MODULE *DeconProofAtomic*

Proofs for the deconstructed Bakery with atomic choice of tickets.

EXTENDS *BakeryDeconstructedAtomic*, *TLAPS*

USE *NAssump*

The *TypeOK* predicate does not quite assert the types of the variables *localNum* and *localCh*, and it doesn't cover the types of the local variables. The following predicate is more precise.

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

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 $self \in Procs$,
            $ncs(\langle self \rangle)$
      PROVE $FullTypeOK'$
    BY $\langle 2 \rangle 1$ DEF *ncs*, *ProcIds*, *SubProcs*, *WrProcs*
  $\langle 2 \rangle 2.$ ASSUME NEW $self \in Procs$,
            $M(\langle self \rangle)$
      PROVE $FullTypeOK'$
    BY $\langle 2 \rangle 2$ DEF *M*, *POP*, *PFunc*, *ProcIds*, *SubProcs*, *WrProcs*
  $\langle 2 \rangle 3.$ ASSUME NEW $self \in Procs$,

$L(\langle self \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 3$ DEF L, $ProcIds$, $SubProcs$, $WrProcs$
$\langle 2 \rangle 4.$ ASSUME NEW $self \in Procs$,
$cs(\langle self \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 4$ DEF cs, $ProcIds$, $SubProcs$, $WrProcs$
$\langle 2 \rangle 5.$ ASSUME NEW $self \in Procs$,
$P(\langle self \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 5$ DEF P, POP, $PFunc$, $ProcIds$, $SubProcs$, $WrProcs$
$\langle 2 \rangle 6.$ 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, $OtherProcs$
$\langle 2 \rangle 7.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$test(\langle self, oth \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 7$, POP_except, $Zenon$ DEF $test$, $OtherProcs$
$\langle 2 \rangle 8.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$Lb(\langle self, oth \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 8$, POP_except, $Zenon$ DEF Lb, $OtherProcs$
$\langle 2 \rangle 9.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L2(\langle self, oth \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 9$, $Zenon$ DEF $L2$
$\langle 2 \rangle 10.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L3(\langle self, oth \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 10$, $Zenon$ DEF $L3$
$\langle 2 \rangle 11.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$wr(\langle self, oth, \text{"wr"} \rangle)$
PROVE $FullTypeOK'$
BY $\langle 2 \rangle 11$, POP_except, $Zenon$ DEF wr, $OtherProcs$
$\langle 2 \rangle 12.$CASE UNCHANGED $vars$
BY $\langle 2 \rangle 12$ DEF $vars$
$\langle 2 \rangle$.HIDE DEF $FullTypeOK$
$\langle 2 \rangle 13.$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 9$, $\langle 2 \rangle 10$, $\langle 2 \rangle 11$, $\langle 2 \rangle 12$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, $\langle 2 \rangle 8$
DEF $Next$, $main$, sub, wrp, $ProcIds$, $SubProcs$, $WrProcs$, $OtherProcs$
$\langle 1 \rangle$.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.

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

THEOREM $Synchronization \triangleq Spec \Rightarrow \Box SyncInv$
$\langle 1 \rangle 1.$ $Init \Rightarrow SyncInv$
  BY $DisjointIds$, $Zenon$ DEF $Init$, $OtherProcs$, $ProcSet$, $ProcIds$, $SubProcs$, $SyncInv$
$\langle 1 \rangle 2.$ $FullTypeOK \land SyncInv \land [Next]_{vars} \Rightarrow SyncInv'$
  $\langle 2 \rangle$ SUFFICES ASSUME $FullTypeOK$,
                 $SyncInv$,
                 $[Next]_{vars}$
           PROVE $SyncInv'$
    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 $self \in Procs$, NEW $i \in Procs \setminus \{self\}$,
           UNCHANGED $pc[\langle i \rangle]$,
           $\forall j \in OtherProcs(i)$: UNCHANGED $pc[\langle i, j \rangle]$
       PROVE $SyncInv!(i)'$
    BY $\langle 2 \rangle 1$
  $\langle 2 \rangle 2.$ ASSUME NEW $self \in Procs$,
           $ncs(\langle self \rangle)$
       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 $\langle 2 \rangle 2$ DEF ncs
    $\langle 3 \rangle$.QED
      BY $\langle 2 \rangle 1$, $Zenon$
  $\langle 2 \rangle 3.$ ASSUME NEW $self \in Procs$,
           $M(\langle self \rangle)$
       PROVE $SyncInv'$
    $\langle 3 \rangle 1.$ $\land pc[\langle self \rangle] = \text{"M"}$
       $\land \forall j \in OtherProcs(self) : pc[\langle self, j \rangle] = \text{"test"}$
       $\land pc' = [pc$ EXCEPT $![\langle self \rangle] = \text{"L"}]$
      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 $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: 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 $\mathit{self} \in \mathit{Procs}$,
$L(\langle \mathit{self} \rangle)$
PROVE $\mathit{SyncInv}'$
$\langle 3 \rangle. \land \forall j \in \mathit{OtherProcs}(\mathit{self}) : pc[\langle \mathit{self}, j \rangle] = \text{“ch”}$
$\land\ \mathit{SyncInv}!(\mathit{self})'$
$\land \forall i \in \mathit{Procs} \setminus \{\mathit{self}\}$:
$\land$ UNCHANGED $pc[\langle i \rangle]$
$\land \forall j \in \mathit{OtherProcs}(i)$: UNCHANGED $pc[\langle i, j \rangle]$
BY $\langle 2 \rangle 5$ DEF L, *SubProcsOf*, *SubProcs*, *OtherProcs*
$\langle 3 \rangle$.QED
BY $\langle 2 \rangle 1$, *Zenon*
$\langle 2 \rangle 6$. ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$cs(\langle \mathit{self} \rangle)$
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 $\langle 2 \rangle 6$ 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 $\mathit{oth} \in \mathit{Procs}$,
$ch(\langle \mathit{self}, \mathit{oth} \rangle)$
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 $self \in Procs$, NEW $oth \in Procs$,
$test(\langle self, oth\rangle)$
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 $\langle 2\rangle 9$ DEF *test*
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 10.$ ASSUME NEW $self \in Procs$, NEW $oth \in Procs$,
$Lb(\langle self, oth\rangle)$
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 $\langle 2\rangle 10$ DEF *Lb*
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 11.$ ASSUME NEW $self \in Procs$, NEW $oth \in Procs$,
$L2(\langle self, oth\rangle)$
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 $\langle 2\rangle 11$ DEF *L2*
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 12.$ ASSUME NEW $self \in Procs$, NEW $oth \in Procs$,
$L3(\langle self, oth\rangle)$
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 $\langle 2\rangle 12$ DEF *L3*
$\langle 3\rangle.$QED
BY $\langle 2\rangle 1$, *Zenon*
$\langle 2\rangle 13.$ ASSUME NEW $self \in Procs$, NEW $oth \in Procs$,
$wrp(\langle self, oth, \text{“wr”}\rangle)$
PROVE $SyncInv'$
$\langle 3\rangle.$UNCHANGED pc

