MODULE *DeconProofNonAtomic*

Proofs for the deconstructed Bakery (non-atomic version).

EXTENDS *BakeryDeconstructedNonAtomic*, *TLAPS*

USE *NAssump*

The *TypeOK* predicate defined in module *BakeryDeconstructedNonAtomic* does not quite assert the types of the variables *localNum* and *localCh*, and it doesn't cover the types of the local variables. We introduce a more precise predicate of type correctness that is used in the proof.

$FullTypeOK \triangleq$
$\quad \land\ number \in [Procs \rightarrow Nat]$
$\quad \land\ localNum \in POP(Nat \cup \{qm\})$
$\quad \land\ localCh \in POP(\{0, 1\})$
$\quad \land\ pc \in [ProcIds \cup SubProcs \cup WrProcs \rightarrow$
$\qquad\qquad \{\text{“ncs”}, \text{“M”}, \text{“M0”}, \text{“L”}, \text{“cs”}, \text{“P”},$
$\qquad\qquad\ \ \text{“ch”}, \text{“test”}, \text{“Lb”}, \text{“L2”}, \text{“L3”},$
$\qquad\qquad\ \ \text{“wr”}\}]$
$\quad \land\ \forall i \in ProcIds : pc[i] \in \{\text{“ncs”}, \text{“M”}, \text{“M0”}, \text{“L”}, \text{“cs”}, \text{“P”}\}$
$\quad \land\ \forall i \in SubProcs : pc[i] \in \{\text{“ch”}, \text{“test”}, \text{“Lb”}, \text{“L2”}, \text{“L3”}\}$
$\quad \land\ \forall i \in WrProcs : pc[i] = \text{“wr”}$
$\quad \land\ unRead \in [ProcIds \rightarrow \text{SUBSET } Procs]$
$\quad \land\ \forall i \in ProcIds : unRead[i] \in \text{SUBSET } OtherProcs(i[1])$
$\quad \land\ v \in [ProcIds \rightarrow Nat]$

THEOREM $Typing \triangleq Spec \Rightarrow \Box FullTypeOK$
$\langle 1 \rangle 1.\ Init \Rightarrow FullTypeOK$
  $\langle 2 \rangle$ SUFFICES ASSUME *Init*
                 PROVE *FullTypeOK*
    OBVIOUS
  $\langle 2 \rangle 1.\ \land\ localNum \in POP(Nat \cup \{qm\})$
        $\land\ localCh \in POP(\{0, 1\})$
    BY *POP_construct*, *Isa* DEF *Init*
  $\langle 2 \rangle$.QED
    BY $\langle 2 \rangle 1$, *DisjointIds* DEF *Init*, *ProcSet*, *FullTypeOK*
$\langle 1 \rangle 2.\ FullTypeOK \land [Next]_{vars} \Rightarrow FullTypeOK'$
  $\langle 2 \rangle$ SUFFICES ASSUME *FullTypeOK*,
                        $[Next]_{vars}$
                 PROVE $FullTypeOK'$
    OBVIOUS
  $\langle 2 \rangle$.USE DEF *FullTypeOK*
  $\langle 2 \rangle 1.$ ASSUME NEW $self \in ProcIds$,
              $ncs(self)$
        PROVE $FullTypeOK'$
    BY $\langle 2 \rangle 1$ DEF *ncs*
  $\langle 2 \rangle 2.$ ASSUME NEW $self \in ProcIds$,
              $M(self)$

```
      PROVE  FullTypeOK'
  BY ⟨2⟩2  DEF M, OtherProcs
⟨2⟩3. ASSUME NEW self ∈ ProcIds,
             M0(self)
      PROVE  FullTypeOK'
  ⟨3⟩1.CASE unRead[self] ≠ {}
    ⟨4⟩.PICK j ∈ unRead[self] :
              ∧ IF localNum[self[1]][j] ≠ qm
                  THEN v' = [v EXCEPT ![self] = Max(v[self], localNum[self[1]][j])]
                  ELSE v' = v
              ∧ unRead' = [unRead EXCEPT ![self] = unRead[self] \ {j}]
              ∧ pc' = [pc EXCEPT ![self] = "M0"]
              ∧ UNCHANGED ⟨number, localNum, localCh⟩
      BY ⟨2⟩3, ⟨3⟩1  DEF M0
    ⟨4⟩.(v ∈ [ProcIds → Nat])'
      ⟨5⟩1.CASE localNum[self[1]][j] = qm
        BY ⟨5⟩1
      ⟨5⟩2.CASE localNum[self[1]][j] ≠ qm
        BY ⟨5⟩2  DEF Max, POP, PFunc, ProcIds
      ⟨5⟩.QED  BY ⟨5⟩1, ⟨5⟩2
    ⟨4⟩.QED
      BY Zenon
  ⟨3⟩2.CASE unRead[self] = {}
    ⟨4⟩.PICK n ∈ Nat :
              ∧ n > v[self]
              ∧ number' = [number EXCEPT ![self[1]] = n]
              ∧ localNum' = [j ∈ Procs ↦
                                  [i ∈ OtherProcs(j) ↦
                                      IF i = self[1] THEN qm
                                                     ELSE localNum[j][i]]]
              ∧ v' = [v EXCEPT ![self] = 0]
              ∧ pc' = [pc EXCEPT ![self] = "L"]
              ∧ UNCHANGED ⟨unRead, localCh⟩
      BY ⟨2⟩3, ⟨3⟩2  DEF M0
    ⟨4⟩.(number ∈ [Procs → Nat])'
      BY Zenon
    ⟨4⟩.QED
      BY DEF POP, PFunc
  ⟨3⟩.QED  BY ⟨3⟩1, ⟨3⟩2
⟨2⟩4. ASSUME NEW self ∈ ProcIds,
             L(self)
      PROVE  FullTypeOK'
  BY ⟨2⟩4  DEF L
⟨2⟩5. ASSUME NEW self ∈ ProcIds,
             cs(self)
```

PROVE $FullTypeOK'$

BY $\langle 2 \rangle 5$ DEF cs

$\langle 2 \rangle 6.$ ASSUME NEW $self \in ProcIds$,
$P(self)$
PROVE $FullTypeOK'$

$\langle 3 \rangle.(number \in [Procs \rightarrow Nat])'$
BY $\langle 2 \rangle 6$, $Zenon$ DEF P

$\langle 3 \rangle.$QED
BY $\langle 2 \rangle 6$ DEF P, POP, $PFunc$

$\langle 2 \rangle 7.$ ASSUME NEW $self \in SubProcs$,
$ch(self)$
PROVE $FullTypeOK'$

$\langle 3 \rangle.(localCh \in POP(\{0, 1\}))'$
BY $\langle 2 \rangle 7$ DEF ch, $SubProcs$, POP, $PFunc$, $OtherProcs$

$\langle 3 \rangle.$QED
BY $\langle 2 \rangle 7$ DEF ch

$\langle 2 \rangle 8.$ ASSUME NEW $self \in SubProcs$,
$test(self)$
PROVE $FullTypeOK'$

$\langle 3 \rangle.(localNum \in POP(Nat \cup \{qm\}))'$
BY $\langle 2 \rangle 8$ DEF $test$, $SubProcs$, POP, $PFunc$, $OtherProcs$

$\langle 3 \rangle.$QED
BY $\langle 2 \rangle 8$ DEF $test$

$\langle 2 \rangle 9.$ ASSUME NEW $self \in SubProcs$,
$Lb(self)$
PROVE $FullTypeOK'$

BY $\langle 2 \rangle 9$ DEF Lb, $SubProcs$, POP, $PFunc$, $OtherProcs$

$\langle 2 \rangle 10.$ ASSUME NEW $self \in SubProcs$,
$L2(self)$
PROVE $FullTypeOK'$

BY $\langle 2 \rangle 10$ DEF $L2$

$\langle 2 \rangle 11.$ ASSUME NEW $self \in SubProcs$,
$L3(self)$
PROVE $FullTypeOK'$

BY $\langle 2 \rangle 11$ DEF $L3$

$\langle 2 \rangle 12.$ ASSUME NEW $self \in WrProcs$,
$wrp(self)$
PROVE $FullTypeOK'$

BY $\langle 2 \rangle 12$ DEF wrp, wr, $WrProcs$, POP, $PFunc$, $OtherProcs$

$\langle 2 \rangle 13.$CASE UNCHANGED $vars$
BY $\langle 2 \rangle 13$ DEF $vars$

$\langle 2 \rangle.$HIDE DEF $FullTypeOK$

$\langle 2 \rangle 14.$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 10$, $\langle 2 \rangle 11$, $\langle 2 \rangle 12$, $\langle 2 \rangle 13$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, $\langle 2 \rangle 8$, $\langle 2 \rangle 9$
DEF $Next$, $main$, sub

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

The following invariant expresses how the main processes and their sub-processes synchronize. This invariant is implicit in the informal presentation where sub-processes appear within the scope of the main processes but must be made explicit in the formal development.

$$
\begin{array}{l}
\mathit{SyncInv} \triangleq \forall i \in \mathit{Procs} : \\
\quad \lor \land pc[\langle i \rangle] \in \{\text{"ncs"}, \text{"cs"}, \text{"P"}\} \\
\quad\quad \land \forall j \in \mathit{OtherProcs}(i) : pc[\langle i, j \rangle] = \text{"ch"} \\
\quad \lor \land pc[\langle i \rangle] = \text{"M"} \\
\quad\quad \land \forall j \in \mathit{OtherProcs}(i) : pc[\langle i, j \rangle] \in \{\text{"ch"}, \text{"test"}\} \\
\quad \lor \land pc[\langle i \rangle] = \text{"M0"} \\
\quad\quad \land \forall j \in \mathit{OtherProcs}(i) : pc[\langle i, j \rangle] = \text{"test"} \\
\quad \lor pc[\langle i \rangle] = \text{"L"}
\end{array}
$$

THEOREM *Synchronization* $\triangleq$ $\mathit{Spec} \Rightarrow \Box \mathit{SyncInv}$

$\langle 1 \rangle 1$. $\mathit{Init} \Rightarrow \mathit{SyncInv}$

BY *DisjointIds*, *Zenon* DEF *Init*, *OtherProcs*, *ProcSet*, *ProcIds*, *SubProcs*, *SyncInv*

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

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

OBVIOUS

$\langle 2 \rangle$.USE DEFS *FullTypeOK*, *SyncInv*

* *TODO*: Tedious decomposition due to an internal error reported by the *SMT* backend.

