
MODULE *P2PBroadcastSpec*

Spec for a reliable *p2p* broadcast.

EXTENDS *Naturals*, *Sequences*, *FiniteSets*

CONSTANT

Proc, Set of processes
Data

VARIABLES

sent, All messages sent by all processors
received_by All messages received. Function from message to receiving processors

vars \triangleq $\langle sent, received_by \rangle$

Message is a record including the sending proc and a data.

Message \triangleq $[from : Proc, data : Data]$

Init \triangleq $\wedge sent = \{\}$
 $\wedge received_by = [m \in Message \mapsto \{\}]$

TypeOK \triangleq $\wedge sent \in SUBSET Message$
 $\wedge received_by \in [Message \rightarrow SUBSET Proc]$

Send message *m*

Send(m) \triangleq $\wedge m \notin sent$ Message is sent only once by the original sender
 $\wedge sent' = sent \cup \{m\}$
 $\wedge UNCHANGED \langle received_by \rangle$

Receive a message *m* at proc *p*

Recv(m, p) \triangleq $\wedge m \in sent$ receive only if *m* was sent first
 $\wedge p \notin received_by[m]$ receive only once
 $\wedge received_by' = [received_by \text{ EXCEPT } ![m] = @ \cup \{p\}]$
 $\wedge UNCHANGED \langle sent \rangle$

Next $\triangleq \exists m \in Message, p \in Proc : Send(m) \vee Recv(m, p)$

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

FairSpec is *Spec* with the addition requirement that it keeps taking steps.

FairSpec $\triangleq Spec \wedge WF_{vars}(Next)$

\ * Modification History
\ * Last modified *Fri Apr 07 14:20:56 CEST 2023* by *kulpreet*
\ * Created *Wed Apr 05 09:47:12 CEST 2023* by *kulpreet*