MODULE *DistRefines*

We use *TLAPS* to prove that the distributed Bakery algorithm refines the deconstructed Bakery algorithm (with atomic choice of ticket numbers).

EXTENDS *BakeryDistributed*, *SequenceTheorems*

LEMMA $ackNotNat \triangleq ack \notin Nat \cup \{qm\}$
BY *NoSetContainsEverything* DEF *ack*

The following lemma should be included in *SequenceTheorems*.

LEMMA $RangeHeadTail \triangleq$
  ASSUME NEW S, NEW $s \in Seq(S) \setminus \{\langle\rangle\}$
  PROVE $Range(s) = \{Head(s)\} \cup Range(Tail(s))$
$\langle 1\rangle 1$. ASSUME NEW $x \in Range(s)$, $x \neq Head(s)$
      PROVE $x \in Range(Tail(s))$
  $\langle 2\rangle 1$. PICK $i \in 2 \,..\, Len(s) : s[i] = x$
    BY $\langle 1\rangle 1$ DEF *Range*
  $\langle 2\rangle 2$. $\land\ Tail(s) \in Seq(S)$
        $\land\ i - 1 \in 1 \,..\, Len(Tail(s))$
        $\land\ Tail(s)[i-1] = x$
    BY $\langle 2\rangle 1$, *HeadTailProperties*
  $\langle 2\rangle$.QED BY $\langle 2\rangle 2$, *RangeEquality*, *Zenon*
$\langle 1\rangle$.QED BY $\langle 1\rangle 1$ DEF *Range*

The following is a full type invariant for the algorithm.

$FullTypeOK \triangleq$
  $\land\ number \in [Procs \to Nat]$
  $\land\ localNum \in POP(Nat)$
  $\land\ localCh \in POP(\{0, 1\})$
  $\land\ ackRcvd \in POP(\{0, 1\})$
  $\land\ q \in POP(Seq(Nat \cup \{ack\}))$
  $\land\ pc \in [ProcSet \to \{\text{“ncs”}, \text{“M”}, \text{“L”}, \text{“cs”}, \text{“P”}, \text{“ch”}, \text{“L0”}, \text{“L2”}, \text{“L3”}, \text{“wr”}\}]$
  $\land\ \forall\, p \in ProcIds : pc[p] \in \{\text{“ncs”}, \text{“M”}, \text{“L”}, \text{“cs”}, \text{“P”}\}$
  $\land\ \forall\, p \in SubProcs : pc[p] \in \{\text{“ch”}, \text{“L0”}, \text{“L2”}, \text{“L3”}\}$
  $\land\ \forall\, p \in MsgProcs : pc[p] = \text{“wr”}$

THEOREM $Typing \triangleq Spec \Rightarrow \Box FullTypeOK$
$\langle 1\rangle 1$. $Init \Rightarrow FullTypeOK$
  $\langle 2\rangle$.SUFFICES ASSUME $Init$PROVE $FullTypeOK$
    OBVIOUS
  $\langle 2\rangle$.$\langle\rangle \in Seq(Nat \cup \{ack\})$
    OBVIOUS
  $\langle 2\rangle$. $\land\ localNum \in POP(Nat)$
      $\land\ localCh \in POP(\{0, 1\})$
      $\land\ ackRcvd \in POP(\{0, 1\})$
      $\land\ q \in POP(Seq(Nat \cup \{ack\}))$

BY $POP\_construct$, Isa DEF $Init$

$\langle 2\rangle$.QED BY $DisjointIds$ DEF $Init$, $FullTypeOK$, $ProcSet$

$\langle 1\rangle 2.\ FullTypeOK \wedge [Next]_{vars} \Rightarrow FullTypeOK'$

$\langle 2\rangle$ SUFFICES ASSUME $FullTypeOK$, $[Next]_{vars}$ PROVE $FullTypeOK'$

OBVIOUS

$\langle 2\rangle$.USE DEF $FullTypeOK$, $OtherProcs$

$\langle 2\rangle 1.$ ASSUME NEW $self \in Procs$, $ncs(\langle self\rangle)$ PROVE $FullTypeOK'$

BY $\langle 2\rangle 1$ DEF ncs, $ProcSet$, $ProcIds$

$\langle 2\rangle 2.$ ASSUME NEW $self \in Procs$, $M(\langle self\rangle)$ PROVE $FullTypeOK'$

$\langle 3\rangle$.PICK $v \in Nat$:

$\wedge\ number' = [number$ EXCEPT $![self] = v]$

$\wedge\ q' = [q$ EXCEPT $![self] =$

$[j \in OtherProcs(self) \mapsto Append(q[self][j],\ v)]]$

$\wedge\ pc' = [pc$ EXCEPT $![\langle self\rangle] =$ "L"$]$

$\wedge$ UNCHANGED $\langle localNum,\ localCh,\ ackRcvd\rangle$

BY $\langle 2\rangle 2$, Isa DEF M

$\langle 3\rangle 1.\ \forall j \in OtherProcs(self) : Append(q[self][j],\ v) \in Seq(Nat \cup \{ack\})$

BY POP_access

$\langle 3\rangle 2.\ q' \in POP(Seq(Nat \cup \{ack\}))$

BY $\langle 3\rangle 1$, $POP\_except\_fun\_type$, Isa

$\langle 3\rangle$.QED BY $\langle 3\rangle 2$ DEF $ProcSet$, $ProcIds$

$\langle 2\rangle 3.$ ASSUME NEW $self \in Procs$, $L(\langle self\rangle)$ PROVE $FullTypeOK'$

BY $\langle 2\rangle 3$ DEF L, $ProcSet$, $ProcIds$

$\langle 2\rangle 4.$ ASSUME NEW $self \in Procs$, $cs(\langle self\rangle)$ PROVE $FullTypeOK'$

BY $\langle 2\rangle 4$ DEF cs, $ProcSet$, $ProcIds$

$\langle 2\rangle 5.$ ASSUME NEW $self \in Procs$, $P(\langle self\rangle)$ PROVE $FullTypeOK'$

$\langle 3\rangle.\ \wedge\ ackRcvd' = [ackRcvd$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto 0]]$

$\wedge\ number' = [number$ EXCEPT $![self] = 0]$

$\wedge\ q' = [q$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto Append(q[self][j],\ 0)]]$

$\wedge\ pc' = [pc$ EXCEPT $![\langle self\rangle] =$ "ncs"$]$

$\wedge$ UNCHANGED $\langle localNum,\ localCh\rangle$

BY $\langle 2\rangle 5$ DEF P

$\langle 3\rangle 1.\ ackRcvd' \in POP(\{0, 1\})$
BY *POP_except_fun_type*, *Isa* – why doesn't this work here?
$\langle 4\rangle$.DEFINE $g(i, j) \triangleq 0$
$\langle 4\rangle 1. \land ackRcvd \in POP(\{0, 1\})$
$\land ackRcvd' = [ackRcvd \text{ EXCEPT } ![self] = [j \in OtherProcs(self) \mapsto g(self, j)]]$
OBVIOUS
$\langle 4\rangle 2.\ \forall j \in OtherProcs(self) : g(self, j) \in \{0, 1\}$
OBVIOUS
$\langle 4\rangle$.HIDE DEF g
$\langle 4\rangle$.QED BY ONLY $\langle 4\rangle 1$, $\langle 4\rangle 2$, *POP_except_fun_type*
$\langle 3\rangle 2.\ \forall j \in OtherProcs(self) : Append(q[self][j], 0) \in Seq(Nat \cup \{ack\})$
BY *POP_access*
$\langle 3\rangle 3.\ q' \in POP(Seq(Nat \cup \{ack\}))$
BY $\langle 3\rangle 2$, *POP_except_fun_type*, *Isa*
$\langle 3\rangle$.QED BY $\langle 3\rangle 1$, $\langle 3\rangle 3$, *Zenon* DEF *ProcSet*, *ProcIds*
$\langle 2\rangle 6$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$ch(\langle self, oth\rangle)$
PROVE $FullTypeOK'$
BY $\langle 2\rangle 6$, *POP_except*, *Zenon* DEF *ch*, *ProcSet*, *SubProcs*
$\langle 2\rangle 7$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L0(\langle self, oth\rangle)$
PROVE $FullTypeOK'$
BY $\langle 2\rangle 7$, *POP_except*, *Zenon* DEF *L0*, *ProcSet*, *SubProcs*
$\langle 2\rangle 8$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L2(\langle self, oth\rangle)$
PROVE $FullTypeOK'$
BY $\langle 2\rangle 8$ DEF *L2*, *ProcSet*, *SubProcs*
$\langle 2\rangle 9$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L3(\langle self, oth\rangle)$
PROVE $FullTypeOK'$
BY $\langle 2\rangle 9$ DEF *L3*, *ProcSet*, *SubProcs*
$\langle 2\rangle 10$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$msg(\langle self, oth, \text{“msg”}\rangle)$
PROVE $FullTypeOK'$
$\langle 3\rangle. \land q[oth][self] \neq \langle\rangle$
$\land$ LET $v \triangleq Head(q[oth][self])$
IN $\land$ IF $v = ack$
THEN $\land ackRcvd' = [ackRcvd \text{ EXCEPT } ![self][oth] = 1]$
$\land$ UNCHANGED *localNum*
ELSE $\land localNum' = [localNum \text{ EXCEPT } ![self][oth] = v]$
$\land$ UNCHANGED *ackRcvd*
$\land$ IF $v \in \{0, ack\}$
THEN $q' = [q \text{ EXCEPT } ![oth][self] = Tail(@)]$
ELSE $q' = [q \text{ EXCEPT } ![oth][self] = Tail(@),$
$![self][oth] = Append(@, ack)]$

$\land$ UNCHANGED $\langle number, localCh, pc\rangle$
BY $\langle 2\rangle 10$ DEF msg, wr
$\langle 3\rangle$.DEFINE $v \triangleq Head(q[oth][self])$
$\langle 3\rangle 0$. $v \in Nat \cup \{ack\}$
BY POP_access
$\langle 3\rangle 1$. $localNum' \in POP(Nat)$
BY $\langle 3\rangle 0$, POP_except, Isa
$\langle 3\rangle 2$. $ackRcvd' \in POP(\{0, 1\})$
BY POP_except, Isa
$\langle 3\rangle 3$. $q' \in POP(Seq(Nat \cup \{ack\}))$
$\langle 4\rangle$.DEFINE $q1 \triangleq [q$ EXCEPT $![oth][self] = Tail(@)]$
$q2 \triangleq [q1$ EXCEPT $![self][oth] = Append(@, ack)]$
$\langle 4\rangle 0$. $Tail(q[oth][self]) \in Seq(Nat \cup \{ack\})$
BY POP_access
$\langle 4\rangle 1$. $q1 \in POP(Seq(Nat \cup \{ack\}))$
BY $\langle 4\rangle 0$, POP_except, Isa
$\langle 4\rangle$.HIDE DEF $q1$
$\langle 4\rangle$a. $Append(q1[self][oth], ack) \in Seq(Nat \cup \{ack\})$
BY $\langle 4\rangle 1$, POP_access
$\langle 4\rangle 2$. $q2 \in POP(Seq(Nat \cup \{ack\}))$
BY $\langle 4\rangle 1$, $\langle 4\rangle$a, POP_except, Isa
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $Zenon$ DEF $q1$
$\langle 3\rangle$.QED BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$
$\langle 2\rangle 11$.CASE UNCHANGED $vars$
BY $\langle 2\rangle 11$ DEF $vars$
$\langle 2\rangle$.HIDE DEF $FullTypeOK$
$\langle 2\rangle 12$. QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 2\rangle 9$, $\langle 2\rangle 10$, $\langle 2\rangle 11$
DEF $Next$, $main$, sub, $ProcIds$, $SubProcs$, $MsgProcs$
$\langle 1\rangle$.QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, PTL DEF $Spec$

The following inductive invariant relates the contents of the communication channels and of the local variables. It is instrumental for the refinement proof below.