$\langle 2 \rangle 1$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $i \in \mathit{Procs} \setminus \{\mathit{self}\}$, UNCHANGED $pc[\langle i \rangle]$, $\forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$ PROVE $\mathit{SyncInv}!(i)'$

BY $\langle 2 \rangle 1$

$\langle 2 \rangle 2$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$, $\mathit{ncs}(\langle \mathit{self} \rangle)$ PROVE $\mathit{SyncInv}'$

$\langle 3 \rangle$. $\land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}$:
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$

BY $\langle 2 \rangle 2$ DEF *ncs*

$\langle 3 \rangle$.QED

BY $\langle 2 \rangle 1$, *Zenon*

$\langle 2 \rangle 3$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$, $M(\langle \mathit{self} \rangle)$ PROVE $\mathit{SyncInv}'$

$\langle 3 \rangle 1$. $\land pc[\langle \mathit{self} \rangle] = \text{"M"}$

$\land \forall j \in OtherProcs(self) : pc[\langle self, j \rangle] = \text{"test"}$
$\land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"M0"}]$
BY $\langle 2 \rangle 3$ DEF M, $SubProcsOf$, $SubProcs$, $OtherProcs$
$\langle 3 \rangle. \land SyncInv!(self)'$
$\land \forall i \in Procs \setminus \{self\} :$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in OtherProcs(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 3 \rangle 1$
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, $Zenon$
$\langle 2 \rangle 4$. ASSUME NEW $self \in Procs$,
$M0(\langle self \rangle)$
PROVE $SyncInv'$
$\langle 3 \rangle 1. \land pc[\langle self \rangle] = \text{"M0"}$
$\land \forall j \in OtherProcs(self) : pc[\langle self, j \rangle] = \text{"test"}$
$\land \exists l \in \{\text{"M0"}, \text{"L"}\} : pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = l]$
BY $\langle 2 \rangle 4$ DEF $M0$
$\langle 3 \rangle. \land SyncInv!(self)'$
$\land \forall i \in Procs \setminus \{self\} :$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in OtherProcs(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 3 \rangle 1$
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, $Zenon$
$\langle 2 \rangle 5$. ASSUME NEW $self \in Procs$,
$L(\langle self \rangle)$
PROVE $SyncInv'$
$\langle 3 \rangle. \land \forall j \in OtherProcs(self) : pc[\langle self, j \rangle] = \text{"ch"}$
$\land SyncInv!(self)'$
$\land \forall i \in Procs \setminus \{self\} :$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in OtherProcs(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2 \rangle 5$ DEF L, $SubProcsOf$, $SubProcs$, $OtherProcs$
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, $Zenon$
$\langle 2 \rangle 6$. ASSUME NEW $self \in Procs$,
$cs(\langle self \rangle)$
PROVE $SyncInv'$
$\langle 3 \rangle. \land SyncInv!(self)'$
$\land \forall i \in Procs \setminus \{self\} :$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in OtherProcs(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2 \rangle 6$ DEF cs
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, $Zenon$

$\langle 2\rangle 7.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$P(\langle \mathit{self} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3\rangle.\ \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}:$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2\rangle 7$ DEF P
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 8.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$\mathit{ch}(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3\rangle.\ \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}:$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2\rangle 8$ DEF ch
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 9.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$\mathit{test}(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3\rangle.\ \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}:$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2\rangle 9$ DEF test
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 10.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$\mathit{Lb}(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3\rangle.\ \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}:$
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2\rangle 10$ DEF Lb
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 11.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$\mathit{L2}(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3\rangle.\ \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}:$

$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2 \rangle 11$ DEF $L2$
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, *Zenon*
$\langle 2 \rangle 12$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$L3(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3 \rangle . \land \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}$:
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2 \rangle 12$ DEF $L3$
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, *Zenon*
$\langle 2 \rangle 13$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{Procs}$,
$\mathit{wrp}(\langle \mathit{self}, \mathit{oth}, \text{"wr"} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3 \rangle$.UNCHANGED pc
BY $\langle 2 \rangle 13$ DEF wrp, wr
$\langle 3 \rangle$.QED
BY *Zenon*
$\langle 2 \rangle 14$.CASE UNCHANGED vars
BY $\langle 2 \rangle 14$, *Zenon* DEF vars
$\langle 2 \rangle$.HIDE DEFS $\mathit{FullTypeOK}$, $\mathit{SyncInv}$
$\langle 2 \rangle 15$. QED
BY $\langle 2 \rangle 2$, $\langle 2 \rangle 11$, $\langle 2 \rangle 12$, $\langle 2 \rangle 13$, $\langle 2 \rangle 14$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, $\langle 2 \rangle 8$, $\langle 2 \rangle 9$, $\langle 2 \rangle 10$
DEF Next, main, sub, $\mathit{ProcIds}$, $\mathit{SubProcs}$, $\mathit{WrProcs}$
$\langle 1 \rangle$.QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, *Typing*, *PTL* DEF *Spec*

The following invariant characterizes the values of *localCh*, *localNum*, and number.

$\mathit{NumInv} \triangleq \forall i \in \mathit{Procs}$:
$\land\ \mathit{number}[i] \neq 0 \equiv pc[\langle i \rangle] \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
$\land \forall j \in \mathit{OtherProcs}(i)$:
$\land\ \mathit{localCh}[j][i] = 1 \equiv pc[\langle i, j \rangle] \in \{\text{"test"}, \text{"Lb"}\}$
$\land\ \mathit{localNum}[j][i] \neq \mathit{number}[i] \Rightarrow$
$\land\ \mathit{localNum}[j][i] = \mathit{qm}$
$\land \lor pc[\langle i \rangle] = \text{"L"} \land pc[\langle i, j \rangle] = \text{"test"}$
$\lor pc[\langle i \rangle] \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$

THEOREM $\mathit{NumberInvariant} \triangleq \mathit{Spec} \Rightarrow \Box \mathit{NumInv}$
$\langle 1 \rangle 1$. $\mathit{Init} \Rightarrow \mathit{NumInv}$
$\langle 2 \rangle 1$. ASSUME Init, NEW $i \in \mathit{Procs}$
PROVE $\mathit{number}[i] = 0 \land pc[\langle i \rangle] \notin \{\text{"L"}, \text{"cs"}, \text{"P"}\}$

BY $\langle 2\rangle 1$, *Zenon* DEF *Init*, *ProcSet*, *ProcIds*

$\langle 2\rangle 2$. ASSUME *Init*, NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $\land\ localCh[j][i] \neq 1 \land pc[\langle i,\, j\rangle] \notin \{\text{“test”},\ \text{“Lb”}\}$
$\land\ localNum[j][i] = number[i]$

BY $\langle 2\rangle 2$, *SubProcId*, *Isa* DEF *Init*, *OtherProcs*, *ProcSet*

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

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

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

OBVIOUS

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

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

$\langle 3\rangle$. $\land\ pc[\langle self\rangle] = \text{“ncs”}$
$\land\ pc' = [pc$ EXCEPT $![\langle self\rangle] = \text{“M”}]$
$\land$ UNCHANGED $\langle number,\ localCh,\ localNum\rangle$

BY $\langle 2\rangle 1$ DEF *ncs*

$\langle 3\rangle 1$. $\forall\, i \in Procs : \forall\, j \in OtherProcs(i)$: UNCHANGED $pc[\langle i,\, j\rangle]$

BY DEF *OtherProcs*

$\langle 3\rangle 2$. ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i\rangle]' \in \{\text{“L”},\ \text{“cs”},\ \text{“P”}\}$

BY DEF *NumInv*

$\langle 3\rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i,\, j\rangle]' \in \{\text{“test”},\ \text{“Lb”}\}$

BY ONLY *NumInv*, UNCHANGED *localCh*, $\langle 3\rangle 1$, *Zenon* DEF *NumInv*

