MODULE *vinv*

EXTENDS *skeen*

$$Integrity \triangleq \forall\, id \in McastID : \forall\, p \in Proc : \land\, delivered[p][id] \equiv dCntr[p][id] = 1 \land\, \neg delivered[p][id] \equiv dCntr[p][id] = 0$$

$$Validity \triangleq \forall\, p \in Proc : \forall\, id \in McastID : delivered[p][id] \Rightarrow id \in mcastedID$$

If process p is not an addressee of message id, p never issues a local timestamp for id.
The owner of the local timestamp $localTS[p][id]$ must be process p.

$$\begin{aligned} ValidOwnedLocalTS \triangleq\ & \land\, (\forall\, id \in McastID : \forall\, p \in Proc \setminus GroupDest[id] : localTS[p][id] = TimestampNull) \\ & \land\, (\forall\, id \in McastID : \forall\, p \in GroupDest[id] : \\ & \quad (localTS[p][id] \neq TimestampNull \\ & \qquad \Rightarrow (\land\, id \in mcastedID \\ & \qquad\quad \land\, localTS[p][id].g = p))) \end{aligned}$$

If process p is not an addressee of message id, no processes send a proposal for message id to process p.
If process p is not an addressee of message id, it never sends a proposal for message id.
If there exists a proposal for message id, message id must be multicast before.

$$\begin{aligned} ValidInTransitProposeTS \triangleq\ & \land\, (\forall\, id \in McastID : \forall\, rcver \in Proc \setminus GroupDest[id] : \forall\, snder \in Proc : \\ & \quad \forall\, m \in inTransit[snder][rcver] : m.id \neq id) \\ & \land\, (\forall\, id \in McastID : \forall\, snder \in Proc \setminus GroupDest[id] : \forall\, rcver \in Proc : \\ & \quad \forall\, m \in inTransit[snder][rcver] : m.id \neq id) \\ & \land\, (\forall\, id \in McastID : \forall\, rcver \in GroupDest[id] : \forall\, snder \in Proc : \\ & \quad \forall\, m \in inTransit[snder][rcver] : m.id = id \Rightarrow id \in mcastedID) \end{aligned}$$

If process p is not an addressee of message id, it never receives any a proposal for message id.
If process p has received a proposal for message id, message id must be multicast before.

$$\begin{aligned} ValidRcvdProposeTS \triangleq\ & \land\, (\forall\, id \in McastID : \forall\, rcver \in Proc \setminus GroupDest[id] : \forall\, snder \in Proc : \\ & \quad proposeTS[rcver][id] = (\{\} <: \{[type \mapsto Int,\ t \mapsto Int,\ id \mapsto Int,\ source \mapsto Int]\})) \\ & \land\, (\forall\, id \in McastID : \forall\, rcver \in GroupDest[id] : \forall\, msg \in proposeTS[rcver][id] : \\ & \quad \land\, msg.id \in mcastedID) \end{aligned}$$

Every local clock is bounded with *MaxClock*

$$BoundedClock \triangleq \forall\, p \in Proc : clock[p] \leq MaxClock$$

If process p issues a global timestamp for message id, message id must be multicast before.
If process p is not an addressee of message id, t never issues a global timestamp for message id.

$$ValidGlobalTS \triangleq$$

$\land \forall\, id \in McastID : \forall\, rcver \in GroupDest[id] :$
$\quad globalTS[rcver][id] \neq TimestampNull \Rightarrow id \in mcastedID$
$\land \forall\, id \in McastID : \forall\, rcver \in Proc \setminus GroupDest[id] :$
$\quad globalTS[rcver][id] = TimestampNull$

If there exists an in-transit multicast message for message id, message id must be multicast before by its multicaster.

$ValidInTransitMcast \triangleq$
$\land \forall\, snder,\ rcver \in Proc : \forall\, id \in McastID : \forall\, m \in inTransit[snder][rcver] :$
$\quad (m.type = MType \land m.id = id) \Rightarrow (snder = Mcaster[id] \land id \in mcastedID)$

Type invariants

$TypeOK \triangleq$
$\land\ clock \in [Proc \to Time \cup \{TimeNull\}]$
$\land\ localTS \in [Proc \to [McastID \to TimestampSet]]$
$\land\ globalTS \in [Proc \to [McastID \to TimestampSet]]$
$\land\ phase \in [Proc \to [McastID \to \{Start,\ Proposed,\ Committed\}]]$
$\land\ rcvdMcastID \in [Proc \to \text{SUBSET}\ McastID]$
$\land\ mcastedID \in \text{SUBSET}\ McastID$
$\land\ inTransit \in [Proc \to [Proc \to \text{SUBSET}\ InTransitMsgSet]]$
$\land\ delivered \in [Proc \to [McastID \to \text{BOOLEAN}\ ]]$
$\land\ proposeTS \in [Proc \to [McastID \to \text{SUBSET}\ ProposeMsgSet]]$
$\land\ dCntr \in [Proc \to [McastID \to \{0, 1\}]]$

If process p commits message id, it has received at least one proposal for message id.
If process p commits message id, it has not issued any global timestamp for message id.

$ValidPhase \triangleq$
$\forall\, p \in Proc : \forall\, id \in McastID :$
$\quad (\land\, phase[p][id] = Committed \Rightarrow (\forall\, q \in GroupDest[id] : \exists\, m \in proposeTS[p][id] : m.source = q)$
$\quad\ \land\, phase[p][id] = Committed \Rightarrow globalTS[p][id] \neq TimestampNull)$

This inductive invariant implies *Validity*.

$IndInv \triangleq$
$\land\ TypeOK$
$\land\ Validity$
$\land\ Integrity$
$\land\ ValidOwnedLocalTS$
$\land\ ValidInTransitProposeTS$
$\land\ ValidRcvdProposeTS$
$\land\ BoundedClock$
$\land\ ValidGlobalTS$
$\land\ ValidInTransitMcast$
$\land\ ValidPhase$

\ * Modification History
\ * Last modified *Mon Sep* 20 16:51:56 *CEST* 2021 by *tran*
\ * Created *Tue Mar* 16 08:59:43 *CET* 2021 by *tran*