$Inv \triangleq$
$\land \forall\, i \in Procs : number[i] \neq 0 \equiv pc[\langle i\rangle] \in \{$ "L", "cs", "P" $\}$
$\land \forall\, i \in Procs : number[i] = 0 \Rightarrow$
$\forall\, j \in OtherProcs(i) : ackRcvd[i][j] = 0 \land ack \notin Range(q[j][i])$
$\land \forall\, i \in Procs : \forall\, j \in OtherProcs(i) : number[i] \neq 0 \Rightarrow$
The following describes a state machine of how ticket numbers are propagated to subprocesses and how acknowledgements are received.
$\lor \land pc[\langle i, j\rangle] =$ "L0"
$\land pc[\langle i\rangle] \quad =$ "L"
$\land number[i] \in Range(q[i][j])$

$\land\ ack \notin Range(q[j][i])$
$\land\ ackRcvd[i][j] = 0$
$\lor\ \land\ pc[\langle i, j\rangle] = \text{“L0”}$
$\land\ pc[\langle i\rangle] \quad = \text{“L”}$
$\land\ number[i] \notin Range(q[i][j])$
$\land\ 0 \notin Range(q[i][j])$
$\land\ ack \in Range(q[j][i])$
$\land\ ackRcvd[i][j] = 0$
$\land\ localNum[j][i] = number[i]$
$\lor\ \land\ number[i] \notin Range(q[i][j])$
$\land\ 0 \notin Range(q[i][j])$
$\land\ ack \notin Range(q[j][i])$
$\land\ ackRcvd[i][j] = 1$
$\land\ localNum[j][i] = number[i]$

$\land \forall\, i \in Procs : \forall\, j \in OtherProcs(i) : \forall\, k,\, l \in 1\,..\,Len(q[i][j]) :$

Facts about the contents of communication channels.

no message appears more than once

$\land\ q[i][j][k] = q[i][j][l] \Rightarrow k = l$

non-zero messages correspond to the current ticket of the sender

$\land\ q[i][j][k] \in Nat \setminus \{0\} \Rightarrow q[i][j][k] = number[i]$

zeros precede ticket numbers

$\land\ q[i][j][k] = 0 \land q[i][j][l] \in Nat \setminus \{0\} \Rightarrow k < l$

THEOREM $Invariance \triangleq Spec \Rightarrow \Box Inv$

$\langle 1\rangle 1.$ $Init \Rightarrow Inv$

$\langle 2\rangle 1.$ ASSUME $Init$, NEW $i \in Procs$
PROVE $\land\ number[i] = 0$
$\land\ pc[\langle i\rangle] \quad \notin \{\text{“L”}, \text{“cs”}, \text{“P”}\}$
BY $\langle 2\rangle 1$, *Zenon* DEF *Init*, *ProcSet*, *ProcIds*, *SubProcs*, *MsgProcs*

$\langle 2\rangle 2.$ ASSUME $Init$, NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $ackRcvd[i][j] = 0 \land ack \notin Range(q[j][i])$
BY $\langle 2\rangle 2$ DEF *Init*, *Range*, *OtherProcs*

$\langle 2\rangle 3.$ ASSUME $Init$, NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1\,..\,Len(q[i][j])$, NEW $l \in 1\,..\,Len(q[i][j])$
PROVE FALSE
BY $\langle 2\rangle 3$ DEF *Init*

$\langle 2\rangle$.QED BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, *Zenon* DEF *Inv*

$\langle 1\rangle 2.$ $FullTypeOK \land Inv \land [Next]_{vars} \Rightarrow Inv'$

$\langle 2\rangle$ SUFFICES ASSUME $FullTypeOK$,
Inv,
$[Next]_{vars}$
PROVE Inv'
OBVIOUS

$\langle 2\rangle$.USE DEF *FullTypeOK*

$\langle 2\rangle 1.$ ASSUME NEW $self \in Procs$,

$ncs(\langle self \rangle)$
PROVE Inv'
BY $\langle 2 \rangle 1$ DEF ncs, Inv, $ProcSet$, $ProcIds$
$\langle 2 \rangle 2$. ASSUME NEW $self \in Procs$,
$M(\langle self \rangle)$
PROVE Inv'
$\langle 3 \rangle$. $\land\ pc[\langle self \rangle] =$ "M"
$\land\ \forall\, oth \in Procs \setminus \{self\} : pc[\langle self,\ oth \rangle] =$ "L0"
$\land\ pc' = [pc$ EXCEPT $![\langle self \rangle] =$ "L"$]$
$\land$ UNCHANGED $\langle localNum,\ ackRcvd \rangle$
BY $\langle 2 \rangle 2$ DEF M, $SubProcsOf$, $SubProcs$
$\langle 3 \rangle$.PICK $v \in Nat \setminus \{0\}$:
$\land\ number' = [number$ EXCEPT $![self] = v]$
$\land\ q' = [q$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto Append(q[self][j],\ v)]]$
BY $\langle 2 \rangle 2$, Isa DEF M
$\langle 3 \rangle 1$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $\land\ q[i][j] \in Seq(Nat \cup \{ack\})$
$\land\ q'[i][j] =$ IF $i = self$ THEN $Append(q[self][j],\ v)$ ELSE $q[i][j]$
BY DEF $OtherProcs$, POP, $PFunc$
$\langle 3 \rangle 2$. $Inv!1'$
$\langle 4 \rangle 1$. $Inv!1$
BY $Zenon$ DEF Inv
$\langle 4 \rangle$.QED
BY $\langle 4 \rangle 1$, $Zenon$ DEF $FullTypeOK$, $ProcSet$, $ProcIds$
$\langle 3 \rangle 3$. ASSUME NEW $i \in Procs$, $number'[i] = 0$, NEW $j \in OtherProcs(i)$
PROVE $ackRcvd'[i][j] = 0 \land ack \notin Range(q'[j][i])$
$\langle 4 \rangle 1$. $ackRcvd'[i][j] = 0$
BY $\langle 3 \rangle 3$ DEF Inv
$\langle 4 \rangle 2$. $ack \notin Range(q[j][i])$
BY $\langle 3 \rangle 3$ DEF Inv
$\langle 4 \rangle 3$. $ack \notin Range(q'[j][i])$
BY ONLY $\langle 4 \rangle 2$, $\langle 3 \rangle 1$, $ackNotNat$, $AppendProperties$ DEF $OtherProcs$
$\langle 4 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 3$
$\langle 3 \rangle 4$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, $number'[i] \neq 0$
PROVE $Inv!3!(i)!(j)!2'$
$\langle 4 \rangle 1$.CASE $i = self$
$\langle 5 \rangle 1$. $pc'[\langle i,\ j \rangle] =$ "L0"
BY $\langle 4 \rangle 1$ DEF $OtherProcs$
$\langle 5 \rangle 2$. $pc'[\langle i \rangle] =$ "L"
BY $\langle 4 \rangle 1$ DEF $ProcSet$, $ProcIds$
$\langle 5 \rangle 3$. $v \in Range(q'[i][j])$
BY ONLY $\langle 3 \rangle 1$, $\langle 4 \rangle 1$, $AppendProperties$
$\langle 5 \rangle 4$. $\land\ ackRcvd[i][j] = 0$
$\land\ ack \notin Range(q[j][i])$
BY $\langle 4 \rangle 1$ DEF Inv

⟨5⟩5. $ack \notin Range(q'[j][i])$
BY ⟨3⟩1, ⟨4⟩1, ⟨5⟩4 DEF *OtherProcs*
⟨5⟩.QED BY ⟨4⟩1, ⟨5⟩1, ⟨5⟩2, ⟨5⟩3, ⟨5⟩4, ⟨5⟩5
⟨4⟩2.CASE $i \neq self$
⟨5⟩1. $Inv!3!(i)!(j)!2$
BY ⟨3⟩4, ⟨4⟩2 DEF *Inv*
⟨5⟩2. UNCHANGED $\langle number[i],\ pc[\langle i\rangle],\ pc[\langle i,\ j\rangle],\ q[i][j]\rangle$
BY ⟨4⟩2, ⟨3⟩1
⟨5⟩3. $ack \in Range(q'[j][i]) \equiv ack \in Range(q[j][i])$
BY ONLY ⟨3⟩1, *ackNotNat*, *AppendProperties* DEF *OtherProcs*
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
⟨3⟩5. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1\,..\,Len(q'[i][j])$, NEW $l \in 1\,..\,Len(q'[i][j])$
PROVE $Inv!4!(i)!(j)!(k,\ l)'$
⟨4⟩1.CASE $i = self$
⟨5⟩.ASSUME NEW $kk \in 1\,..\,Len(q[self][j])$
PROVE $q[self][j][kk] \in \{0,\ ack\}$
⟨6⟩1. $number[self] = 0$
BY DEF *Inv*
⟨6⟩2. $q[self][j][kk] \in Nat \cup \{ack\}$
BY ONLY ⟨3⟩1, ⟨4⟩1
⟨6⟩3. $q[self][j][kk] \in Nat \setminus \{0\} \Rightarrow q[self][j][kk] = number[self]$
BY ⟨3⟩1, ⟨4⟩1 DEF *Inv*
⟨6⟩.QED BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩3
⟨5⟩.QED BY ⟨3⟩1, ⟨4⟩1, *ackNotNat* DEF *Inv*
⟨4⟩2.CASE $i \neq self$
BY ⟨3⟩1, ⟨4⟩2 DEF *Inv*
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
⟨3⟩.QED BY ONLY ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5 DEF *Inv*
⟨2⟩3. ASSUME NEW $self \in Procs$,
$L(\langle self\rangle)$
PROVE Inv'
BY ⟨2⟩3 DEF *L*, *FullTypeOK*, *Inv*, *ProcSet*, *ProcIds*, *SubProcsOf*, *SubProcs*, *OtherProcs*
⟨2⟩4. ASSUME NEW $self \in Procs$,
$cs(\langle self\rangle)$
PROVE Inv'
BY ⟨2⟩4 DEF *cs*, *FullTypeOK*, *Inv*, *ProcSet*, *ProcIds*, *OtherProcs*
⟨2⟩5. ASSUME NEW $self \in Procs$,
$P(\langle self\rangle)$
PROVE Inv'
⟨3⟩. $\wedge\ pc[\langle self\rangle] =$ "P"
$\wedge\ ackRcvd' = [ackRcvd$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto 0]]$
$\wedge\ number' = [number$ EXCEPT $![self] = 0]$
$\wedge\ q' = [q$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto Append(q[self][j],\ 0)]]$

$\land\ pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{“ncs”}]$
$\land$ UNCHANGED $localNum$
BY $\langle 2 \rangle 5$ DEF P
$\langle 3 \rangle 1$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $\land\ ackRcvd'[i][j] = \text{IF } i = self \text{ THEN } 0 \text{ ELSE } ackRcvd[i][j]$
$\land\ q[i][j] \in Seq(Nat \cup \{ack\})$
$\land\ q'[i][j] = \text{IF } i = self \text{ THEN } Append(q[i][j], 0) \text{ ELSE } q[i][j]$
BY DEF $FullTypeOK$, POP, $PFunc$
$\langle 3 \rangle 2$. ASSUME NEW $i \in Procs$
PROVE $number'[i] \neq 0 \equiv pc'[\langle i \rangle] \in \{\text{“L”}, \text{“cs”}, \text{“P”}\}$
BY DEF $FullTypeOK$, Inv, $ProcSet$, $ProcIds$
$\langle 3 \rangle 3$. ASSUME NEW $i \in Procs$, $number'[i] = 0$, NEW $j \in OtherProcs(i)$
PROVE $ackRcvd'[i][j] = 0 \land ack \notin Range(q'[j][i])$
$\langle 4 \rangle 1$.CASE $i = self$
$\langle 5 \rangle .ack \notin Range(q[j][i])$
BY $\langle 4 \rangle 1$, $Zenon$ DEF Inv
$\langle 5 \rangle$.QED BY $\langle 3 \rangle 1$, $\langle 4 \rangle 1$, Isa DEF $OtherProcs$
$\langle 4 \rangle 2$.CASE $j = self$
$\langle 5 \rangle 1$. $ackRcvd[i][j] = 0 \land ack \notin Range(q[j][i])$
BY $\langle 3 \rangle 3$, $\langle 4 \rangle 2$ DEF Inv, $OtherProcs$
$\langle 5 \rangle$.QED BY ONLY $\langle 3 \rangle 1$, $\langle 4 \rangle 2$, $\langle 5 \rangle 1$, $AppendProperties$, $ackNotNat$ DEF $OtherProcs$
$\langle 4 \rangle 3$.CASE $i \neq self \land j \neq self$
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 3$, $\langle 4 \rangle 3$ DEF Inv
$\langle 4 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$
$\langle 3 \rangle 4$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, $number'[i] \neq 0$
PROVE $Inv!3!(i)!(j)!2'$
$\langle 4 \rangle 1$. $Inv!3!(i)!(j)!2$
BY $\langle 3 \rangle 4$ DEF Inv
$\langle 4 \rangle 2$. UNCHANGED $\langle pc[\langle i \rangle], pc[\langle i, j \rangle], number[i], q[i][j], ackRcvd[i][j] \rangle$
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 4$
$\langle 4 \rangle 3$. $ack \in Range(q'[j][i]) \equiv ack \in Range(q[j][i])$
BY ONLY $\langle 3 \rangle 1$, $\langle 3 \rangle 4$, $AppendProperties$, $ackNotNat$ DEF $OtherProcs$
$\langle 4 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$
$\langle 3 \rangle 5$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1 \,..\, Len(q'[i][j])$, NEW $l \in 1 \,..\, Len(q'[i][j])$
PROVE $Inv!4!(i)!(j)!(k, l)'$
$\langle 4 \rangle 1$.CASE $i = self$
$\langle 5 \rangle 1$. $\land\ number[self] \notin Range(q[self][j])$
$\land\ 0 \notin Range(q[self][j])$
BY $\langle 4 \rangle 1$, $Zenon$ DEF Inv
$\langle 5 \rangle 2$. ASSUME NEW $n \in 1 \,..\, Len(q[self][j])$
PROVE $q[self][j][n] = ack$
BY ONLY $\langle 3 \rangle 1$, $\langle 4 \rangle 1$, $\langle 5 \rangle 1$, Inv, $RangeEquality$ DEF Inv
$\langle 5 \rangle$.QED BY $\langle 3 \rangle 1$, $\langle 4 \rangle 1$, $\langle 5 \rangle 2$, $ackNotNat$ DEF Inv
$\langle 4 \rangle 2$.CASE $i \neq self$