$\langle 3\rangle 4$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i\rangle]' = \text{“L”} \land pc[\langle i,\, j\rangle]' = \text{“test”}$
$\lor\ pc[\langle i\rangle]' \in \{\text{“ncs”},\ \text{“M”},\ \text{“M0”}\}$

BY $\langle 3\rangle 4$ DEF *NumInv*

$\langle 3\rangle$.QED BY ONLY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, *Zenon* DEF *NumInv*

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

$\langle 3\rangle$. $\land\ pc[\langle self\rangle] = \text{“M”}$
$\land\ pc' = [pc$ EXCEPT $![\langle self\rangle] = \text{“M0”}]$
$\land$ UNCHANGED $\langle number,\ localCh,\ localNum\rangle$

BY $\langle 2\rangle 2$ DEF *M*

$\langle 3\rangle 1$. $\forall\, i \in Procs : \forall\, j \in OtherProcs(i)$: UNCHANGED $pc[\langle i,\, j\rangle]$

BY DEF *OtherProcs*

$\langle 3 \rangle 2.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF $NumInv$
$\langle 3 \rangle 3.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY $NumInv$, UNCHANGED $localCh$, $\langle 3 \rangle 1$, $Zenon$ DEF $NumInv$
$\langle 3 \rangle 4.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\lor\ pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3 \rangle 4$ DEF $NumInv$
$\langle 3 \rangle$.QED BY ONLY $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $Zenon$ DEF $NumInv$
$\langle 2 \rangle 3.$ ASSUME NEW $self \in Procs$,
$M0(\langle self \rangle)$
PROVE $NumInv'$
$\langle 3 \rangle 1.$CASE $unRead[\langle self \rangle] \neq \{\}$
$\langle 4 \rangle$.UNCHANGED $\langle pc, number, localCh, localNum \rangle$
BY $\langle 2 \rangle 3$, $\langle 3 \rangle 1$ DEF $M0$
$\langle 4 \rangle$.QED BY Isa DEF $NumInv$
$\langle 3 \rangle 2.$CASE $unRead[\langle self \rangle] = \{\}$
$\langle 4 \rangle.\ \land\ pc[\langle self \rangle] = \text{"M0"}$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"L"}]$
$\land\ \exists\, n \in \{m \in Nat : m > v[\langle self \rangle]\} : number' = [number \text{ EXCEPT } ![self] = n]$
$\land\ localNum' = [j \in Procs \mapsto$
$[i \in OtherProcs(j) \mapsto$
$\text{IF } i = self \text{ THEN } qm \text{ ELSE } localNum[j][i]]]$
$\land$ UNCHANGED $localCh$
BY $\langle 2 \rangle 3$, $\langle 3 \rangle 2$ DEF $M0$
$\langle 4 \rangle 1.$ $\forall\, i \in Procs : \forall\, j \in OtherProcs(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY DEF $OtherProcs$
$\langle 4 \rangle 2.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF $NumInv$, $ProcIds$
$\langle 4 \rangle 3.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY $NumInv$, UNCHANGED $localCh$, $\langle 4 \rangle 1$, $Zenon$ DEF $NumInv$, $OtherProcs$
$\langle 4 \rangle 4.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\lor\ pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 4 \rangle 4$ DEF $NumInv$, $SyncInv$, $OtherProcs$
$\langle 4 \rangle$.QED BY ONLY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$, $\langle 4 \rangle 4$, $Zenon$ DEF $NumInv$
$\langle 3 \rangle$.QED BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$

$\langle 2\rangle 4.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$\quad L(\langle \mathit{self} \rangle)$
PROVE NumInv'

$\langle 3\rangle.$ $\land\ pc[\langle \mathit{self} \rangle] = \text{"L"}$
$\land\ \forall j \in \mathit{OtherProcs}(\mathit{self}) : pc[\langle \mathit{self}, j \rangle] = \text{"ch"}$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle \mathit{self} \rangle] = \text{"cs"}]$
$\land$ UNCHANGED $\langle \mathit{number}, \mathit{localNum}, \mathit{localCh} \rangle$
BY $\langle 2\rangle 4$ DEF L, $\mathit{OtherProcs}$, $\mathit{SubProcsOf}$, $\mathit{SubProcs}$

$\langle 3\rangle 1.$ $\forall i \in \mathit{Procs} : \forall j \in \mathit{OtherProcs}(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY DEF $\mathit{OtherProcs}$

$\langle 3\rangle 2.$ ASSUME NEW $i \in \mathit{Procs}$
PROVE $\mathit{number}[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF NumInv

$\langle 3\rangle 3.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$
PROVE $\mathit{localCh}[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY NumInv, UNCHANGED $\mathit{localCh}$, $\langle 3\rangle 1$, Zenon DEF NumInv

$\langle 3\rangle 4.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$,
$\quad \mathit{localNum}[j][i]' \neq \mathit{number}[i]'$
PROVE $\land\ \mathit{localNum}[j][i]' = qm$
$\quad \land\ \lor\ pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\quad\quad \lor\ pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3\rangle 4$ DEF NumInv

$\langle 3\rangle.$QED BY ONLY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, Zenon DEF NumInv

$\langle 2\rangle 5.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$\quad cs(\langle \mathit{self} \rangle)$
PROVE NumInv'

$\langle 3\rangle.$ $\land\ pc[\langle \mathit{self} \rangle] = \text{"cs"}$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle \mathit{self} \rangle] = \text{"P"}]$
$\land$ UNCHANGED $\langle \mathit{number}, \mathit{localNum}, \mathit{localCh} \rangle$
BY $\langle 2\rangle 5$ DEF cs

$\langle 3\rangle 1.$ $\forall i \in \mathit{Procs} : \forall j \in \mathit{OtherProcs}(i) :$ UNCHANGED $pc[\langle i, j \rangle]$
BY DEF $\mathit{OtherProcs}$

$\langle 3\rangle 2.$ ASSUME NEW $i \in \mathit{Procs}$
PROVE $\mathit{number}[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF NumInv

$\langle 3\rangle 3.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$
PROVE $\mathit{localCh}[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY NumInv, UNCHANGED $\mathit{localCh}$, $\langle 3\rangle 1$, Zenon DEF NumInv

$\langle 3\rangle 4.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$,
$\quad \mathit{localNum}[j][i]' \neq \mathit{number}[i]'$
PROVE $\land\ \mathit{localNum}[j][i]' = qm$
$\quad \land\ \lor\ pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\quad\quad \lor\ pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3\rangle 4$ DEF NumInv

$\langle 3\rangle.$QED BY ONLY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, Zenon DEF NumInv

$\langle 2\rangle 6.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$P(\langle \mathit{self} \rangle)$
PROVE NumInv'

$\langle 3\rangle.$ $\land\ \mathit{pc}[\langle \mathit{self} \rangle] = \text{"P"}$
$\land\ \mathit{pc}' = [\mathit{pc}$ EXCEPT $![\langle \mathit{self} \rangle] = \text{"ncs"}]$
$\land\ \mathit{number}' = [\mathit{number}$ EXCEPT $![\mathit{self}] = 0]$
$\land\ \mathit{localNum}' = [j \in \mathit{Procs} \mapsto$
$[i \in \mathit{OtherProcs}(j) \mapsto$
IF $i = \mathit{self}$ THEN qm ELSE $\mathit{localNum}[j][i]]]$
$\land$ UNCHANGED $\mathit{localCh}$
BY $\langle 2\rangle 6$ DEF P

$\langle 3\rangle 1.$ $\forall\, i \in \mathit{Procs} : \forall\, j \in \mathit{OtherProcs}(i) :$ UNCHANGED $\mathit{pc}[\langle i, j \rangle]$
BY DEF $\mathit{OtherProcs}$

$\langle 3\rangle 2.$ ASSUME NEW $i \in \mathit{Procs}$
PROVE $\mathit{number}[i]' \neq 0 \equiv \mathit{pc}[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF NumInv, $\mathit{ProcIds}$

$\langle 3\rangle 3.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$
PROVE $\mathit{localCh}[j][i]' = 1 \equiv \mathit{pc}[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY NumInv, UNCHANGED $\mathit{localCh}$, $\langle 3\rangle 1$, Zenon DEF NumInv

$\langle 3\rangle 4.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$,
$\mathit{localNum}[j][i]' \neq \mathit{number}[i]'$
PROVE $\land\ \mathit{localNum}[j][i]' = \mathit{qm}$
$\land\ \lor\ \mathit{pc}[\langle i \rangle]' = \text{"L"} \land \mathit{pc}[\langle i, j \rangle]' = \text{"test"}$
$\lor\ \mathit{pc}[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3\rangle 4$ DEF NumInv, $\mathit{ProcIds}$, $\mathit{OtherProcs}$

$\langle 3\rangle.$QED BY ONLY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, Zenon DEF NumInv

$\langle 2\rangle 7.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{OtherProcs}(\mathit{self})$,
$\mathit{ch}(\langle \mathit{self}, \mathit{oth} \rangle)$
PROVE NumInv'

