Integrity\ \triangleq\ \Box((\exists\, self \in Processes : SelectedMessage \in received[self]) \Rightarrow \Diamond\Box(\forall\, self \in Processes : Cardinal$$

$$TotalOrder\ \triangleq$$