BY $\langle 3\rangle 1$, $\langle 4\rangle 2$ DEF *Inv*

$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle$.QED BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, *Zenon* DEF *Inv*

$\langle 2\rangle 6$. ASSUME NEW $self \in Procs$, NEW $oth \in Procs \setminus \{self\}$, $ch(\langle self, oth\rangle)$
PROVE Inv'

BY $\langle 2\rangle 6$ DEF *FullTypeOK*, *Inv*, *ch*, *ProcSet*, *ProcIds*, *SubProcs*

$\langle 2\rangle 7$. ASSUME NEW $self \in Procs$, NEW $oth \in Procs \setminus \{self\}$, $L0(\langle self, oth\rangle)$
PROVE Inv'

BY $\langle 2\rangle 7$ DEF *FullTypeOK*, *Inv*, *L0*, *ProcSet*, *ProcIds*, *SubProcs*

$\langle 2\rangle 8$. ASSUME NEW $self \in Procs$, NEW $oth \in Procs \setminus \{self\}$, $L2(\langle self, oth\rangle)$
PROVE Inv'

BY $\langle 2\rangle 8$ DEF *FullTypeOK*, *Inv*, *L2*, *ProcSet*, *ProcIds*, *SubProcs*

$\langle 2\rangle 9$. ASSUME NEW $self \in Procs$, NEW $oth \in Procs \setminus \{self\}$, $L3(\langle self, oth\rangle)$
PROVE Inv'

BY $\langle 2\rangle 9$ DEF *FullTypeOK*, *Inv*, *L3*, *ProcSet*, *ProcIds*, *SubProcs*

$\langle 2\rangle 10$. ASSUME NEW $self \in Procs$, NEW $oth \in Procs \setminus \{self\}$, $msg(\langle self, oth, \text{“msg”}\rangle)$
PROVE Inv'

$\langle 3\rangle$.DEFINE $v \triangleq Head(q[oth][self])$

$\langle 3\rangle$. $\land\ q[oth][self] \neq \langle\rangle$
$\land$ IF $v = ack$
THEN $\land\ ackRcvd' = [ackRcvd$ EXCEPT $![self][oth] = 1]$
$\land\ localNum' = localNum$
ELSE $\land\ localNum' = [localNum$ EXCEPT $![self][oth] = v]$
$\land\ ackRcvd' = ackRcvd$
$\land$ UNCHANGED $\langle pc, number\rangle$

BY $\langle 2\rangle 10$ DEF *msg*, *wr*

$\langle 3\rangle$q. IF $v \in \{0, ack\}$
THEN $q' = [q$ EXCEPT $![oth][self] = Tail(@)]$
ELSE $q' = [q$ EXCEPT $![oth][self] = Tail(@),$
$![self][oth] = Append(q[self][oth], ack)]$

BY $\langle 2\rangle 10$ DEF *msg*, *wr*

$\langle 3\rangle 1$. $Inv!1'$
BY DEF *Inv*

$\langle 3\rangle 2$.CASE $v = ack$

$\langle 4\rangle$.$ack \in Range(q[oth][self])$
BY $\langle 3\rangle 2$ DEF *FullTypeOK*, *POP*, *PFunc*, *OtherProcs*, *Range*

$\langle 4\rangle$. $\land\ ackRcvd' = [ackRcvd$ EXCEPT $![self][oth] = 1]$
$\land\ localNum' = localNum$
$\land\ q' = [q$ EXCEPT $![oth][self] = Tail(@)]$
$\land\ q[oth][self] \in Seq(Nat \cup \{ack\})$

$\land\ Tail(q[oth][self]) \in Seq(Nat \cup \{ack\})$
BY $\langle 3\rangle 2$, $\langle 3\rangle$q, *POP_access* DEF *OtherProcs*
$\langle 4\rangle 1$. $q'[oth][self] = Tail(q[oth][self])$
BY *POP_except*, *Isa* DEF *OtherProcs*

$\langle 4\rangle 2$. ASSUME NEW $i \in Procs$, $number[i] = 0$, NEW $j \in OtherProcs(i)$
PROVE $\land\ ackRcvd'[i][j] = 0$
$\land\ ack \notin Range(q'[j][i])$
$\langle 5\rangle 1$. $\land\ ackRcvd[i][j] = 0$
$\land\ ack \notin Range(q[j][i])$
BY $\langle 4\rangle 2$ DEF *Inv*
$\langle 5\rangle 2$. $ackRcvd'[i][j] = ackRcvd[i][j]$
BY $\langle 5\rangle 1$, *POP_except*
$\langle 5\rangle 3$. $q'[j][i] = q[j][i]$
BY $\langle 5\rangle 1$, *POP_except* DEF *OtherProcs*
$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$
$\langle 4\rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, $number[i] \neq 0$
PROVE *Inv*!3!(i)!(j)!2′
$\langle 5\rangle 1$.CASE $i = self \land j = oth$
$\langle 6\rangle 1$. $\land\ number[self] \notin Range(q[self][oth])$
$\land\ 0 \notin Range(q[self][oth])$
$\land\ localNum[oth][self] = number[self]$
BY $\langle 4\rangle 3$, $\langle 5\rangle 1$, *Zenon* DEF *Inv*
$\langle 6\rangle 2$. $ackRcvd'[self][oth] = 1$
BY *POP_except*, *Isa* DEF *OtherProcs*
$\langle 6\rangle 3$. $q'[self][oth] = q[self][oth]$
BY *POP_except* DEF *OtherProcs*
$\langle 6\rangle 4$. ASSUME $ack \in Range(Tail(q[oth][self]))$
PROVE FALSE
$\langle 7\rangle 1$. PICK $k \in 1\,..\,Len(Tail(q[oth][self])) : Tail(q[oth][self])[k] = ack$
BY $\langle 6\rangle 4$ DEF *Range*
$\langle 7\rangle 2$. $\land\ k + 1 \in 1\,..\,Len(q[oth][self])$
$\land\ q[oth][self][k + 1] = ack$
$\land\ q[oth][self][1] = ack$
BY $\langle 3\rangle 2$, $\langle 7\rangle 1$
$\langle 7\rangle$.QED BY $\langle 7\rangle 2$ DEF *Inv*, *OtherProcs*
$\langle 6\rangle$.QED BY $\langle 5\rangle 1$, $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$, $\langle 4\rangle 1$, $\langle 6\rangle 4$
$\langle 5\rangle 2$.CASE $i = oth \land j = self$
$\langle 6\rangle 1$. UNCHANGED $\langle ackRcvd[oth][self], q[self][oth]\rangle$
BY *POP_except* DEF *OtherProcs*
$\langle 6\rangle 2$. ASSUME NEW $n \in Nat$
PROVE $n \in Range(q[oth][self]) \equiv n \in Range(Tail(q[oth][self]))$
BY $\langle 3\rangle 2$, *ackNotNat*, *RangeHeadTail*
$\langle 6\rangle$.QED BY $\langle 4\rangle 3$, $\langle 5\rangle 2$, $\langle 6\rangle 1$, $\langle 4\rangle 1$, $\langle 6\rangle 2$ DEF *Inv*, *OtherProcs*
$\langle 5\rangle 3$.CASE $\land \neg(i = self \land j = oth)$

$\wedge \neg(i = oth \wedge j = self)$
BY $\langle 4\rangle 3$, $\langle 5\rangle 3$, *POP_except* DEF *Inv*, *OtherProcs*
$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$
$\langle 4\rangle 4$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1 \,..\, Len(q'[i][j])$, NEW $l \in 1 \,..\, Len(q'[i][j])$
PROVE $Inv!4!(i)!(j)!(k,\ l)'$
$\langle 5\rangle 0$. $Inv!4!(i)!(j)$
BY DEF *Inv*
$\langle 5\rangle 1$.CASE $i = oth \wedge j = self$
$\langle 6\rangle$. $\wedge\ k \in 1 \,..\, Len(Tail(q[oth][self]))$
$\wedge\ l \in 1 \,..\, Len(Tail(q[oth][self]))$
BY $\langle 4\rangle 1$, $\langle 5\rangle 1$, *Zenon*
$\langle 6\rangle$. $\wedge\ k + 1 \in 1 \,..\, Len(q[oth][self])$
$\wedge\ l + 1 \in 1 \,..\, Len(q[oth][self])$
$\wedge\ Tail(q[oth][self])[k] = q[oth][self][k + 1]$
$\wedge\ Tail(q[oth][self])[l] = q[oth][self][l + 1]$
OBVIOUS
$\langle 6\rangle$.QED BY $\langle 4\rangle 1$, $\langle 5\rangle 0$, $\langle 5\rangle 1$
$\langle 5\rangle 2$.CASE $\neg(i = oth \wedge j = self)$
BY $\langle 5\rangle 0$, $\langle 5\rangle 2$, *POP_except*
$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$
$\langle 4\rangle$.QED BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ DEF *Inv* $Inv!1'$ is trivially preserved
$\langle 3\rangle 3$.CASE $v = 0$
$\langle 4\rangle .0 \in Range(q[oth][self])$
BY $\langle 3\rangle 3$ DEF *FullTypeOK*, *POP*, *PFunc*, *OtherProcs*, *Range*
$\langle 4\rangle$. $\wedge\ ackRcvd' = ackRcvd$
$\wedge\ localNum' = [localNum$ EXCEPT $![self][oth] = 0]$
$\wedge\ q' = [q$ EXCEPT $![oth][self] = Tail(@)]$
$\wedge\ q[oth][self] \in Seq(Nat \cup \{ack\})$
$\wedge\ Tail(q[oth][self]) \in Seq(Nat \cup \{ack\})$
BY $\langle 3\rangle 3$, $\langle 3\rangle$q, *POP_access*, *ackNotNat* DEF *OtherProcs*
$\langle 4\rangle 1$. $q'[oth][self] = Tail(q[oth][self])$
BY *POP_except*, *Isa* DEF *OtherProcs*
$\langle 4\rangle 2$. ASSUME NEW $i \in Procs$, $number[i] = 0$, NEW $j \in OtherProcs(i)$
PROVE $ackRcvd'[i][j] = 0 \wedge ack \notin Range(q'[j][i])$
$\langle 5\rangle 1$. $ackRcvd[i][j] = 0 \wedge ack \notin Range(q[j][i])$
BY $\langle 4\rangle 2$ DEF *Inv*
$\langle 5\rangle 2$.CASE $i = self \wedge j = oth$
BY $\langle 4\rangle 1$, $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF *Range*
$\langle 5\rangle 3$.CASE $\neg(i = self \wedge j = oth)$
BY $\langle 5\rangle 1$, $\langle 5\rangle 3$, *POP_except* DEF *OtherProcs*
$\langle 5\rangle$.QED BY $\langle 5\rangle 2$, $\langle 5\rangle 3$
$\langle 4\rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, $number[i] \neq 0$
PROVE $Inv!3!(i)!(j)!2'$
$\langle 5\rangle 1$.CASE $i = self \wedge j = oth$

⟨6⟩1. UNCHANGED ⟨$q[self][oth]$, $localNum[oth][self]$⟩
BY POP_except DEF $OtherProcs$
⟨6⟩2. $ack \in Range(q'[oth][self]) \equiv ack \in Range(q[oth][self])$
BY ⟨3⟩3, ⟨4⟩1, $ackNotNat$, $RangeHeadTail$
⟨6⟩.QED BY ⟨4⟩3, ⟨5⟩1, ⟨6⟩1, ⟨6⟩2 DEF Inv
⟨5⟩2.CASE $i = oth \land j = self$
⟨6⟩1. UNCHANGED $q[self][oth]$
BY POP_except DEF $OtherProcs$
⟨6⟩2. $number[i] \in Range(q'[oth][self]) \equiv number[i] \in Range(q[oth][self])$
BY ⟨3⟩3, ⟨4⟩1, ⟨4⟩3, $RangeHeadTail$
⟨6⟩.QED BY ⟨4⟩3, ⟨5⟩2, ⟨6⟩1, ⟨6⟩2 DEF Inv
⟨5⟩3.CASE $\land \neg(i = self \land j = oth)$
$\land \neg(i = oth \land j = self)$
BY ⟨4⟩3, ⟨5⟩3, POP_except DEF Inv, $OtherProcs$
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3
⟨4⟩4. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1 \,..\, Len(q'[i][j])$, NEW $l \in 1 \,..\, Len(q'[i][j])$
PROVE $Inv!4!(i)!(j)!(k,\ l)'$
⟨5⟩0. $Inv!4!(i)!(j)$
BY DEF Inv
⟨5⟩1.CASE $i = oth \land j = self$
⟨6⟩. $\land k \in 1 \,..\, Len(Tail(q[oth][self]))$
$\land l \in 1 \,..\, Len(Tail(q[oth][self]))$
BY ⟨4⟩1, ⟨5⟩1, $Zenon$
⟨6⟩. $\land k + 1 \in 1 \,..\, Len(q[oth][self])$
$\land l + 1 \in 1 \,..\, Len(q[oth][self])$
$\land Tail(q[oth][self])[k] = q[oth][self][k + 1]$
$\land Tail(q[oth][self])[l] = q[oth][self][l + 1]$
OBVIOUS
⟨6⟩.QED BY ⟨4⟩1, ⟨5⟩0, ⟨5⟩1
⟨5⟩2.CASE $\neg(i = oth \land j = self)$
BY ⟨5⟩0, ⟨5⟩2, POP_except
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2
⟨4⟩.QED BY ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 DEF Inv
⟨3⟩4.CASE $v \in Nat \setminus \{0\}$
⟨4⟩a. $v = number[oth]$
BY ⟨3⟩4 DEF Inv, $OtherProcs$
⟨4⟩b. $number[oth] \in Range(q[oth][self])$
BY ⟨4⟩a DEF $FullTypeOK$, POP, $PFunc$, $OtherProcs$, $Range$
⟨4⟩. $\land ackRcvd' = ackRcvd$
$\land localNum' = [localNum$ EXCEPT $![self][oth] = v]$
$\land q' = [q$ EXCEPT $![oth][self] = Tail(@)$,
$![self][oth] = Append(q[self][oth],\ ack)]$
$\land q[oth][self] \in Seq(Nat \cup \{ack\})$
$\land Tail(q[oth][self]) \in Seq(Nat \cup \{ack\})$