$\langle 3\rangle.$ $\land\ \mathit{pc}[\langle \mathit{self}, \mathit{oth} \rangle] = \text{"ch"}$
$\land\ \mathit{pc}[\langle \mathit{self} \rangle] = \text{"M"}$
$\land\ \mathit{pc}' = [\mathit{pc}$ EXCEPT $![\langle \mathit{self}, \mathit{oth} \rangle] = \text{"test"}]$
$\land\ \mathit{localCh}' = [\mathit{localCh}$ EXCEPT $![\mathit{oth}][\mathit{self}] = 1]$
$\land$ UNCHANGED $\langle \mathit{number}, \mathit{localNum} \rangle$
BY $\langle 2\rangle 7$ DEF ch

$\langle 3\rangle 1.$ ASSUME NEW $i \in \mathit{Procs}$
PROVE $\mathit{number}[i]' \neq 0 \equiv \mathit{pc}[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF NumInv

$\langle 3\rangle 2.$ ASSUME NEW $i \in \mathit{Procs}$, NEW $j \in \mathit{OtherProcs}(i)$
PROVE $\mathit{localCh}[j][i]' = 1 \equiv \mathit{pc}[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$

$\langle 4\rangle 1.$CASE $i = \mathit{self} \land j = \mathit{oth}$
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF NumInv, $\mathit{OtherProcs}$, $\mathit{SubProcs}$, POP, PFunc

$\langle 4\rangle 2.$CASE $\neg(i = \mathit{self} \land j = \mathit{oth})$

$\langle 5\rangle 1.$ UNCHANGED $\langle \mathit{localCh}[j][i], \mathit{pc}[\langle i, j \rangle] \rangle$
BY $\langle 3\rangle 2$, $\langle 4\rangle 2$

$\langle 5\rangle$.QED BY ONLY $NumInv$, $\langle 5\rangle 1$, $Zenon$ DEF $NumInv$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}, \text{“M0”}\}$
BY $\langle 3\rangle 3$ DEF $NumInv$
$\langle 3\rangle$.QED BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2\rangle 8$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$test(\langle self, oth \rangle)$
PROVE $NumInv'$
$\langle 3\rangle$. $\land\ pc[\langle self, oth \rangle] = \text{“test”}$
$\land\ pc[\langle self \rangle] = \text{“L”}$
$\land\ pc' = [pc$ EXCEPT $![\langle self, oth \rangle] = \text{“Lb”}]$
$\land\ localNum' = [localNum$ EXCEPT $![oth][self] = number[self]]$
$\land$ UNCHANGED $\langle number, localCh \rangle$
BY $\langle 2\rangle 8$ DEF $test$
$\langle 3\rangle 1$. ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{“L”}, \text{“cs”}, \text{“P”}\}$
BY DEF $NumInv$
$\langle 3\rangle 2$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{“test”}, \text{“Lb”}\}$
$\langle 4\rangle 1$.CASE $i = self \land j = oth$
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF $NumInv$, $OtherProcs$, $SubProcs$
$\langle 4\rangle 2$.CASE $\neg(i = self \land j = oth)$
$\langle 5\rangle 1$. UNCHANGED $\langle localCh[j][i], pc[\langle i, j \rangle] \rangle$
BY $\langle 3\rangle 2$, $\langle 4\rangle 2$
$\langle 5\rangle$.QED BY ONLY $NumInv$, $\langle 5\rangle 1$, $Zenon$ DEF $NumInv$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}, \text{“M0”}\}$
$\langle 4\rangle 1$.CASE $i = self \land j = oth$
BY $\langle 3\rangle 3$, $\langle 4\rangle 1$ DEF $NumInv$, $OtherProcs$, $SubProcs$, POP, $PFunc$
$\langle 4\rangle 2$.CASE $\neg(i = self \land j = oth)$
BY $\langle 3\rangle 3$, $\langle 4\rangle 2$ DEF $NumInv$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle$.QED BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2\rangle 9$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$Lb(\langle self, oth \rangle)$
PROVE $NumInv'$
$\langle 3\rangle$. $\land\ pc[\langle self, oth \rangle] = \text{“Lb”}$

$\wedge\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] =$ "L2"$]$
$\wedge\ localCh' = [localCh$ EXCEPT $![oth][self] = 0]$
$\wedge$ UNCHANGED $\langle number, localNum\rangle$
BY $\langle 2\rangle 9$ DEF Lb
$\langle 3\rangle 1.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i\rangle]' \in \{$"L", "cs", "P"$\}$
BY DEF $NumInv$
$\langle 3\rangle 2.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j\rangle]' \in \{$"test", "Lb"$\}$
$\langle 4\rangle 1.$CASE $i = self \wedge j = oth$
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF $NumInv$, $OtherProcs$, $SubProcs$, POP, $PFunc$
$\langle 4\rangle 2.$CASE $\neg(i = self \wedge j = oth)$
$\langle 5\rangle 1.$ UNCHANGED $\langle localCh[j][i], pc[\langle i, j\rangle]\rangle$
BY $\langle 3\rangle 2$, $\langle 4\rangle 2$
$\langle 5\rangle$.QED BY ONLY $NumInv$, $\langle 5\rangle 1$, $Zenon$ DEF $NumInv$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 3.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\wedge\ localNum[j][i]' = qm$
$\wedge\ \vee\ pc[\langle i\rangle]' =$ "L" $\wedge\ pc[\langle i, j\rangle]' =$ "test"
$\vee\ pc[\langle i\rangle]' \in \{$"ncs", "M", "M0"$\}$
BY $\langle 3\rangle 3$ DEF $NumInv$
$\langle 3\rangle$.QED BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2\rangle 10.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L2(\langle self, oth\rangle)$
PROVE $NumInv'$
$\langle 3\rangle.\ \wedge\ pc[\langle self, oth\rangle] =$ "L2"
$\wedge\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] =$ "L3"$]$
$\wedge$ UNCHANGED $\langle number, localNum, localCh\rangle$
BY $\langle 2\rangle 10$ DEF $L2$
$\langle 3\rangle 1.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i\rangle]' \in \{$"L", "cs", "P"$\}$
BY DEF $NumInv$
$\langle 3\rangle 2.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j\rangle]' \in \{$"test", "Lb"$\}$
$\langle 4\rangle 1.$CASE $i = self \wedge j = oth$
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $pc'[\langle self, oth\rangle] =$ "L3", $Zenon$ DEF $NumInv$, $OtherProcs$, $SubProcs$
$\langle 4\rangle 2.$CASE $\neg(i = self \wedge j = oth)$
$\langle 5\rangle 1.$ UNCHANGED $pc[\langle i, j\rangle]$
BY $\langle 3\rangle 2$, $\langle 4\rangle 2$
$\langle 5\rangle$.QED BY ONLY $NumInv$, UNCHANGED $localCh$, $\langle 5\rangle 1$, $Zenon$ DEF $NumInv$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 3.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\wedge\ localNum[j][i]' = qm$

$\wedge \vee pc[\langle i \rangle]' = \text{"L"} \wedge pc[\langle i, j \rangle]' = \text{"test"}$
$\vee pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3 \rangle 3$ DEF $NumInv$
$\langle 3 \rangle$.QED BY ONLY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2 \rangle 11$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L3(\langle self, oth \rangle)$
PROVE $NumInv'$
$\langle 3 \rangle$. $\wedge\ pc[\langle self, oth \rangle] = \text{"L3"}$
$\wedge\ pc' = [pc$ EXCEPT $![\langle self, oth \rangle] = \text{"ch"}]$
$\wedge$ UNCHANGED $\langle number, localNum, localCh \rangle$
BY $\langle 2 \rangle 11$ DEF $L3$
$\langle 3 \rangle 1$. ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF $NumInv$
$\langle 3 \rangle 2$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
$\langle 4 \rangle 1$.CASE $i = self \wedge j = oth$
BY $\langle 3 \rangle 2$, $\langle 4 \rangle 1$, $pc'[\langle self, oth \rangle] = \text{"ch"}$, $Zenon$ DEF $NumInv$, $OtherProcs$, $SubProcs$
$\langle 4 \rangle 2$.CASE $\neg(i = self \wedge j = oth)$
$\langle 5 \rangle 1$. UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 3 \rangle 2$, $\langle 4 \rangle 2$
$\langle 5 \rangle$.QED BY ONLY $NumInv$, UNCHANGED $localCh$, $\langle 5 \rangle 1$, $Zenon$ DEF $NumInv$
$\langle 4 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$
$\langle 3 \rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\wedge\ localNum[j][i]' = qm$
$\wedge \vee pc[\langle i \rangle]' = \text{"L"} \wedge pc[\langle i, j \rangle]' = \text{"test"}$
$\vee pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY $\langle 3 \rangle 3$ DEF $NumInv$
$\langle 3 \rangle$.QED BY ONLY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2 \rangle 12$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$wrp(\langle self, oth, \text{"wr"} \rangle)$
PROVE $NumInv'$
$\langle 3 \rangle$. $\wedge\ pc[\langle self \rangle] \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
$\wedge\ localNum' = [localNum$ EXCEPT $![oth][self] = 0]$
$\wedge$ UNCHANGED $\langle pc, number, localCh \rangle$
BY $\langle 2 \rangle 12$ DEF wrp, wr
$\langle 3 \rangle 1$. ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i \rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY DEF $NumInv$
$\langle 3 \rangle 2$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$
PROVE $localCh[j][i]' = 1 \equiv pc[\langle i, j \rangle]' \in \{\text{"test"}, \text{"Lb"}\}$
BY ONLY $NumInv$, UNCHANGED $\langle pc, localCh \rangle$, $Zenon$ DEF $NumInv$
$\langle 3 \rangle 3$. ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$

PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\lor\ pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}, \text{"M0"}\}$
BY ⟨3⟩3, *POP_except* DEF *NumInv*, *OtherProcs*
⟨3⟩.QED BY ONLY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, *Zenon* DEF *NumInv*
⟨2⟩13.CASE UNCHANGED *vars*
BY ⟨2⟩13, *Isa* DEF *vars*, *NumInv*
⟨2⟩14. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9, ⟨2⟩10, ⟨2⟩11, ⟨2⟩12, ⟨2⟩13
DEF *Next*, *main*, *sub*, *ProcIds*, *SubProcs*, *WrProcs*, *OtherProcs*
⟨1⟩.QED BY ⟨1⟩1, ⟨1⟩2, *Typing*, *Synchronization*, *PTL* DEF *Spec*

The following properties are stated in the explanations of the various predicates.