$\wedge\ q[self][oth] \in Seq(Nat \cup \{ack\})$
$\wedge\ Append(q[self][oth],\ ack) \in Seq(Nat \cup \{ack\})$
BY $\langle 3\rangle 4$, $\langle 3\rangle$q, *POP_access*, *ackNotNat* DEF *OtherProcs*

$\langle 4\rangle$d. ASSUME $0 \in Range(q[oth][self])$
PROVE FALSE

$\langle 5\rangle$.PICK $k \in 1\,..\,Len(q[oth][self]) : q[oth][self][k] = 0$
BY $\langle 4\rangle$d, *RangeEquality*

$\langle 5\rangle$.QED BY $\langle 3\rangle 4$ DEF *Inv*, *OtherProcs*

$\langle 4\rangle 1. \wedge\ q' \in POP(Seq(Nat \cup \{ack\}))$
$\wedge\ q'[oth][self] = Tail(q[oth][self])$
$\wedge\ q'[self][oth] = Append(q[self][oth],\ ack)$
$\wedge\ \forall\, i \in Procs : \forall\, j \in Procs \setminus \{i\} :$
$\neg(i = self \wedge j = oth) \wedge \neg(i = oth \wedge j = self)$
$\Rightarrow q'[i][j] = q[i][j]$

$\langle 5\rangle$.DEFINE $tl \triangleq Tail(q[oth][self])$
$qq \triangleq [q$ EXCEPT $![oth][self] = tl]$

$\langle 5\rangle .tl \in Seq(Nat \cup \{ack\})$
OBVIOUS needed because we will hide the definition of *tl*

$\langle 5\rangle 1.\ q' = [qq$ EXCEPT $![self][oth] = Append(q[self][oth],\ ack)]$
OBVIOUS

$\langle 5\rangle$.HIDE DEF *tl*

$\langle 5\rangle 2. \wedge\ qq \in POP(Seq(Nat \cup \{ack\}))$
$\wedge\ qq[oth][self] = tl$
BY *POP_except*, *Isa* DEF *OtherProcs*

$\langle 5\rangle 3.\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) :$
$i \neq oth \vee j \neq self \Rightarrow qq[i][j] = q[i][j]$
BY *POP_except* DEF *OtherProcs*

$\langle 5\rangle$.HIDE DEF *qq*

$\langle 5\rangle 4. \wedge\ q' \in POP(Seq(Nat \cup \{ack\}))$
$\wedge\ q'[self][oth] = Append(q[self][oth],\ ack)$
$\wedge\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) :$
$i \neq self \vee j \neq oth \Rightarrow q'[i][j] = qq[i][j]$
BY ONLY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $Append(q[self][oth],\ ack) \in Seq(Nat \cup \{ack\})$, *POP_except*, *Isa* DEF *OtherProcs*

$\langle 5\rangle$.QED BY ONLY $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$ DEF *OtherProcs*, *tl*

$\langle 4\rangle 5.$ ASSUME NEW $i \in Procs$, $number'[i] = 0$, NEW $j \in OtherProcs(i)$
PROVE $ackRcvd'[i][j] = 0 \wedge ack \notin Range(q'[j][i])$

$\langle 5\rangle 1.\ ackRcvd'[i][j] = 0 \wedge ack \notin Range(q[j][i])$
BY $\langle 4\rangle 5$ DEF *Inv*

$\langle 5\rangle 2.\ i \neq oth$
BY $\langle 3\rangle 4$, $\langle 4\rangle$a, $\langle 4\rangle 5$

$\langle 5\rangle 3$.CASE $i = self \wedge j = oth$

$\langle 6\rangle .Range(Tail(q[oth][self])) \subseteq Range(q[oth][self])$
BY DEF *Range*

$\langle 6\rangle$.QED BY $\langle 4\rangle 1$, $\langle 5\rangle 1$, $\langle 5\rangle 3$, *Zenon*

⟨5⟩4.CASE $i \neq self \lor j \neq oth$
BY ONLY ⟨4⟩1, ⟨5⟩1, ⟨5⟩2, ⟨5⟩4 DEF *OtherProcs*
⟨5⟩.QED BY ⟨5⟩3, ⟨5⟩4
⟨4⟩6. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, $number'[i] \neq 0$
PROVE $Inv!3!(i)!(j)!2'$
⟨5⟩1. $Inv!3!(i)!(j)!2$
BY ⟨4⟩6 DEF *Inv*
⟨5⟩2.CASE $i = self \land j = oth$
⟨6⟩1. $\forall n \in Nat : n \in Range(q[self][oth]) \equiv n \in Range(q'[self][oth])$
BY ONLY $q[self][oth] \in Seq(Nat \cup \{ack\})$, ⟨4⟩1, *ackNotNat*, *AppendProperties*
⟨6⟩2. $ack \in Range(q[oth][self]) \equiv ack \in Range(q'[oth][self])$
BY ⟨3⟩4, ⟨4⟩1, *ackNotNat*, *RangeHeadTail*
⟨6⟩3. UNCHANGED $localNum[oth][self]$
BY ⟨3⟩4, *POP_except*
⟨6⟩.QED BY ⟨5⟩1, ⟨5⟩2, ⟨6⟩1, ⟨6⟩2, ⟨6⟩3, *Zenon*
⟨5⟩3.CASE $i = oth \land j = self$
⟨6⟩1. $\land\ pc[\langle oth,\ self\rangle] = \text{“L0”}$
$\land\ pc[\langle oth\rangle] = \text{“L”}$
$\land\ ackRcvd[oth][self] = 0$
BY ⟨5⟩1, ⟨5⟩3, ⟨4⟩b
⟨6⟩2. $\land\ number[oth] \notin Range(q'[oth][self])$
$\land\ 0 \notin Range(q'[oth][self])$
⟨7⟩.ASSUME $v \in Range(Tail(q[oth][self]))$
PROVE FALSE
⟨8⟩1. PICK $k \in 1 \,..\, Len(Tail(q[oth][self])) : Tail(q[oth][self])[k] = v$
BY DEF *Range*
⟨8⟩2. $k + 1 \in 1 \,..\, Len(q[oth][self]) \land q[oth][self][k + 1] = v$
BY ⟨8⟩1
⟨8⟩.QED BY ⟨8⟩2 DEF *Inv*, *OtherProcs*
⟨7⟩.QED BY ⟨4⟩a, ⟨4⟩d, ⟨4⟩1, *RangeHeadTail*
⟨6⟩3. $ack \in Range(q'[self][oth])$
BY ⟨4⟩1, *AppendProperties*, *Isa*
⟨6⟩4. $localNum'[self][oth] = number[oth]$
BY ⟨4⟩a, *POP_except*, *Isa* DEF *OtherProcs*
⟨6⟩.QED BY ⟨5⟩3, ⟨6⟩1, ⟨6⟩2, ⟨6⟩3, ⟨6⟩4
⟨5⟩4.CASE $\neg(i = self \land j = oth) \land \neg(i = oth \land j = self)$
⟨6⟩.UNCHANGED $\langle q[i][j],\ q[j][i]\rangle$
BY ONLY ⟨4⟩1, ⟨5⟩4 DEF *OtherProcs*
⟨6⟩.QED BY ⟨5⟩1, ⟨5⟩4, *POP_except* DEF *OtherProcs*
⟨5⟩.QED BY ⟨5⟩2, ⟨5⟩3, ⟨5⟩4
⟨4⟩7. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
NEW $k \in 1 \,..\, Len(q'[i][j])$, NEW $l \in 1 \,..\, Len(q'[i][j])$
PROVE $Inv!4!(i)!(j)!(k,\ l)'$
⟨5⟩0. $Inv!4!(i)!(j)$
BY DEF *Inv*

⟨5⟩1. CASE $i = self \land j = oth$
⟨6⟩1. $\forall\, n \in 1 \,..\, Len(q'[self][oth]) :$
$q'[self][oth][n] \in Nat \Rightarrow \land\, n \in 1 \,..\, Len(q[self][oth])$
$\land\, q[self][oth][n] = q'[self][oth][n]$
BY ONLY $q[self][oth] \in Seq(Nat \cup \{ack\})$, ⟨4⟩1, *ackNotNat*
⟨6⟩2. ASSUME NEW $n \in 1 \,..\, Len(q'[self][oth])$, $q'[self][oth][n] = ack$
PROVE $n = Len(q'[self][oth])$
⟨7⟩1. $ack \notin Range(q[self][oth])$
BY ⟨3⟩4, ⟨4⟩a, ⟨4⟩b, *Zenon* DEF *Inv*, *OtherProcs*
⟨7⟩. QED BY ONLY $q[self][oth] \in Seq(Nat \cup \{ack\})$, ⟨4⟩1, ⟨6⟩2, ⟨7⟩1 DEF *Range*
⟨6⟩3. $Len(q'[self][oth]) = Len(q[self][oth]) + 1$
BY ⟨4⟩1
⟨6⟩4. ASSUME $q'[self][oth][k] = q'[self][oth][l]$
PROVE $k = l$
⟨7⟩1. CASE $q'[self][oth][k] \in Nat$
BY ONLY ⟨5⟩0, ⟨5⟩1, ⟨6⟩1, ⟨6⟩4, ⟨7⟩1
⟨7⟩2. CASE $q'[self][oth][k] = ack$
BY ONLY ⟨5⟩1, ⟨6⟩2, ⟨6⟩4, ⟨7⟩2, *Zenon*
⟨7⟩. QED BY ONLY ⟨7⟩1, ⟨7⟩2, ⟨4⟩1, ⟨5⟩1, *POP_access* DEF *OtherProcs*
⟨6⟩5. ASSUME $q'[self][oth][k] \in Nat \setminus \{0\}$
PROVE $q'[self][oth][k] = number[self]$
BY ONLY ⟨5⟩0, ⟨5⟩1, ⟨6⟩1, ⟨6⟩5
⟨6⟩6. ASSUME $q'[self][oth][k] = 0$, $q'[self][oth][l] \in Nat \setminus \{0\}$
PROVE $k < l$
BY ONLY ⟨5⟩0, ⟨5⟩1, ⟨6⟩1, ⟨6⟩6
⟨6⟩. QED BY ⟨5⟩1, ⟨6⟩4, ⟨6⟩5, ⟨6⟩6
⟨5⟩2. CASE $i = oth \land j = self$
⟨6⟩1. $q'[oth][self] = Tail(q[oth][self])$
BY ⟨4⟩1
⟨6⟩2. $\land\, k + 1 \in 1 \,..\, Len(q[oth][self]) \land q'[oth][self][k] = q[oth][self][k + 1]$
$\land\, l + 1 \in 1 \,..\, Len(q[oth][self]) \land q'[oth][self][l] = q[oth][self][l + 1]$
BY ONLY $q[oth][self] \in Seq(Nat \cup \{ack\})$, ⟨5⟩2, ⟨6⟩1
⟨6⟩. QED BY ⟨5⟩0, ⟨5⟩2, ⟨6⟩2
⟨5⟩3. CASE $\neg(i = self \land j = oth) \land \neg(i = oth \land j = self)$
⟨6⟩. $q'[i][j] = q[i][j]$
BY ONLY ⟨4⟩1, ⟨5⟩3 DEF *OtherProcs*
⟨6⟩. QED BY ⟨5⟩0, *Zenon*
⟨5⟩. QED BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3, *Zenon*
⟨4⟩. QED BY ONLY ⟨3⟩1, ⟨4⟩5, ⟨4⟩6, ⟨4⟩7 DEF *Inv*
⟨3⟩. QED BY ⟨3⟩2, ⟨3⟩3, ⟨3⟩4 DEF *FullTypeOK*, *POP*, *PFunc*, *OtherProcs*
⟨2⟩11. CASE UNCHANGED *vars*
BY ⟨2⟩11 DEF *Inv*, *vars*
⟨2⟩12. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9, ⟨2⟩10, ⟨2⟩11
DEF *Next*, *ProcIds*, *SubProcs*, *MsgProcs*, *main*, *sub*

$\langle 1 \rangle$.QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, *Typing*, *PTL* DEF *Spec*

The following operators define the refinement mapping.

$$
\begin{array}{l}
DecLN \triangleq \quad \text{value to substitute for } localNumber \\
\quad [i \in Procs \mapsto [j \in OtherProcs(i) \mapsto \\
\quad\ \text{IF } number[j] \in Range(q[j][i]) \text{ THEN } qm \\
\quad\ \text{ELSE } localNum[i][j] \\
\quad]]
\end{array}
$$

$$DecProcSet \triangleq ProcIds \cup SubProcs \cup WrProcs$$

$$
\begin{array}{l}
DecPC \triangleq \quad PC \text{ value of the deconstructed Bakery algorithm} \\
\quad [self \in DecProcSet \mapsto \\
\qquad \text{IF } self \in ProcIds \text{ THEN } pc[self] \\
\qquad\ \text{ELSE IF } self \in SubProcs \\
\qquad\ \text{THEN IF } pc[self] = \text{“L0”} \\
\qquad\qquad\ \text{THEN IF } pc[\langle self[1] \rangle] = \text{“L”} \wedge DecLN[self[2]][self[1]] = number[self[1]] \\
\qquad\qquad\qquad\ \text{THEN “Lb” ELSE “test”} \\
\qquad\qquad\ \text{ELSE } pc[self] \\
\qquad\ \text{ELSE “wr”}]
\end{array}
$$

LEMMA $DecLN\_type \triangleq$
$FullTypeOK \Rightarrow DecLN \in POP(Nat \cup \{qm\})$
$\langle 1 \rangle$.DEFINE $s(i, j) \triangleq$ IF $number[j] \in Range(q[j][i])$ THEN qm
ELSE $localNum[i][j]$
$\langle 1 \rangle .FullTypeOK \Rightarrow \forall\, i \in Procs : \forall\, j \in OtherProcs(i) : s(i, j) \in Nat \cup \{qm\}$
BY POP_access DEF $FullTypeOK$, $OtherProcs$
$\langle 1 \rangle$.QED BY $POP\_construct$, *Isa* DEF $DecLN$

Instantiation of the high-level spec for the refinement mapping.

$$
\begin{array}{l}
Dec \triangleq \text{INSTANCE } BakeryDeconstructedAtomic \\
\qquad\ \text{WITH } localNum \leftarrow DecLN,\ pc \leftarrow DecPC
\end{array}
$$

$$DecSafety \triangleq Dec!Init \wedge \Box[Dec!Next]_{(Dec!vars)}$$

LEMMA $DecEqualities \triangleq$
$\wedge\, Dec!Procs = Procs$
$\wedge\, Dec!ProcSet = DecProcSet$
$\wedge\, Dec!ProcIds = ProcIds$
$\wedge\, Dec!SubProcs = SubProcs$
$\wedge\, Dec!WrProcs = WrProcs$
$\wedge\, \forall\, p : Dec!SubProcsOf(p) = SubProcsOf(p)$
$\wedge\, \forall\, p : Dec!OtherProcs(p) = OtherProcs(p)$
$\wedge\, \forall\, x, y : Dec! \ll (x, y) \gg = \ll (x, y) \gg$

$\land \forall\, x,\, y : Dec!Max(x,\, y) = Max(x,\, y)$
$\land\, Dec!qm = qm$
BY DEF $Dec!Procs$, $Procs$, $Dec!ProcSet$, $DecProcSet$, $Dec!ProcIds$, $Dec!SubProcs$, $Dec!WrProcs$, $ProcIds$, $SubProcs$, $WrProcs$, $Dec!SubProcsOf$, $SubProcsOf$, $Dec!OtherProcs$, $OtherProcs$, $Dec!\ll$, $\ll$, $Dec!Max$, Max, $Dec!qm$, qm

---

Proof of refinement (safety part).

THEOREM $Refinement \triangleq Spec \Rightarrow DecSafety$
⟨1⟩1. $Init \Rightarrow Dec!Init$
⟨2⟩.SUFFICES ASSUME $Init$PROVE $Dec!Init$
OBVIOUS
⟨2⟩1. $number = [i \in Procs \mapsto 0]$
BY DEF $Init$
⟨2⟩2. $DecLN = [i \in Procs \mapsto [j \in OtherProcs(i) \mapsto 0]]$
BY DEF $Init$, $DecLN$, $Range$, $OtherProcs$
⟨2⟩3. $localCh = [i \in Procs \mapsto [j \in OtherProcs(i) \mapsto 0]]$
BY DEF $Init$
⟨2⟩4. $DecPC = [self \in DecProcSet \mapsto$ CASE $self \in ProcIds \to$ "ncs"
$\square self \in SubProcs \to$ "ch"
$\square self \in WrProcs \to$ "wr"$]$
BY $DisjointIds$ DEF $Init$, $ProcSet$, $DecPC$, $DecProcSet$
⟨2⟩.QED BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, $DecEqualities$ DEF $Dec!Init$
⟨1⟩2. $\land\, FullTypeOK \land DecLN \in POP(Nat \cup \{qm\}) \land (DecLN \in POP(Nat \cup \{qm\}))'$
$\land\, Inv \land Inv'$
$\land\, [Next]_{vars}$
$\Rightarrow [Dec!Next]_{(Dec!vars)}$
⟨2⟩ SUFFICES ASSUME $FullTypeOK$, $DecLN \in POP(Nat \cup \{qm\})$, $DecLN' \in POP(Nat \cup \{qm\})$, Inv, Inv', $[Next]_{vars}$
PROVE $[Dec!Next]_{(Dec!vars)}$
OBVIOUS
⟨2⟩.USE DEF $FullTypeOK$
⟨2⟩1. ASSUME NEW $self \in Procs$, $ncs(\langle self \rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$
⟨3⟩.$\langle self \rangle \in ProcIds$
BY DEF $ProcIds$
⟨3⟩1. $DecPC[\langle self \rangle] =$ "ncs"
BY ⟨2⟩1, $DisjointIds$ DEF ncs, $DecPC$, $DecProcSet$
⟨3⟩2. UNCHANGED $\langle number,\, DecLN,\, localCh \rangle$
BY ⟨2⟩1 DEF ncs, $DecLN$
⟨3⟩3. $DecPC' = [DecPC$ EXCEPT $![\langle self \rangle] =$ "M"$]$
⟨4⟩.DEFINE $exc \triangleq [DecPC$ EXCEPT $![\langle self \rangle] =$ "M"$]$

⟨4⟩1. ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = exc[p]$
BY ⟨2⟩1, ⟨3⟩2, *DisjointIds* DEF ncs, $DecPC$, $DecProcSet$, $ProcSet$
⟨4⟩.QED BY ⟨4⟩1, *Zenon* DEF $DecPC$
⟨3⟩4. $Dec!ncs(\langle self \rangle)$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF $Dec!ncs$
⟨3⟩.QED BY ⟨3⟩4, *DecEqualities* DEF $Dec!Next$, $Dec!main$, $ProcIds$
⟨2⟩2. ASSUME NEW $self \in Procs$,
$M(\langle self \rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$
⟨3⟩. $\wedge \langle self \rangle \in ProcIds$
BY DEF $ProcIds$
⟨3⟩.PICK $v \in Nat \setminus \{0\}$:
$\wedge$ $pc[\langle self \rangle] =$ "M"
$\wedge$ $\forall j \in OtherProcs(self) : pc[\langle self, j \rangle] =$ "L0"
$\wedge$ $\forall j \in OtherProcs(self) : v > localNum[self][j]$
$\wedge$ $number' = [number$ EXCEPT $![self] = v]$
$\wedge$ $q' = [q$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto Append(q[self][j], v)]]$
$\wedge$ $pc' = [pc$ EXCEPT $![\langle self \rangle] =$ "L"$]$
$\wedge$ UNCHANGED $\langle localNum, localCh, ackRcvd \rangle$
BY ⟨2⟩2, *SubProcsOfEquality*, *Isa* DEF M, $OtherProcs$
⟨3⟩1. $DecPC[\langle self \rangle] =$ "M"
BY *DisjointIds* DEF $DecPC$, $DecProcSet$
⟨3⟩2. $\forall p \in Dec!SubProcsOf(self) : DecPC[p] =$ "test"
BY *DecEqualities*, *DisjointIds* DEF $SubProcsOf$, $SubProcs$, $OtherProcs$, $DecPC$, $DecProcSet$
⟨3⟩3. $\forall j \in OtherProcs(self) : DecLN[self][j] \neq qm \Rightarrow v > DecLN[self][j]$
BY DEF $DecLN$, $OtherProcs$
⟨3⟩4. $DecLN' = [j \in Procs \mapsto [i \in OtherProcs(j) \mapsto$
IF $i = self$ THEN qm ELSE $DecLN[j][i]]]$
⟨4⟩.SUFFICES ASSUME NEW $j \in Procs$, NEW $i \in OtherProcs(j)$
PROVE $DecLN'[j][i] =$ IF $i = self$ THEN qm ELSE $DecLN[j][i]$
BY *Zenon* DEF $DecLN$, $OtherProcs$
⟨4⟩1.CASE $i = self$
⟨5⟩.DEFINE $g(x, y) \triangleq Append(q[x][y], v)$
⟨5⟩1. $j \in OtherProcs(self)$
BY ⟨4⟩1 DEF $OtherProcs$
⟨5⟩2. $q[self][j] \in Seq(Nat \cup \{ack\})$
BY ⟨4⟩1, POP_access DEF $OtherProcs$
⟨5⟩3. $\forall oth \in OtherProcs(self)$:
$\wedge q[self][oth] \in Seq(Nat \cup \{ack\})$
$\wedge g(self, oth) \in Seq(Nat \cup \{ack\})$
BY ⟨4⟩1, POP_access
⟨5⟩4. $q'[self][j] = g(self, j)$
⟨6⟩1. $q' = [q$ EXCEPT $![self] = [oth \in OtherProcs(self) \mapsto g(self, oth)]]$
OBVIOUS

⟨6⟩.HIDE DEF g
⟨6⟩.QED
BY ONLY ⟨5⟩1, ⟨5⟩3, ⟨6⟩1, *POP_except_fun_value*, *FullTypeOK*, *IsaM*("blast")
⟨5⟩5. $number'[self] \in Range(q'[self][j])$
BY ⟨5⟩2, ⟨5⟩4, *Isa* DEF *Range*
⟨5⟩.QED BY ⟨4⟩1, ⟨5⟩2, ⟨5⟩5 DEF *DecLN*, *OtherProcs*
⟨4⟩2.CASE $i \neq self$
BY ⟨4⟩2 DEF *DecLN*, *OtherProcs*
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
⟨3⟩5. $DecPC' = [DecPC \text{ EXCEPT } ![\langle self \rangle] = \text{"L"}]$
⟨4⟩.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = \text{IF } p = \langle self \rangle \text{ THEN "L" ELSE } DecPC[p]$
BY *Zenon* DEF *DecPC*
⟨4⟩2.CASE $p \in ProcIds$
BY ⟨4⟩2 DEF *DecPC*, *ProcSet*
⟨4⟩3.CASE $p \in SubProcs$
⟨5⟩.$p \notin ProcIds$
BY ⟨4⟩3, *DisjointIds*
⟨5⟩.UNCHANGED $pc[p]$
BY DEF *ProcSet*
⟨5⟩1.CASE $p[1] = self$
⟨6⟩1. PICK $oth \in OtherProcs(self) : p = \langle self, oth \rangle$
BY ⟨4⟩3, ⟨5⟩1 DEF *SubProcs*, *OtherProcs*
⟨6⟩2. $DecPC[p] = \text{"test"}$
BY ⟨4⟩3, ⟨6⟩1 DEF *DecPC*
⟨6⟩3. $DecLN'[oth][self] = qm$
BY ⟨3⟩4 DEF *OtherProcs*
⟨6⟩4. $DecPC'[p] = \text{"test"}$
BY ⟨4⟩3, ⟨6⟩1, ⟨6⟩3, *qmNotNat*, *Zenon* DEF *DecPC*
⟨6⟩.QED BY ⟨6⟩2, ⟨6⟩4
⟨5⟩2.CASE $p[1] \neq self$
⟨6⟩1. UNCHANGED $\langle DecLN[p[2]][p[1]], number[p[1]] \rangle$
BY ⟨3⟩4, ⟨4⟩3, ⟨5⟩2 DEF *SubProcs*, *OtherProcs*
⟨6⟩2. UNCHANGED $pc[\langle p[1] \rangle]$
BY ⟨4⟩3, ⟨5⟩2 DEF *SubProcs*, *ProcSet*
⟨6⟩.QED BY ⟨4⟩3, ⟨6⟩1, ⟨6⟩2, *DisjointIds* DEF *DecPC*
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2
⟨4⟩4.CASE $p \in WrProcs$
BY ⟨4⟩4, *DisjointIds* DEF *DecPC*
⟨4⟩.QED BY ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 DEF *DecProcSet*
⟨3⟩6. $Dec!M(\langle self \rangle)$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, *DecEqualities*, *Zenon* DEF $Dec!M$
⟨3⟩.QED BY ⟨3⟩6, *DecEqualities* DEF $Dec!Next$, $Dec!main$
⟨2⟩3. ASSUME NEW $self \in Procs$,
$L(\langle self \rangle)$