LEMMA *inBakeryNum* $\triangleq$
ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$inBakery(i, j)$, *FullTypeOK*, *SyncInv*, *NumInv*
PROVE $\land\ number[i] \in Nat \setminus \{0\}$
$\land\ localNum[j][i] = number[i]$
BY DEF *inBakery*, *FullTypeOK*, *SyncInv*, *NumInv*

LEMMA *passedInBakery* $\triangleq$
ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$, NEW *LL*
PROVE $\land\ passed(i, j, LL) \Rightarrow inBakery(i, j)$
$\land\ passed(i, j, LL)' \Rightarrow inBakery(i, j)'$
BY DEF *passed*, *inBakery*

We now prove the main invariant of the algorithm.

THEOREM *Invariance* $\triangleq$ $Spec \Rightarrow \Box I$
⟨1⟩1. $Init \Rightarrow I$
BY *Zenon*
DEF *Init*, *I*, *OtherProcs*, *Inv*, *inBakery*, *passed*,
ProcSet, *ProcIds*, *SubProcs*, *WrProcs*
⟨1⟩2. $FullTypeOK \land SyncInv \land NumInv \land I \land [Next]_{vars} \Rightarrow I'$
⟨2⟩ SUFFICES ASSUME *FullTypeOK*, *SyncInv*, *NumInv*,
I,
$[Next]_{vars}$
PROVE I'
OBVIOUS
⟨2⟩.USE DEF *FullTypeOK*
⟨2⟩1. ASSUME NEW $self \in Procs$,
$ncs(\langle self \rangle)$
PROVE I'
⟨3⟩.USE ⟨2⟩1 DEF *ncs*

$\langle 3\rangle 1.\ \forall\, i,\, j \in Procs : inBakery(i,\, j)' \equiv inBakery(i,\, j)$

BY DEF $inBakery$

$\langle 3\rangle 2.\ \forall\, i,\, j \in Procs : \forall\, w \in Nat : inDoorwayVal(i,\, j,\, w)' \equiv inDoorwayVal(i,\, j,\, w)$

BY DEF $inDoorwayVal$

$\langle 3\rangle 3.\ \forall\, i,\, j \in Procs : inDoorway(i,\, j)' \equiv inDoorway(i,\, j)$

BY DEF $inDoorway$

$\langle 3\rangle 4.\ \forall\, i,\, j \in Procs :$

$\land\, passed(i,\, j,\, \text{“L2”})' \equiv passed(i,\, j,\, \text{“L2”})$

$\land\, passed(i,\, j,\, \text{“L3”})' \equiv passed(i,\, j,\, \text{“L3”})$

BY DEF $passed$

$\langle 3\rangle 5.\ \forall\, i,\, j \in Procs : Before(i,\, j)' \equiv Before(i,\, j)$

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEF $Before$, $Outside$

$\langle 3\rangle$.QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF I, Inv, $OtherProcs$

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

$M(\langle self\rangle)$

PROVE I'

$\langle 3\rangle$.USE $\langle 2\rangle 2$ DEF M

$\langle 3\rangle 1.\ \forall\, i,\, j \in Procs : inBakery(i,\, j)' \equiv inBakery(i,\, j)$

BY DEF $inBakery$

$\langle 3\rangle 2.\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) : \forall\, w \in Nat :$

$inDoorwayVal(i,\, j,\, w)' \equiv inDoorwayVal(i,\, j,\, w)$

BY DEF $inDoorwayVal$

$\langle 3\rangle 3.\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) :$

$inDoorway(i,\, j)' \equiv inDoorway(i,\, j)$

BY DEF $inDoorway$

$\langle 3\rangle 4.\ \forall\, i,\, j \in Procs :$

$\land\, passed(i,\, j,\, \text{“L2”})' \equiv passed(i,\, j,\, \text{“L2”})$

$\land\, passed(i,\, j,\, \text{“L3”})' \equiv passed(i,\, j,\, \text{“L3”})$

BY DEF $passed$

$\langle 3\rangle 5.\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) : Before(i,\, j)' \equiv Before(i,\, j)$

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEF $Before$, $Outside$, $OtherProcs$

$\langle 3\rangle$.QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF I, Inv, $OtherProcs$

$\langle 2\rangle 3.$ ASSUME NEW $self \in Procs$,

$M0(\langle self\rangle)$

PROVE I'

$\langle 3\rangle 1.$CASE $unRead[\langle self\rangle] \neq \{\}$

$\langle 4\rangle$.PICK $j \in unRead[\langle self\rangle] :$

$\land\, pc[\langle self\rangle] = \text{“M0”}$

$\land$ IF $localNum[self][j] \neq qm$

THEN $v' = [v$ EXCEPT $![\langle self\rangle] = Max(v[\langle self\rangle],\, localNum[self][j])]$

ELSE $v' = v$

$\land\, unRead' = [unRead$ EXCEPT $![\langle self\rangle] = unRead[\langle self\rangle] \setminus \{j\}]$

$\land$ UNCHANGED $\langle pc,\, number\rangle$

BY ⟨2⟩3, ⟨3⟩1 DEF $M0$

⟨4⟩. $\land j \in Procs$
$\land j \in OtherProcs(self)$
$\land self \in OtherProcs(j)$

BY DEF $ProcIds$, $OtherProcs$

⟨4⟩1. $\forall p, q \in Procs : inBakery(p, q)' \equiv inBakery(p, q)$

BY DEF $inBakery$

⟨4⟩2. $\forall p \in Procs : \forall q \in OtherProcs(p) :$
$inDoorway(p, q)' \equiv \lor self = p \land q = j$
$\lor inDoorway(p, q)$

BY DEF $inDoorway$, $OtherProcs$, $ProcIds$

⟨4⟩3. ASSUME $localNum[self][j] \neq qm$
PROVE $inDoorwayVal(self, j, number[j])'$

⟨5⟩1. $v'[\langle self \rangle] \geq localNum[self][j]$

BY ⟨4⟩3 DEF $ProcIds$, POP, $PFunc$, Max

⟨5⟩2. $NumInv!(j)!2!(self)$

BY DEF $NumInv$

⟨5⟩.QED BY ⟨4⟩3, ⟨5⟩1, ⟨5⟩2 DEF $inDoorwayVal$, $ProcIds$

⟨4⟩4. $\forall p, q \in Procs :$
$\land passed(p, q, \text{“L2”})' \equiv passed(p, q, \text{“L2”})$
$\land passed(p, q, \text{“L3”})' \equiv passed(p, q, \text{“L3”})$

BY DEF $passed$

⟨4⟩5. ASSUME NEW $p \in Procs \setminus \{self\}$, NEW $q \in OtherProcs(p)$,
$q \neq self \lor p \neq j$
PROVE $Before(q, p)' \equiv Before(q, p)$

⟨5⟩. $Outside(p, q)' \equiv Outside(p, q)$

BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩5 DEF $Outside$, $OtherProcs$

⟨5⟩.UNCHANGED $v[\langle p \rangle]$

BY ⟨4⟩5 DEF $ProcIds$, $OtherProcs$

⟨5⟩.QED BY ⟨4⟩1, ⟨4⟩4, ⟨4⟩5 DEF $Before$, $inDoorwayVal$, $OtherProcs$

For the converse relation we only have an implication.