PROVE $[Dec!Next]_{(Dec!vars)}$

$\langle 3\rangle$. $\wedge\ pc[\langle self\rangle] = \text{“L”}$
$\wedge\ \forall\, oth \in OtherProcs(self) : pc[\langle self,\ oth\rangle] = \text{“ch”}$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self\rangle] = \text{“cs”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ localCh,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 3$ DEF L, $SubProcsOf$, $SubProcs$, $OtherProcs$

$\langle 3\rangle.\langle self\rangle \in ProcIds$
BY DEF $ProcIds$

$\langle 3\rangle 1$. $DecPC[\langle self\rangle] = \text{“L”}$
BY DEF $DecPC$, $DecProcSet$

$\langle 3\rangle 2$. $\forall\, p \in SubProcsOf(self) : DecPC[p] = \text{“ch”}$
BY DEF $SubProcsOf$, $SubProcs$, $OtherProcs$, $DecPC$, $DecProcSet$

$\langle 3\rangle 3$. UNCHANGED $DecLN$
BY DEF $DecLN$

$\langle 3\rangle 4$. $DecPC' = [DecPC \text{ EXCEPT } ![\langle self\rangle] = \text{“cs”}]$
$\langle 4\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = \text{IF } p = \langle self\rangle \text{ THEN “cs” ELSE } DecPC[p]$
BY *Zenon* DEF $DecPC$

$\langle 4\rangle 1$.CASE $p \in ProcIds$
BY $\langle 4\rangle 1$ DEF $DecPC$, $ProcSet$

$\langle 4\rangle 2$.CASE $p \in SubProcs$
$\langle 5\rangle.p \notin ProcIds$
BY $\langle 4\rangle 2$, $DisjointIds$
$\langle 5\rangle$.UNCHANGED $pc[p]$
BY DEF $ProcSet$
$\langle 5\rangle 1$.CASE $p[1] = self$
BY $\langle 4\rangle 2$, $\langle 5\rangle 1$ DEF $SubProcs$, $OtherProcs$, $DecPC$
$\langle 5\rangle 2$.CASE $p[1] \neq self$
BY $\langle 4\rangle 2$, $\langle 5\rangle 2$, $\langle 3\rangle 3$ DEF $DecPC$, $SubProcs$, $ProcSet$
$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 3$.CASE $p \in WrProcs$
BY $\langle 4\rangle 3$, $DisjointIds$ DEF $DecPC$

$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $DecProcSet$

$\langle 3\rangle 5$. $Dec!L(\langle self\rangle)$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $DecEqualities$ DEF $Dec!L$

$\langle 3\rangle$.QED BY $\langle 3\rangle 5$, $DecEqualities$ DEF $Dec!Next$, $Dec!main$

$\langle 2\rangle 4$. ASSUME NEW $self \in Procs$,
$cs(\langle self\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$

$\langle 3\rangle$. $\wedge\ pc[\langle self\rangle] = \text{“cs”}$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self\rangle] = \text{“P”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ localCh,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 4$ DEF cs

$\langle 3\rangle.\langle self\rangle \in ProcIds$
BY DEF $ProcIds$

⟨3⟩1. $DecPC[\langle self \rangle] =$ "cs"
BY DEF $DecPC$, $DecProcSet$
⟨3⟩2. UNCHANGED $DecLN$
BY DEF $DecLN$
⟨3⟩3. $DecPC' = [DecPC$ EXCEPT $![\langle self \rangle] =$ "P"$]$
⟨4⟩.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] =$ IF $p = \langle self \rangle$ THEN "P" ELSE $DecPC[p]$
BY *Zenon* DEF $DecPC$
⟨4⟩1.CASE $p \in ProcIds$
BY ⟨4⟩1 DEF $DecPC$, $ProcSet$
⟨4⟩2.CASE $p \in SubProcs$
⟨5⟩.$p \notin ProcIds$
BY ⟨4⟩2, $DisjointIds$
⟨5⟩.UNCHANGED $pc[p]$
BY DEF $ProcSet$
⟨5⟩1.CASE $p[1] = self$
BY ⟨4⟩2, ⟨5⟩1 DEF $SubProcs$, $DecPC$
⟨5⟩2.CASE $p[1] \neq self$
BY ⟨4⟩2, ⟨5⟩2, ⟨3⟩2 DEF $DecPC$, $SubProcs$, $ProcSet$
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2
⟨4⟩3.CASE $p \in WrProcs$
BY ⟨4⟩3, $DisjointIds$ DEF $DecPC$
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF $DecProcSet$
⟨3⟩4. $Dec!cs(\langle self \rangle)$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, $DecEqualities$ DEF $Dec!cs$
⟨3⟩.QED BY ⟨3⟩4, $DecEqualities$ DEF $Dec!Next$, $Dec!main$
⟨2⟩5. ASSUME NEW $self \in Procs$,
$P(\langle self \rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$
⟨3⟩. $\wedge\ pc[\langle self \rangle] =$ "P"
$\wedge\ number' = [number$ EXCEPT $![self] = 0]$
$\wedge\ q' = [q$ EXCEPT $![self] = [j \in OtherProcs(self) \mapsto Append(q[self][j], 0)]]$
$\wedge\ pc' = [pc$ EXCEPT $![\langle self \rangle] =$ "ncs"$]$
$\wedge$ UNCHANGED $\langle localNum, localCh \rangle$
BY ⟨2⟩5 DEF P
⟨3⟩.$\langle self \rangle \in ProcIds$
BY DEF $ProcIds$
⟨3⟩1. $DecPC[\langle self \rangle] =$ "P"
BY DEF $DecPC$, $DecProcSet$
⟨3⟩2. $DecLN' = [j \in Procs \mapsto [i \in OtherProcs(j) \mapsto$
IF $i = self$ THEN qm ELSE $DecLN[j][i]]]$
⟨4⟩.SUFFICES ASSUME NEW $j \in Procs$, NEW $i \in OtherProcs(j)$
PROVE $DecLN'[j][i] =$ IF $i = self$ THEN qm ELSE $DecLN[j][i]$
BY *Zenon* DEF $DecLN$
⟨4⟩1.CASE $i = self$

⟨5⟩.DEFINE $g(x,\ y) \triangleq Append(q[x][y],\ 0)$
⟨5⟩1. $j \in OtherProcs(self)$
BY ⟨4⟩1 DEF $OtherProcs$
⟨5⟩2. $q[self][j] \in Seq(Nat \cup \{ack\})$
BY ⟨4⟩1, POP_access DEF $OtherProcs$
⟨5⟩3. $\forall\, oth \in OtherProcs(self) :$
$\land\ q[self][oth] \in Seq(Nat \cup \{ack\})$
$\land\ g(self,\ oth) \in Seq(Nat \cup \{ack\})$
BY ⟨4⟩1, POP_access
⟨5⟩4. $q'[self][j] = g(self,\ j)$
⟨6⟩1. $q' = [q$ EXCEPT $![self] = [oth \in OtherProcs(self) \mapsto g(self,\ oth)]]$
OBVIOUS
⟨6⟩.HIDE DEF g
⟨6⟩.QED
BY ONLY ⟨5⟩1, ⟨5⟩3, ⟨6⟩1, $POP\_except\_fun\_value$, $FullTypeOK$, $IsaM(\text{“blast”})$
⟨5⟩5. $number'[self] \in Range(q'[self][j])$
BY ⟨5⟩2, ⟨5⟩4, Isa DEF $Range$
⟨5⟩.QED BY ⟨4⟩1, ⟨5⟩2, ⟨5⟩5 DEF $DecLN$, $OtherProcs$
⟨4⟩2.CASE $i \neq self$
BY ⟨4⟩2 DEF $DecLN$, $OtherProcs$
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
⟨3⟩3. $DecPC' = [DecPC$ EXCEPT $![\langle self \rangle] =$ “ncs”$]$
⟨4⟩.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] =$ IF $p = \langle self \rangle$ THEN “ncs” ELSE $DecPC[p]$
BY $Zenon$ DEF $DecPC$
⟨4⟩1.CASE $p \in ProcIds$
BY ⟨4⟩1 DEF $DecPC$, $ProcSet$
⟨4⟩2.CASE $p \in SubProcs$
⟨5⟩.$p \notin ProcIds$
BY ⟨4⟩2, $DisjointIds$
⟨5⟩.UNCHANGED $pc[p]$
BY DEF $ProcSet$
⟨5⟩1.CASE $p[1] = self$
BY ⟨4⟩2, ⟨5⟩1, $Zenon$ DEF $SubProcs$, $OtherProcs$, $DecPC$
⟨5⟩2.CASE $p[1] \neq self$
⟨6⟩.UNCHANGED $pc[\langle p[1] \rangle]$
BY ⟨5⟩2 DEF $SubProcs$, $ProcSet$
⟨6⟩.UNCHANGED $DecLN[p[2]][p[1]]$
BY ⟨5⟩2, ⟨4⟩2, ⟨3⟩2 DEF $SubProcs$, $OtherProcs$
⟨6⟩.QED BY DEF $DecPC$, $DecProcSet$
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2
⟨4⟩3.CASE $p \in WrProcs$
BY ⟨4⟩3, $DisjointIds$ DEF $DecPC$
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3 DEF $DecProcSet$
⟨3⟩4. $Dec!P(\langle self \rangle)$

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *DecEqualities* DEF $Dec!P$

$\langle 3\rangle$.QED BY $\langle 3\rangle 4$, *DecEqualities* DEF $Dec!Next$, $Dec!main$

$\langle 2\rangle 6$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$ch(\langle self,\ oth\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$

$\langle 3\rangle$. $\wedge\ pc[\langle self,\ oth\rangle] = \text{“ch”}$
$\wedge\ pc[\langle self\rangle] = \text{“M”}$
$\wedge\ localCh' = [localCh \text{ EXCEPT } ![oth][self] = 1]$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“L0”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 6$ DEF ch

$\langle 3\rangle.\langle self,\ oth\rangle \in SubProcs \setminus ProcIds$
BY DEF $SubProcs$, $ProcIds$, $OtherProcs$

$\langle 3\rangle 1$. $DecPC[\langle self,\ oth\rangle] = \text{“ch”}$
BY DEF $DecPC$, $DecProcSet$

$\langle 3\rangle 2$. $DecPC[\langle self\rangle] = \text{“M”}$
BY DEF $DecPC$, $DecProcSet$, $ProcIds$

$\langle 3\rangle 3$. UNCHANGED $DecLN$
BY DEF $DecLN$

$\langle 3\rangle 4$. $DecPC' = [DecPC \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“test”}]$
$\langle 4\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = \text{IF } p = \langle self,\ oth\rangle \text{ THEN “test” ELSE } DecPC[p]$
BY *Zenon* DEF $DecPC$
$\langle 4\rangle$.QED BY $\langle 3\rangle 3$, *DisjointIds* DEF $DecPC$, $DecProcSet$, $ProcIds$, $ProcSet$

$\langle 3\rangle 5$. $Dec!ch(\langle self,\ oth\rangle)$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, *DecEqualities* DEF $Dec!ch$

$\langle 3\rangle$.QED BY $\langle 3\rangle 5$, *DecEqualities* DEF $Dec!Next$, $Dec!sub$

$\langle 2\rangle 7$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L0(\langle self,\ oth\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$

$\langle 3\rangle$. $\wedge\ pc[\langle self,\ oth\rangle] = \text{“L0”}$
$\wedge\ pc[\langle self\rangle] = \text{“L”}$
$\wedge\ ackRcvd[self][oth] = 1$
$\wedge\ localCh' = [localCh \text{ EXCEPT } ![oth][self] = 0]$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“L2”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 7$ DEF $L0$

$\langle 3\rangle.\langle self,\ oth\rangle \in SubProcs \setminus ProcIds$
BY DEF $SubProcs$, $ProcIds$, $OtherProcs$

$\langle 3\rangle 1$. $DecPC[\langle self,\ oth\rangle] = \text{“Lb”}$
BY DEF Inv, $DecPC$, $DecProcSet$, $DecLN$, $ProcSet$, $OtherProcs$

$\langle 3\rangle 2$. UNCHANGED $DecLN$
BY DEF $DecLN$

$\langle 3\rangle 3$. $DecPC' = [DecPC \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“L2”}]$
$\langle 4\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$

PROVE $DecPC'[p] = \text{IF } p = \langle self,\ oth\rangle \text{ THEN } \text{“L2”} \text{ ELSE } DecPC[p]$
BY *Zenon* DEF *DecPC*
$\langle 4\rangle$.QED BY $\langle 3\rangle 2$, *DisjointIds* DEF *DecPC*, *DecProcSet*, *ProcIds*, *ProcSet*
$\langle 3\rangle 4$. $Dec!Lb(\langle self,\ oth\rangle)$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *DecEqualities* DEF $Dec!Lb$
$\langle 3\rangle$.QED BY $\langle 3\rangle 4$, *DecEqualities* DEF $Dec!Next$, $Dec!sub$
$\langle 2\rangle 8$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L2(\langle self,\ oth\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$
$\langle 3\rangle$. $\wedge\ pc[\langle self,\ oth\rangle] = \text{“L2”}$
$\wedge\ localCh[self][oth] = 0$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“L3”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ localCh,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 8$ DEF *L2*
$\langle 3\rangle$.$\langle self,\ oth\rangle \in SubProcs \setminus ProcIds$
BY DEF *SubProcs*, *ProcIds*, *OtherProcs*
$\langle 3\rangle 1$. $DecPC[\langle self,\ oth\rangle] = \text{“L2”}$
BY DEF *DecPC*, *DecProcSet*
$\langle 3\rangle 2$. UNCHANGED *DecLN*
BY DEF *DecLN*
$\langle 3\rangle 3$. $DecPC' = [DecPC \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“L3”}]$
$\langle 4\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = \text{IF } p = \langle self,\ oth\rangle \text{ THEN } \text{“L3”} \text{ ELSE } DecPC[p]$
BY *Zenon* DEF *DecPC*
$\langle 4\rangle$.QED BY $\langle 3\rangle 2$, *DisjointIds* DEF *DecPC*, *DecProcSet*, *ProcIds*, *ProcSet*
$\langle 3\rangle 4$. $Dec!L2(\langle self,\ oth\rangle)$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *DecEqualities* DEF $Dec!L2$
$\langle 3\rangle$.QED BY $\langle 3\rangle 4$, *DecEqualities* DEF $Dec!Next$, $Dec!sub$
$\langle 2\rangle 9$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L3(\langle self,\ oth\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$
$\langle 3\rangle$. $\wedge\ pc[\langle self,\ oth\rangle] = \text{“L3”}$
$\wedge\ \vee\ localNum[self][oth] = 0$
$\vee\ \langle number[self],\ self\rangle \ll \langle localNum[self][oth],\ oth\rangle$
$\wedge\ pc' = [pc \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“ch”}]$
$\wedge$ UNCHANGED $\langle number,\ localNum,\ localCh,\ ackRcvd,\ q\rangle$
BY $\langle 2\rangle 9$ DEF *L3*
$\langle 3\rangle$.$\langle self,\ oth\rangle \in SubProcs \setminus ProcIds$
BY DEF *SubProcs*, *ProcIds*, *OtherProcs*
$\langle 3\rangle 1$. $DecPC[\langle self,\ oth\rangle] = \text{“L3”}$
BY DEF *DecPC*, *DecProcSet*
$\langle 3\rangle$a. ASSUME $DecLN[self][oth] \notin \{0,\ qm\}$
PROVE $\langle number[self],\ self\rangle \ll \langle DecLN[self][oth],\ oth\rangle$
BY $\langle 3\rangle$a DEF *DecLN*
$\langle 3\rangle 2$. UNCHANGED *DecLN*

BY DEF $DecLN$

$\langle 3\rangle 3.\ DecPC' = [DecPC \text{ EXCEPT } ![\langle self,\ oth\rangle] = \text{“ch”}]$

$\langle 4\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] = \text{IF } p = \langle self,\ oth\rangle \text{ THEN “ch” ELSE } DecPC[p]$

BY *Zenon* DEF $DecPC$

$\langle 4\rangle$.QED BY $\langle 3\rangle 2$, *DisjointIds* DEF $DecPC$, $DecProcSet$, $ProcIds$, $ProcSet$

$\langle 3\rangle 4.\ Dec!L3(\langle self,\ oth\rangle)$

BY $\langle 3\rangle 1$, $\langle 3\rangle$a, $\langle 3\rangle 2$, $\langle 3\rangle 3$, *DecEqualities* DEF $Dec!L3$

$\langle 3\rangle$.QED BY $\langle 3\rangle 4$, *DecEqualities* DEF $Dec!Next$, $Dec!sub$

$\langle 2\rangle 10$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$msg(\langle self,\ oth,\ \text{“msg”}\rangle)$
PROVE $[Dec!Next]_{(Dec!vars)}$

$\langle 3\rangle.\ \wedge\ pc[\langle self,\ oth,\ \text{“msg”}\rangle] = \text{“wr”}$
$\wedge\ q[oth][self] \neq \langle\rangle$
$\wedge$ LET $v \triangleq Head(q[oth][self])$IN
$\wedge$ IF $v = ack$
THEN $\wedge\ ackRcvd' = [ackRcvd \text{ EXCEPT } ![self][oth] = 1]$
$\wedge$ UNCHANGED $localNum$
ELSE $\wedge\ localNum' = [localNum \text{ EXCEPT } ![self][oth] = v]$
$\wedge$ UNCHANGED $ackRcvd$
$\wedge$ IF $v \in \{0,\ ack\}$
THEN $q' = [q \text{ EXCEPT } ![oth][self] = Tail(q[oth][self])]$
ELSE $q' = [q \text{ EXCEPT } ![oth][self] = Tail(q[oth][self]),$
$![self][oth] = Append(q[self][oth],\ ack)]$
$\wedge$ UNCHANGED $\langle pc,\ number,\ localCh\rangle$

BY $\langle 2\rangle 10$ DEF msg, wr

$\langle 3\rangle$.DEFINE $v \triangleq Head(q[oth][self])$

$\langle 3\rangle 1$.CASE $v = ack$

$\langle 4\rangle 1$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $number'[j] \in Range(q'[j][i]) \equiv number[j] \in Range(q[j][i])$

$\langle 5\rangle 1$.CASE $i = self \wedge j = oth$

$\langle 6\rangle$.$q[j][i] \in Seq(Nat \cup \{ack\})$
BY *POP_access* DEF $OtherProcs$

$\langle 6\rangle 1.\ q'[j][i] = Tail(q[j][i])$
BY $\langle 3\rangle 1$, $\langle 5\rangle 1$, *Isa* DEF POP, $PFunc$, $OtherProcs$

$\langle 6\rangle 4.\ Range(q'[j][i]) \cup \{ack\} = Range(q[j][i])$
BY $\langle 3\rangle 1$, $\langle 5\rangle 1$, $\langle 6\rangle 1$, *RangeHeadTail*

$\langle 6\rangle 5.\ number[j] \neq ack$
BY *ackNotNat* DEF $OtherProcs$

$\langle 6\rangle$.QED BY $\langle 6\rangle 4$, $\langle 6\rangle 5$

$\langle 5\rangle 2$.CASE $\neg(i = self \wedge j = oth)$
BY $\langle 3\rangle 1$, $\langle 5\rangle 2$ DEF POP, $PFunc$, $OtherProcs$

$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 2$. UNCHANGED $DecLN$
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$ DEF $DecLN$

⟨4⟩3. UNCHANGED $DecPC$
BY ⟨4⟩2 DEF $DecPC$
⟨4⟩4. UNCHANGED $Dec!vars$
BY ⟨4⟩2, ⟨4⟩3 DEF $Dec!vars$
⟨4⟩.QED BY ⟨4⟩4
⟨3⟩2.CASE $v = 0 \land number[oth] = 0$
⟨4⟩.$\langle oth,\ self,\ \text{“wr”}\rangle \in WrProcs \setminus (ProcIds \cup SubProcs)$
BY $DisjointIds$ DEF $WrProcs$, $OtherProcs$
⟨4⟩1. $DecPC[\langle oth,\ self,\ \text{“wr”}\rangle] = \text{“wr”}$
BY DEF $DecPC$, $DecProcSet$
⟨4⟩2. $DecLN[self][oth] = qm$
BY ⟨3⟩2, POP_access, $RangeHeadTail$ DEF $DecLN$, $OtherProcs$
⟨4⟩3. $\land\ pc[\langle oth\rangle] \in \{\text{“ncs”},\ \text{“M”}\}$
$\land\ DecPC[\langle oth\rangle] = pc[\langle oth\rangle]$
BY ⟨3⟩2 DEF $DecPC$, $DecProcSet$, Inv, $OtherProcs$, $ProcIds$
⟨4⟩4. $DecLN' = [DecLN$ EXCEPT $![self][oth] = 0]$
Can the proof of this step be simplified?
⟨5⟩1. SUFFICES ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $DecLN'[i][j] =$ IF $i = self \land j = oth$ THEN 0 ELSE $DecLN[i][j]$
BY POP_except_equal, Isa
⟨5⟩2. $q' = [q$ EXCEPT $![oth][self] = Tail(q[oth][self])]$
BY ⟨3⟩2
⟨5⟩3. $localNum' = [localNum$ EXCEPT $![self][oth] = 0]$
BY ⟨3⟩2, $ackNotNat$
⟨5⟩4.CASE $i = self \land j = oth$
⟨6⟩1. $q'[oth][self] = Tail(q[oth][self])$
BY ⟨5⟩2 DEF POP, $PFunc$, $OtherProcs$
⟨6⟩2. $\land\ 1 \in 1\ ..\ Len(q[oth][self])$
$\land\ number[oth] = q[oth][self][1]$
BY ⟨3⟩2
⟨6⟩.$q[oth][self] \in Seq(Nat \cup \{ack\})$
BY POP_access DEF $OtherProcs$
⟨6⟩3. ASSUME $number[oth] \in Range(Tail(q[oth][self]))$
PROVE FALSE
⟨7⟩.DEFINE $tl \triangleq Tail(q[oth][self])$
⟨7⟩1. PICK $k \in 1\ ..\ Len(tl) : tl[k] = number[oth]$
BY ⟨6⟩3 DEF $Range$
⟨7⟩2. $\land\ k + 1 \in 1\ ..\ Len(q[oth][self])$
$\land\ q[oth][self][k + 1] = number[oth]$
BY ⟨7⟩1
⟨7⟩3. $Inv!4!(oth)!(self)$
BY DEF Inv, $OtherProcs$
⟨7⟩.QED BY ⟨6⟩2, ⟨7⟩2, ⟨7⟩3
⟨6⟩.QED BY ⟨5⟩3, ⟨5⟩4, ⟨6⟩1, ⟨6⟩3 DEF $DecLN$, POP, $PFunc$
⟨5⟩5.CASE $\neg(i = self \land j = oth)$

BY $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 5$ DEF $DecLN$

$\langle 5\rangle$.QED BY $\langle 5\rangle 4$, $\langle 5\rangle 5$

$\langle 4\rangle 5$. $DecPC' = [DecPC$ EXCEPT $![\langle oth, self, \text{“wr”}\rangle] = \text{“wr”}]$

$\langle 5\rangle$.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] =$ IF $p = \langle oth, self, \text{“wr”}\rangle$ THEN “wr” ELSE $DecPC[p]$

BY *Zenon* DEF $DecPC$

$\langle 5\rangle 1$.CASE $p \in ProcIds$

BY $\langle 5\rangle 1$ DEF $DecPC$

$\langle 5\rangle 2$.CASE $p \in SubProcs$

$\langle 6\rangle$.PICK $i, j \in Procs : i \neq j \wedge p = \langle i, j\rangle$

BY $\langle 5\rangle 2$ DEF $SubProcs$

$\langle 6\rangle 1$. $DecPC[p] =$ IF $pc[p] =$ “L0”
THEN IF $pc[\langle i\rangle] =$ “L” $\wedge\ DecLN[j][i] = number[i]$
THEN “Lb” ELSE “test”
ELSE $pc[p]$

BY $\langle 5\rangle 2$, $DisjointIds$ DEF $DecPC$, $DecProcSet$

$\langle 6\rangle 2$. $DecPC'[p] =$ IF $pc[p] =$ “L0”
THEN IF $pc[\langle i\rangle] =$ “L” $\wedge\ DecLN'[j][i] = number[i]$
THEN “Lb” ELSE “test”
ELSE $pc[p]$

BY $\langle 5\rangle 2$, $DisjointIds$ DEF $DecPC$, $DecProcSet$

$\langle 6\rangle 3$. $pc[\langle i\rangle] =$ “L” $\Rightarrow DecLN'[j][i] = DecLN[j][i]$

BY $\langle 4\rangle 3$, $\langle 4\rangle 4$

$\langle 6\rangle$.QED BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$

$\langle 5\rangle 3$.CASE $p \in WrProcs$

BY $\langle 5\rangle 3$, $DisjointIds$ DEF $DecPC$

$\langle 5\rangle$.QED BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF $DecProcSet$

$\langle 4\rangle 6$. $Dec!wr(\langle oth, self, \text{“wr”}\rangle)$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$, $DecEqualities$ DEF $Dec!wr$

$\langle 4\rangle$.QED BY $\langle 4\rangle 6$, $DecEqualities$ DEF $Dec!Next$, $Dec!wrp$

$\langle 3\rangle 3$.CASE $v = 0 \wedge number[oth] \neq 0$

$\langle 4\rangle 1$. $\wedge\ localNum' = [localNum$ EXCEPT $![self][oth] = 0]$
$\wedge\ q' = [q$ EXCEPT $![oth][self] = Tail(q[oth][self])]$

BY $\langle 3\rangle 3$, $ackNotNat$

$\langle 4\rangle 2$. UNCHANGED $DecLN$

$\langle 5\rangle$.SUFFICES ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $DecLN'[i][j] = DecLN[i][j]$