⟨4⟩6. ASSUME NEW $p \in Procs \setminus \{self\}$, NEW $q \in OtherProcs(p)$,
$q \neq self \lor p \neq j$
PROVE $Before(p, q) \Rightarrow Before(p, q)'$

⟨5⟩1. $Outside(q, p)' \equiv Outside(q, p)$

BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩6 DEF $Outside$, $OtherProcs$

⟨5⟩2. $inDoorwayVal(q, p, number[p]) \Rightarrow inDoorwayVal(q, p, number[p])'$

⟨6⟩. $p \in unRead'[\langle q \rangle] \equiv p \in unRead[\langle q \rangle]$

BY ⟨4⟩6

⟨6⟩. $v[\langle q \rangle] \geq number[p] \Rightarrow v[\langle q \rangle]' \geq number'[p]$

⟨7⟩1.CASE $q = self$

BY ⟨7⟩1 DEF $ProcIds$, $OtherProcs$, Max, POP, $PFunc$

⟨7⟩2.CASE $q \neq self$

BY ⟨7⟩2 DEF $ProcIds$, $OtherProcs$

⟨7⟩.QED BY ⟨4⟩6, ⟨7⟩1, ⟨7⟩2

$\langle 6 \rangle$.QED BY DEF *inDoorwayVal*
$\langle 5 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 4$, $\langle 5 \rangle 1$, $\langle 5 \rangle 2$ DEF *Before*, *OtherProcs*
$\langle 4 \rangle 7$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, $inBakery(p, q)$
PROVE $Before(p, q)' \lor Before(q, p)' \lor inDoorway(q, p)'$
$\langle 5 \rangle 1$.CASE $p = self$ $\neg inBakery(p, q)$
BY $\langle 4 \rangle 7$, $\langle 5 \rangle 1$ DEF *inBakery*, *SyncInv*
$\langle 5 \rangle 2$.CASE $q = self \land p = j$ $inDoorway(self, j)'$
BY $\langle 4 \rangle 2$, $\langle 5 \rangle 2$ DEF *OtherProcs*
$\langle 5 \rangle 3$.CASE $p \neq self \land (q \neq self \lor p \neq j)$
BY $\langle 4 \rangle 2$, $\langle 4 \rangle 5$, $\langle 4 \rangle 6$, $\langle 4 \rangle 7$, $\langle 5 \rangle 3$ DEF *I*, *Inv*, *OtherProcs*
$\langle 5 \rangle$.QED BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$
$\langle 4 \rangle 8$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, $passed(p, q, \text{"L2"})$
PROVE $Before(p, q)' \lor Before(q, p)'$
$\langle 5 \rangle 1$.CASE $p = self$ $\neg passed(self, q, \text{"L2"})$
BY $\langle 4 \rangle 8$, $\langle 5 \rangle 1$ DEF *passed*, *SyncInv*
$\langle 5 \rangle 2$.CASE $q = self \land p = j$
$\langle 6 \rangle 1$. $inBakery(j, self)$
BY $\langle 4 \rangle 8$, $\langle 5 \rangle 2$ DEF *passed*, *inBakery*
$\langle 6 \rangle 2$. $localNum[self][j] \neq qm$
BY $\langle 6 \rangle 1$, *inBakeryNum*, *qmNotNat* DEF *POP*, *PFunc*
$\langle 6 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 3$, $\langle 5 \rangle 2$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$ DEF *Before*
$\langle 5 \rangle 3$.CASE $p \neq self \land (q \neq self \lor p \neq j)$
BY $\langle 4 \rangle 5$, $\langle 4 \rangle 6$, $\langle 4 \rangle 8$, $\langle 5 \rangle 3$ DEF *I*, *Inv*, *OtherProcs*
$\langle 5 \rangle$.QED BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$
$\langle 4 \rangle 9$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, $passed(p, q, \text{"L3"})$
PROVE $Before(p, q)'$
$\langle 5 \rangle 1$.CASE $p = self$ $\neg passed(self, q, \text{"L3"})$
BY $\langle 4 \rangle 9$, $\langle 5 \rangle 1$ DEF *passed*, *SyncInv*
$\langle 5 \rangle 2$.CASE $q = self \land p = j$
$\langle 6 \rangle 1$. $inBakery(j, self)$
BY $\langle 4 \rangle 9$, $\langle 5 \rangle 2$ DEF *passed*, *inBakery*
$\langle 6 \rangle 2$. $localNum[self][j] \neq qm$
BY $\langle 6 \rangle 1$, *inBakeryNum*, *qmNotNat*, *Isa* DEF *POP*, *PFunc*
$\langle 6 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 3$, $\langle 5 \rangle 2$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$ DEF *Before*
$\langle 5 \rangle 3$.CASE $p \neq self \land (q \neq self \lor p \neq j)$
BY $\langle 4 \rangle 5$, $\langle 4 \rangle 6$, $\langle 4 \rangle 9$, $\langle 5 \rangle 3$ DEF *I*, *Inv*, *OtherProcs*
$\langle 5 \rangle$.QED BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$
$\langle 4 \rangle$.QED BY $\langle 4 \rangle 1$, $\langle 4 \rangle 4$, $\langle 4 \rangle 7$, $\langle 4 \rangle 8$, $\langle 4 \rangle 9$ DEF *OtherProcs*, *I*, *Inv*
$\langle 3 \rangle 2$.CASE $unRead[\langle self \rangle] = \{\}$
$\langle 4 \rangle$.PICK $n \in Nat$:
$\land pc[\langle self \rangle] = \text{"M0"}$
$\land n > v[\langle self \rangle]$
$\land number' = [number \text{ EXCEPT } ![self] = n]$
$\land localNum' = [j \in Procs \mapsto$
$[i \in OtherProcs(j) \mapsto$

```
                                   IF i = self THEN qm
                                                ELSE localNum[j][i]]]
              ∧ v' = [v EXCEPT ![⟨self⟩] = 0]
              ∧ pc' = [pc EXCEPT ![⟨self⟩] = "L"]
              ∧ UNCHANGED unRead
      BY ⟨2⟩3, ⟨3⟩2 DEF M0
    ⟨4⟩1. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
          PROVE inBakery(p, q)' ≡ inBakery(p, q)
      BY DEF inBakery, SyncInv
    ⟨4⟩2. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
          PROVE inDoorway(p, q)' ≡ inDoorway(p, q)
      BY ⟨3⟩2 DEF inDoorway, SyncInv
    ⟨4⟩3. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p), NEW w ∈ Nat
          PROVE inDoorwayVal(p, q, w) ⇒ inDoorwayVal(p, q, w)'
       Here we only have an implication since for p = self we
       cannot conclude v[⟨self⟩] ≥ w from number'[self] ≥ w.
      BY ⟨3⟩2 DEF inDoorwayVal, SyncInv, ProcIds
    ⟨4⟩4. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
          PROVE ∧ passed(p, q, "L2")' ≡ passed(p, q, "L2")
                ∧ passed(p, q, "L3")' ≡ passed(p, q, "L3")
      BY DEF passed, SyncInv
    ⟨4⟩5. ∀ p ∈ OtherProcs(self) : ¬inBakery(self, p)
      BY DEF inBakery, SyncInv
    ⟨4⟩6. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
          PROVE Before(p, q) ⇒ Before(p, q)'
      BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, ⟨4⟩5, Zenon DEF Before, Outside, OtherProcs
    ⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩4, ⟨4⟩6 DEF I, Inv, OtherProcs
  ⟨3⟩.QED BY ⟨3⟩1, ⟨3⟩2
⟨2⟩4. ASSUME NEW self ∈ Procs,
             L(⟨self⟩)
      PROVE I'
  ⟨3⟩. ∧ pc[⟨self⟩] = "L"
       ∧ ∀ p ∈ SubProcsOf(self) : pc[p] = "ch"
       ∧ pc' = [pc EXCEPT ![⟨self⟩] = "cs"]
       ∧ UNCHANGED ⟨number, unRead, v⟩
    BY ⟨2⟩4 DEF L
  ⟨3⟩1. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE inBakery(p, q)' ≡ inBakery(p, q)
    BY DEF inBakery
  ⟨3⟩2. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE inDoorway(p, q)' ≡ inDoorway(p, q)
    BY DEF inDoorway, ProcIds, SubProcsOf, SubProcs, OtherProcs
  ⟨3⟩3. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p), NEW w ∈ Nat
        PROVE inDoorwayVal(p, q, w)' ≡ inDoorwayVal(p, q, w)
    BY DEF inDoorwayVal, ProcIds, SubProcsOf, SubProcs, OtherProcs
```