BY DEF $DecLN$

$\langle 5\rangle 1$.CASE $i = self \wedge j = oth$

$\langle 6\rangle 1$. $localNum'[self][oth] \neq number'[oth]$

BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, POP_except, Isa

$\langle 6\rangle 2$. $Inv!3!(oth)!(self)'$

BY DEF $OtherProcs$, Inv

$\langle 6\rangle 3$. $number'[oth] \in Range(q'[oth][self])$

BY $\langle 3\rangle 3$, $\langle 6\rangle 1$, $\langle 6\rangle 2$

⟨6⟩4. $\land\ q[oth][self] \in Seq(Nat \cup \{ack\})$
$\land\ Tail(q[oth][self]) \in Seq(Nat \cup \{ack\})$
BY POP_access DEF $OtherProcs$
⟨6⟩5. $q'[oth][self] = Tail(q[oth][self])$
BY ⟨4⟩1, ⟨6⟩4, $FullTypeOK$, POP_except, Isa DEF $OtherProcs$
⟨6⟩6. $number[oth] \in Range(q[oth][self])$
BY ⟨3⟩3, ⟨4⟩1, ⟨6⟩3, ⟨6⟩4, ⟨6⟩5, $RangeHeadTail$
⟨6⟩.QED BY ⟨5⟩1, ⟨6⟩3, ⟨6⟩6 DEF $DecLN$
⟨5⟩2.CASE $\neg(i = self \land j = oth)$
BY ⟨4⟩1, ⟨5⟩2 DEF $DecLN$
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2
⟨4⟩3. UNCHANGED $DecPC$
BY ⟨4⟩2 DEF $DecPC$
⟨4⟩.QED BY ⟨4⟩2, ⟨4⟩3 DEF $Dec!vars$
⟨3⟩4.CASE $v \in Nat \setminus \{0\}$
⟨4⟩.$\langle oth,\ self\rangle \in SubProcs \setminus (ProcIds \cup WrProcs)$
BY $DisjointIds$ DEF $SubProcs$, $OtherProcs$
⟨4⟩1. $q[oth][self] \in Seq(Nat \cup \{ack\})$
BY POP_access DEF $OtherProcs$
⟨4⟩2. $\land\ 1 \in 1\,..\,Len(q[oth][self])$
$\land\ v = q[oth][self][1]$
BY ⟨4⟩1
⟨4⟩3. $\land\ Inv!3!(oth)!(self)$
$\land\ Inv!4!(oth)!(self)$
BY DEF $OtherProcs$, Inv
⟨4⟩4. $v = number[oth]$
BY ⟨3⟩4, ⟨4⟩2, ⟨4⟩3, $Zenon$
⟨4⟩5. $number[oth] \in Nat$
BY DEF $OtherProcs$
⟨4⟩6. $number[oth] \in Range(q[oth][self])$
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩4, $RangeEquality$
⟨4⟩7. $\land\ pc[\langle oth\rangle] =$ "L"
$\land\ pc[\langle oth,\ self\rangle] =$ "L0"
BY ⟨3⟩4, ⟨4⟩3, ⟨4⟩6
⟨4⟩8. $DecLN[self][oth] = qm$
BY ⟨4⟩6 DEF $DecLN$
⟨4⟩9. $\land\ DecPC[\langle oth,\ self\rangle] =$ "test"
$\land\ DecPC[\langle oth\rangle] =$ "L"
BY ⟨4⟩7, ⟨4⟩8, $qmNotNat$, $Zenon$ DEF $DecPC$, $DecProcSet$, $OtherProcs$, $ProcIds$
⟨4⟩10. $DecLN' = [DecLN$ EXCEPT $![self][oth] = number[oth]]$
⟨5⟩1. $localNum' = [localNum$ EXCEPT $![self][oth] = number[oth]]$
BY ⟨3⟩4, ⟨4⟩4, $ackNotNat$
⟨5⟩2. $\land\ q' \in POP(Seq(Nat \cup \{ack\}))$
$\land\ \forall\, k \in Procs : \forall\, l \in OtherProcs(k) :$
$q'[k][l] =$ IF $k = self \land l = oth$ THEN $Append(q[self][oth],\ ack)$

ELSE IF $k = oth \land l = self$ THEN $Tail(q[oth][self])$
ELSE $q[k][l]$

$\langle 6 \rangle$.DEFINE $tl \triangleq Tail(q[oth][self])$
$qq \triangleq [q \text{ EXCEPT } ![oth][self] = tl]$

$\langle 6 \rangle 1$. $tl \in Seq(Nat \cup \{ack\})$
BY $\langle 4 \rangle 1$

$\langle 6 \rangle 2$. $q' = [qq \text{ EXCEPT } ![self][oth] = Append(q[self][oth], ack)]$
BY $\langle 3 \rangle 4$, *ackNotNat*

$\langle 6 \rangle$.HIDE DEF tl

$\langle 6 \rangle 3$. $qq \in POP(Seq(Nat \cup \{ack\}))$
BY ONLY *FullTypeOK*, $\langle 6 \rangle 1$, *POP_except*, *Zenon* DEF *OtherProcs*

$\langle 6 \rangle 4$. $qq[oth][self] = tl$
BY ONLY *FullTypeOK*, $\langle 6 \rangle 1$, *POP_except*, *Isa* DEF *OtherProcs*

$\langle 6 \rangle 5$. $\forall\, k \in Procs : \forall\, l \in OtherProcs(k) :$
$k \neq oth \lor l \neq self \Rightarrow qq[k][l] = q[k][l]$
BY ONLY *FullTypeOK*, $\langle 6 \rangle 1$, *POP_except* DEF *OtherProcs*

$\langle 6 \rangle$.HIDE DEF qq

$\langle 6 \rangle 6$. $Append(q[self][oth], ack) \in Seq(Nat \cup \{ack\})$
BY *POP_access*

$\langle 6 \rangle 7$. $\land\, q' \in POP(Seq(Nat \cup \{ack\}))$
$\land\, q'[self][oth] = Append(q[self][oth], ack)$
$\land\, \forall\, k \in Procs : \forall\, l \in OtherProcs(k) :$
$k \neq self \lor l \neq oth \Rightarrow q'[k][l] = qq[k][l]$
BY ONLY $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, $\langle 6 \rangle 6$, *POP_except*, *Isa*

$\langle 6 \rangle 8$. ASSUME NEW $k \in Procs$, NEW $l \in OtherProcs(k)$
PROVE $q'[k][l] =$ IF $k = self \land l = oth$ THEN $Append(q[self][oth], ack)$
ELSE IF $k = oth \land l = self$ THEN $Tail(q[oth][self])$
ELSE $q[k][l]$

$\langle 7 \rangle 1$.CASE $k = self \land l = oth$
BY $\langle 7 \rangle 1$, $\langle 6 \rangle 7$

$\langle 7 \rangle 2$.CASE $k = oth \land l = self$
BY $\langle 7 \rangle 2$, $\langle 6 \rangle 7$, $\langle 6 \rangle 4$ DEF *OtherProcs*, tl

$\langle 7 \rangle 3$.CASE $\neg(k = self \land l = oth) \land \neg(k = oth \land l = self)$
BY $\langle 7 \rangle 3$, $\langle 6 \rangle 7$, $\langle 6 \rangle 5$ DEF *OtherProcs*

$\langle 7 \rangle$.QED BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $\langle 7 \rangle 3$

$\langle 6 \rangle$.QED BY $\langle 6 \rangle 7$, $\langle 6 \rangle 8$

$\langle 5 \rangle 3$. SUFFICES ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $DecLN'[i][j] =$ IF $i = self \land j = oth$ THEN $number[oth]$ ELSE $DecLN[i][j]$
BY $\langle 4 \rangle 5$, *POP_except_equal*, *Isa*

$\langle 5 \rangle 4$.CASE $i = self \land j = oth$

$\langle 6 \rangle 3$. ASSUME $number[oth] \in Range(Tail(q[oth][self]))$
PROVE FALSE

$\langle 7 \rangle$.DEFINE $tl \triangleq Tail(q[oth][self])$

$\langle 7 \rangle 1$. PICK $k \in 1 \,..\, Len(tl) : tl[k] = number[oth]$
BY $\langle 6 \rangle 3$ DEF *Range*

⟨7⟩2. ∧ $k + 1 \in 1 \,..\, Len(q[oth][self])$
∧ $q[oth][self][k + 1] = number[oth]$
BY ⟨7⟩1
⟨7⟩.QED BY ONLY ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, ⟨7⟩2
⟨6⟩.QED BY ⟨5⟩1, ⟨5⟩4, ⟨5⟩2, ⟨6⟩3 DEF *DecLN*, *POP*, *PFunc*, *OtherProcs*
⟨5⟩5.CASE $i = oth \wedge j = self$
⟨6⟩1. ∧ $q[self][oth] \in Seq(Nat \cup \{ack\})$
∧ $q'[self][oth] = Append(q[self][oth], ack)$
BY ⟨5⟩2, *POP_access*, *Zenon* DEF *OtherProcs*
⟨6⟩2. $number'[self] \in Range(q'[self][oth]) \equiv number[self] \in Range(q[self][oth])$
BY ⟨6⟩1, *AppendProperties*, *ackNotNat* DEF *OtherProcs*
⟨6⟩3. $localNum'[oth][self] = localNum[oth][self]$
BY ⟨4⟩5, ⟨5⟩1, *POP_except* DEF *OtherProcs*
⟨6⟩.QED BY ⟨5⟩5, ⟨6⟩2, ⟨6⟩3 DEF *DecLN*, *OtherProcs*
⟨5⟩6.CASE $\neg(i = self \wedge j = oth) \wedge \neg(i = oth \wedge j = self)$
⟨6⟩1. $q'[j][i] = q[j][i]$
BY ⟨5⟩6, ⟨5⟩2 DEF *OtherProcs*
⟨6⟩2. $localNum'[i][j] = localNum[i][j]$
BY ⟨5⟩6, ⟨4⟩5, ⟨5⟩1, *POP_except* DEF *OtherProcs*
⟨6⟩.QED BY ⟨5⟩6, ⟨6⟩1, ⟨6⟩2 DEF *DecLN*
⟨5⟩.QED BY ⟨5⟩4, ⟨5⟩5, ⟨5⟩6
⟨4⟩11. $DecPC' = [DecPC$ EXCEPT $![\langle oth, self\rangle] =$ "Lb"$]$
⟨5⟩.SUFFICES ASSUME NEW $p \in DecProcSet$
PROVE $DecPC'[p] =$ IF $p = \langle oth, self\rangle$ THEN "Lb" ELSE $DecPC[p]$
BY *Zenon* DEF *DecPC*
⟨5⟩1.CASE $p \in ProcIds$
BY ⟨5⟩1 DEF *DecPC*
⟨5⟩2.CASE $p \in SubProcs$
⟨6⟩.PICK $i, j \in Procs : i \neq j \wedge p = \langle i, j\rangle$
BY ⟨5⟩2 DEF *SubProcs*
⟨6⟩1.CASE $i = oth \wedge j = self$
⟨7⟩.$DecLN'[self][oth] = number'[oth]$
BY ⟨4⟩10, ⟨4⟩5, *POP_except*, *Isa*
⟨7⟩.QED BY ⟨5⟩2, ⟨6⟩1, ⟨4⟩7, *DisjointIds* DEF *DecPC*
⟨6⟩2.CASE $\neg(i = oth \wedge j = self)$
⟨7⟩.$DecLN'[j][i] = DecLN[j][i]$
BY ⟨4⟩10, ⟨4⟩5, ⟨6⟩2, *POP_except*
⟨7⟩.QED BY ⟨5⟩2, ⟨6⟩2, *DisjointIds* DEF *DecPC*
⟨6⟩.QED BY ⟨6⟩1, ⟨6⟩2
⟨5⟩3.CASE $p \in WrProcs$
BY ⟨5⟩3, *DisjointIds* DEF *DecPC*
⟨5⟩.QED BY ⟨5⟩1, ⟨5⟩2, ⟨5⟩3 DEF *DecProcSet*
⟨4⟩12. $Dec!test(\langle oth, self\rangle)$
BY ⟨4⟩9, ⟨4⟩10, ⟨4⟩11, *DecEqualities* DEF $Dec!test$
⟨4⟩.QED BY ⟨4⟩12, *DecEqualities* DEF $Dec!Next$, $Dec!sub$

⟨3⟩.QED BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, *POP_access* DEF *OtherProcs*
⟨2⟩11.CASE UNCHANGED *vars*
BY ⟨2⟩11 DEF *vars*, *Dec*!*vars*, *DecLN*, *DecPC*
⟨2⟩12. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9, ⟨2⟩10, ⟨2⟩11
DEF *Next*, *main*, *sub*, *ProcIds*, *SubProcs*, *MsgProcs*, *OtherProcs*
⟨1⟩.QED
BY ⟨1⟩1, ⟨1⟩2, *Typing*, *DecLN_type*, *Invariance*, *PTL* DEF *Spec*, *DecSafety*

* Modification History
* Last modified *Tue Nov* 16 18:51:45 *CET* 2021 by *merz*
* Created *Thu Sep* 02 11:41:20 *CEST* 2021 by *merz*