$\langle 3 \rangle 4.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $\land\, passed(p, q, \text{“L2”})' \equiv passed(p, q, \text{“L2”})$
$\land\, passed(p, q, \text{“L3”})' \equiv passed(p, q, \text{“L3”})$
BY DEF $passed$, $SubProcsOf$, $SubProcs$, $OtherProcs$, $ProcIds$
$\langle 3 \rangle$.QED BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$ DEF I, Inv, $Before$, $Outside$, $OtherProcs$
$\langle 2 \rangle 5.$ ASSUME NEW $self \in Procs$,
$cs(\langle self \rangle)$
PROVE I'
$\langle 3 \rangle.$ $\land\, pc[\langle self \rangle] = \text{“cs”}$
$\land\, pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{“P”}]$
$\land$ UNCHANGED $\langle number, unRead, v \rangle$
BY $\langle 2 \rangle 5$ DEF cs
$\langle 3 \rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q) \land p \neq self$
BY DEF $inBakery$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$
BY DEF $inDoorway$
$\langle 3 \rangle 3.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$
BY DEF $inDoorwayVal$
$\langle 3 \rangle 4.$ ASSUME NEW $p \in Procs \setminus \{self\}$, NEW $q \in OtherProcs(p)$
PROVE $\land\, passed(p, q, \text{“L2”})' \equiv passed(p, q, \text{“L2”})$
$\land\, passed(p, q, \text{“L3”})' \equiv passed(p, q, \text{“L3”})$
BY DEF $passed$
$\langle 3 \rangle 5.$ $\forall\, q \in OtherProcs(self)$:
$\land\, passed(self, q, \text{“L2”}) \land \neg passed(self, q, \text{“L2”})'$
$\land\, passed(self, q, \text{“L3”}) \land \neg passed(self, q, \text{“L3”})'$
BY DEF $passed$, $SyncInv$, $ProcIds$
$\langle 3 \rangle 6.$ ASSUME NEW $p \in Procs \setminus \{self\}$, NEW $q \in OtherProcs(p) \setminus \{self\}$
PROVE $Before(p, q) \Rightarrow Before(p, q)'$
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$ DEF $Before$, $Outside$, $OtherProcs$
$\langle 3 \rangle 7.$ $\forall\, q \in OtherProcs(self) : inBakery(q, self)' \Rightarrow Before(q, self)'$
BY $\langle 3 \rangle 1$ DEF $Before$, $Outside$, $inDoorway$ have $Outside(self, q)'$
$\langle 3 \rangle$.QED
BY $passedInBakery$, $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$, $\langle 3 \rangle 7$ DEF $OtherProcs$, I, Inv
$\langle 2 \rangle 6.$ ASSUME NEW $self \in Procs$,
$P(\langle self \rangle)$
PROVE I'
$\langle 3 \rangle.$ $\land\, pc[\langle self \rangle] = \text{“P”}$
$\land\, number' = [number \text{ EXCEPT } ![self] = 0]$
$\land\, pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{“ncs”}]$
$\land$ UNCHANGED $\langle unRead, v \rangle$
BY $\langle 2 \rangle 6$ DEF P
$\langle 3 \rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$
⟨3⟩2. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$
BY DEF $inDoorway$
⟨3⟩3. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$
BY DEF $inDoorwayVal$
⟨3⟩4. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $\land\, passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"})$
$\land\, passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$
BY DEF $passed$
⟨3⟩5. $\forall q \in OtherProcs(self) : \neg inBakery(self, q)$
BY DEF $inBakery$, $SyncInv$
⟨3⟩9. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $Before(p, q) \Rightarrow Before(p, q)'$
⟨4⟩1.CASE $q = self$ follows from $Outside(self, p)'$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩5, ⟨3⟩9, ⟨4⟩1 DEF $Before$, $inDoorway$, $Outside$, $OtherProcs$
⟨4⟩2.CASE $q \neq self$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩9, ⟨4⟩2 DEF $Before$, $OtherProcs$, $Outside$
⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
⟨3⟩.QED BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩4, ⟨3⟩9 DEF I, Inv, $OtherProcs$
⟨2⟩7. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$ch(\langle self, oth \rangle)$
PROVE I'
⟨3⟩. $\land\, pc[\langle self, oth \rangle] = \text{"ch"}$
$\land\, pc[\langle self \rangle] = \text{"M"}$
$\land\, pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{"test"}]$
$\land$ UNCHANGED $\langle number, unRead, v \rangle$
BY ⟨2⟩7 DEF ch
⟨3⟩1. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$
⟨3⟩2. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$
BY DEF $inDoorway$
⟨3⟩3. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$
BY DEF $inDoorwayVal$
⟨3⟩4. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $\land\, passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"})$
$\land\, passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$
BY DEF $passed$
⟨3⟩.QED BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4 DEF I, Inv, $Before$, $OtherProcs$, $Outside$
⟨2⟩8. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,

$\quad\quad test(\langle self, oth \rangle)$

PROVE I'

$\langle 3 \rangle.\ \wedge pc[\langle self, oth \rangle] = \text{“test”}$
$\quad \wedge pc[\langle self \rangle] = \text{“L”}$
$\quad \wedge pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{“Lb”}]$
$\quad \wedge \text{UNCHANGED } \langle number, unRead, v \rangle$

BY $\langle 2 \rangle 8$ DEF $test$

$\langle 3 \rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q) \vee (p = self \wedge q = oth)$

BY DEF $inBakery, ProcIds, SubProcs, OtherProcs$

$\langle 3 \rangle 2.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q) \wedge \neg(p = self \wedge q = oth)$

BY DEF $inDoorway, ProcIds, SubProcs, OtherProcs$

$\langle 3 \rangle 3.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w) \wedge \neg(p = self \wedge q = oth)$

BY DEF $inDoorwayVal, ProcIds, SubProcs, OtherProcs$

$\langle 3 \rangle 4.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $\wedge passed(p, q, \text{“L2”})' \equiv passed(p, q, \text{“L2”})$
$\quad\quad \wedge passed(p, q, \text{“L3”})' \equiv passed(p, q, \text{“L3”})$

BY DEF $passed$

$\langle 3 \rangle 5.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, $Before(p, q)$
PROVE $Before(p, q)'$

$\langle 4 \rangle 1.$CASE $p = oth \wedge q = self$

$\langle 5 \rangle 1.$ $inBakery(oth, self)' \wedge inBakery(self, oth)'$
BY $\langle 3 \rangle 5, \langle 3 \rangle 1, \langle 4 \rangle 1$ DEF $Before, OtherProcs$

$\langle 5 \rangle 2.$ $inDoorway(self, oth) \wedge \neg inBakery(self, oth)$
BY DEF $inDoorway, inBakery$

$\langle 5 \rangle 3.$ $inDoorwayVal(self, oth, number[oth])$
BY $\langle 3 \rangle 5, \langle 4 \rangle 1, \langle 5 \rangle 2$ DEF $Before, Outside$

$\langle 5 \rangle 4.$ $\langle number[oth], oth \rangle \ll \langle number[self], self \rangle$
BY $\langle 5 \rangle 3$ DEF $inDoorwayVal, \ll, OtherProcs$

$\langle 5 \rangle.$QED BY $\langle 4 \rangle 1, \langle 5 \rangle 1, \langle 5 \rangle 4$ DEF $Before, passed$

$\langle 4 \rangle 2.$CASE $p \neq oth \vee q \neq self$
BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4, \langle 3 \rangle 5, \langle 4 \rangle 2$ DEF $Before, Outside, OtherProcs$

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

$\langle 3 \rangle 6.$ ASSUME $inBakery(oth, self)$
PROVE $Before(self, oth)' \vee Before(oth, self)'$

$\langle 4 \rangle 1.$ $inBakery(self, oth)' \wedge inBakery(oth, self)'$
BY $\langle 3 \rangle 6, \langle 3 \rangle 1$ DEF $OtherProcs$

$\langle 4 \rangle 2.$ $\neg passed(self, oth, \text{“L3”})'$
BY DEF $passed$

$\langle 4 \rangle 3.$CASE $passed(oth, self, \text{“L3”})$ — $Before(oth, self)$, hence $Before(oth, self)'$
BY $\langle 4 \rangle 3, \langle 3 \rangle 5$ DEF $I, Inv, OtherProcs$

$\langle 4 \rangle 4.$CASE $\neg passed(oth, self, \text{“L3”})$ — $Before(self, oth)' \vee Before(oth, self)'$
BY $\langle 4 \rangle 1, \langle 4 \rangle 2, \langle 4 \rangle 4, \langle 3 \rangle 4, TotalOrder$ DEF $Before, OtherProcs$

```
    ⟨4⟩.QED  BY ⟨4⟩3, ⟨4⟩4
  ⟨3⟩7. Before(self, oth)′ ∨ Before(oth, self)′ ∨ inDoorway(oth, self)′
    ⟨4⟩1.CASE Outside(oth, self)   inBakery(self, oth)′ ∧ Outside(oth, self)′
      BY ⟨4⟩1, ⟨3⟩1, ⟨3⟩2  DEF Before, Outside, OtherProcs
    ⟨4⟩2.CASE inDoorway(oth, self)   inDoorway(oth, self)′
      BY ⟨4⟩2, ⟨3⟩2  DEF OtherProcs
    ⟨4⟩3.CASE inBakery(oth, self)
      BY ⟨4⟩3, ⟨3⟩6
    ⟨4⟩.QED  BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3  DEF Outside
  ⟨3⟩.QED  BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7  DEF I, Inv, OtherProcs
⟨2⟩9. ASSUME NEW self ∈ Procs, NEW oth ∈ OtherProcs(self),
             Lb(⟨self, oth⟩)
      PROVE  I′
  ⟨3⟩. ∧ pc[⟨self, oth⟩] = "Lb"
       ∧ pc′ = [pc EXCEPT ![⟨self, oth⟩] = "L2"]
       ∧ UNCHANGED ⟨number, unRead, v⟩
    BY ⟨2⟩9  DEF Lb
  ⟨3⟩1. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE  inBakery(p, q)′ ≡ inBakery(p, q)
    BY DEF inBakery
  ⟨3⟩2. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE  inDoorway(p, q)′ ≡ inDoorway(p, q)
    BY DEF inDoorway
  ⟨3⟩3. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p), NEW w ∈ Nat
        PROVE  inDoorwayVal(p, q, w)′ ≡ inDoorwayVal(p, q, w)
    BY DEF inDoorwayVal
  ⟨3⟩4. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE  ∧ passed(p, q, "L2")′ ≡ passed(p, q, "L2")
               ∧ passed(p, q, "L3")′ ≡ passed(p, q, "L3")
    BY DEF passed
  ⟨3⟩.QED  BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4  DEF I, Inv, Before, Outside, OtherProcs
⟨2⟩10. ASSUME NEW self ∈ Procs, NEW oth ∈ OtherProcs(self),
              L2(⟨self, oth⟩)
       PROVE  I′
  ⟨3⟩. ∧ pc[⟨self, oth⟩] = "L2"
       ∧ localCh[self][oth] = 0
       ∧ pc′ = [pc EXCEPT ![⟨self, oth⟩] = "L3"]
       ∧ UNCHANGED ⟨number, unRead, v⟩
    BY ⟨2⟩10  DEF L2
  ⟨3⟩1. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE  inBakery(p, q)′ ≡ inBakery(p, q)
    BY DEF inBakery
  ⟨3⟩2. ASSUME NEW p ∈ Procs, NEW q ∈ OtherProcs(p)
        PROVE  inDoorway(p, q)′ ≡ inDoorway(p, q)
    BY DEF inDoorway
```

$\langle 3\rangle 3.\ \neg inDoorway(oth, self)$
BY DEF $inDoorway$, $NumInv$, $SyncInv$, $OtherProcs$
$\langle 3\rangle 4.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$
BY DEF $inDoorwayVal$
$\langle 3\rangle 5.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $\land\ passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"}) \lor (p = self \land q = oth)$
$\land\ passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$
BY DEF $passed$, $ProcIds$, $SubProcs$, $OtherProcs$
$\langle 3\rangle 6.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $Before(p, q)' \equiv Before(p, q)$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF $Before$, $Outside$, $OtherProcs$
$\langle 3\rangle$.QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $passedInBakery$ DEF I, Inv, $OtherProcs$
$\langle 2\rangle 11.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L3(\langle self, oth\rangle)$
PROVE I'
$\langle 3\rangle.\ \land\ pc[\langle self, oth\rangle] = \text{"L3"}$
$\land\ \lor\ localNum[self][oth] \in \{0, qm\}$
$\lor\ \langle number[self], self\rangle \ll \langle localNum[self][oth], oth\rangle$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle self, oth\rangle] = \text{"ch"}]$
$\land$ UNCHANGED $\langle number, unRead, v\rangle$
BY $\langle 2\rangle 11$ DEF $L3$
$\langle 3\rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$
$\langle 3\rangle 2.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$
BY DEF $inDoorway$
$\langle 3\rangle 3.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$
PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$
BY DEF $inDoorwayVal$
$\langle 3\rangle 4.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"})$
$\langle 4\rangle 1.$CASE $p = self \land q = oth$
BY $\langle 4\rangle 1$ DEF $passed$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$
$\langle 4\rangle 2.$CASE $p \neq self \lor q \neq oth$
BY $\langle 4\rangle 2$ DEF $passed$
$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 5.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"}) \lor (p = self \land q = oth)$
$\langle 4\rangle 1.\ passed(p, q, \text{"L3"}) \lor (p = self \land q = oth) \Rightarrow passed(p, q, \text{"L3"})'$
BY DEF $passed$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$
$\langle 4\rangle 2.\ passed(p, q, \text{"L3"})' \land \neg(p = self \land q = oth) \Rightarrow passed(p, q, \text{"L3"})$
BY DEF $passed$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$

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

$\langle 3\rangle 6$. $passed(self, oth, \text{“L2”})$

BY DEF $passed$

$\langle 3\rangle 7$. ASSUME $Before(oth, self)$ PROVE FALSE

$\langle 4\rangle 1$. $inBakery(oth, self)$

BY $\langle 3\rangle 7$ DEF $Before$

$\langle 4\rangle 2$. $\neg Outside(self, oth)$

BY DEF $Outside$, $inBakery$

$\langle 4\rangle 3$. $\neg inDoorwayVal(self, oth, number[oth])$

BY DEF $inDoorwayVal$, $SyncInv$

$\langle 4\rangle 4$. $\langle number[oth], oth\rangle \ll \langle number[self], self\rangle$

BY $\langle 3\rangle 7$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $Before$

$\langle 4\rangle 5$. $\land\ number[oth] = localNum[self][oth]$

$\land\ number[oth] \in Nat \setminus \{0\}$

BY $inBakeryNum$, $\langle 4\rangle 1$, $Zenon$ DEF $OtherProcs$

$\langle 4\rangle 6$. $\langle number[self], self\rangle \ll \langle number[oth], oth\rangle$

BY $\langle 4\rangle 5$, $qmNotNat$

$\langle 4\rangle$.QED BY $\langle 4\rangle 6$, $\langle 4\rangle 4$, $AsymmetricOrder$ DEF $OtherProcs$

$\langle 3\rangle 8$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, $q \neq self \lor p \neq oth$

PROVE $Before(p, q)' \equiv Before(p, q)$

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 5$, $\langle 3\rangle 8$ DEF $Before$, $Outside$, $OtherProcs$

$\langle 3\rangle$.QED BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$, $\langle 3\rangle 8$ DEF I, Inv, $OtherProcs$

$\langle 2\rangle$X.CASE UNCHANGED $\langle pc, number, unRead, v\rangle$

$\langle 3\rangle 1$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

PROVE $inBakery(p, q)' \equiv inBakery(p, q)$

BY $\langle 2\rangle$X DEF $inBakery$

$\langle 3\rangle 2$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$

BY $\langle 2\rangle$X DEF $inDoorway$

$\langle 3\rangle 4$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$, NEW $w \in Nat$

PROVE $inDoorwayVal(p, q, w)' \equiv inDoorwayVal(p, q, w)$

BY $\langle 2\rangle$X DEF $inDoorwayVal$

$\langle 3\rangle 5$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

PROVE $\land\ passed(p, q, \text{“L2”})' \equiv passed(p, q, \text{“L2”})$

$\land\ passed(p, q, \text{“L3”})' \equiv passed(p, q, \text{“L3”})$

BY $\langle 2\rangle$X DEF $passed$

$\langle 3\rangle 6$. ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

PROVE $Before(p, q)' \equiv Before(p, q)$

BY $\langle 2\rangle$X, $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 5$ DEF $Before$, $Outside$, $OtherProcs$

$\langle 3\rangle$.QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF I, Inv, $OtherProcs$

$\langle 2\rangle 12$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,

$wr(\langle self, oth, \text{“wr”}\rangle)$

PROVE I'

BY $\langle 2\rangle 12$, $\langle 2\rangle$X DEF wr

$\langle 2\rangle 13.$CASE UNCHANGED *vars*
BY $\langle 2\rangle 13$, $\langle 2\rangle$X DEF *vars*
$\langle 2\rangle 14.$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 2\rangle 9$, $\langle 2\rangle 10$, $\langle 2\rangle 11$, $\langle 2\rangle 12$, $\langle 2\rangle 13$
DEF *Next*, *main*, *sub*, *ProcIds*, *SubProcs*, *WrProcs*, *wrp*, *OtherProcs*
$\langle 1\rangle$.QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, *Typing*, *Synchronization*, *NumberInvariant*, *PTL* DEF *Spec*

It follows that the algorithm guarantees mutual exclusion.

THEOREM $Spec \Rightarrow \Box MutualExclusion$
$\langle 1\rangle 1.$ $FullTypeOK \land SyncInv \land I \Rightarrow MutualExclusion$
$\langle 2\rangle$.SUFFICES ASSUME *FullTypeOK*, *SyncInv*, *I*,
NEW $p \in Procs$, NEW $q \in Procs$, $q \neq p$,
$pc[\langle p\rangle] =$ "cs", $pc[\langle q\rangle] =$ "cs"
PROVE FALSE
BY DEF *MutualExclusion*, *ProcIds*
$\langle 2\rangle 1.$ $passed(p, q, \text{"L3"}) \land passed(q, p, \text{"L3"})$
BY DEF *passed*, *SyncInv*, *OtherProcs*
$\langle 2\rangle 2.$ $Before(p, q) \land Before(q, p)$
BY $\langle 2\rangle 1$ DEF *I*, *Inv*, *OtherProcs*
$\langle 2\rangle 3.$ $\neg Outside(p, q) \land \neg Outside(q, p)$
BY DEF *Outside*, *inBakery*, *SyncInv*, *OtherProcs*
$\langle 2\rangle 4.$ $\neg inDoorwayVal(p, q, number[q]) \land \neg inDoorwayVal(q, p, number[p])$
BY DEF *inDoorwayVal*
$\langle 2\rangle 5.$ $\land \langle number[p], p\rangle \ll \langle number[q], q\rangle$
$\land \langle number[q], q\rangle \ll \langle number[p], p\rangle$
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$ DEF *Before*
$\langle 2\rangle$.QED BY $\langle 2\rangle 5$, *AsymmetricOrder* DEF *FullTypeOK*
$\langle 1\rangle$.QED BY $\langle 1\rangle 1$, *Typing*, *Synchronization*, *Invariance*, *PTL*

---

* Modification History
* Last modified *Wed Nov* 17 18:50:05 *CET* 2021 by *merz*
* Created *Thu Jul* 01 12:26:36 *CEST* 2021 by *merz*