BY ⟨2⟩13 DEF *wrp*, *wr*
⟨3⟩.QED
BY *Zenon*
⟨2⟩14.CASE UNCHANGED *vars*
BY ⟨2⟩14, *Zenon* DEF *vars*
⟨2⟩.HIDE DEFS *FullTypeOK*, *SyncInv*
⟨2⟩15. QED
BY ⟨2⟩2, ⟨2⟩11, ⟨2⟩12, ⟨2⟩13, ⟨2⟩14, ⟨2⟩3, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9, ⟨2⟩10
DEF *Next*, *main*, *sub*, *ProcIds*, *SubProcs*, *WrProcs*
⟨1⟩.QED BY ⟨1⟩1, ⟨1⟩2, *Typing*, *PTL* DEF *Spec*

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

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

THEOREM $NumberInvariant \triangleq Spec \Rightarrow \Box NumInv$
⟨1⟩1. $Init \Rightarrow NumInv$
⟨2⟩1. ASSUME *Init*, NEW $i \in Procs$
PROVE $number[i] = 0 \land pc[\langle i \rangle] \notin \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
BY ⟨2⟩1, *Zenon* DEF *Init*, *ProcSet*, *ProcIds*
⟨2⟩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 ⟨2⟩2, *SubProcId*, *Isa* DEF *Init*, *OtherProcs*, *ProcSet*
⟨2⟩.QED BY ⟨2⟩1, ⟨2⟩2, *Zenon* DEF *NumInv*
⟨1⟩2. $FullTypeOK \land NumInv \land [Next]_{vars} \Rightarrow NumInv'$
⟨2⟩ SUFFICES ASSUME *FullTypeOK*,
NumInv,
$[Next]_{vars}$
PROVE $NumInv'$
OBVIOUS
⟨2⟩.USE DEF *FullTypeOK*
⟨2⟩1. ASSUME NEW $self \in Procs$,
$ncs(\langle self \rangle)$
PROVE $NumInv'$
⟨3⟩. $\land pc[\langle self \rangle] = \text{"ncs"}$
$\land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"M"}]$
$\land$ 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 $\land\ localNum[j][i]' = qm$

$\land\ \lor\ pc[\langle i\rangle]' = \text{"L"} \land pc[\langle i, j\rangle]' = \text{"test"}$

$\lor\ pc[\langle i\rangle]' \in \{\text{"ncs"}, \text{"M"}\}$

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 $NumInv'$

$\langle 3\rangle$.PICK $v \in Nat \setminus \{0\}$:

$\land\ pc[\langle self\rangle] = \text{"M"}$

$\land\ \forall\, p \in Procs \setminus \{self\} : pc[\langle self, p\rangle] = \text{"test"}$

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

$\land\ localNum' = [j \in Procs \mapsto$

$[i \in OtherProcs(j) \mapsto$

IF $i = self$ THEN qm

ELSE $localNum[j][i]]]$

$\land\ pc' = [pc$ EXCEPT $![\langle self\rangle] = \text{"L"}]$

$\land$ UNCHANGED $localCh$

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

$\langle 3\rangle 1.\ \forall\, i \in Procs : \forall\, j \in OtherProcs(i) :$ 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 $NumInv$, $ProcIds$

$\langle 3\rangle 3.$ 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 $\land\ localNum[j][i]' = qm$

$\land\ \lor\ pc[\langle i\rangle]' = \text{"L"} \land pc[\langle i, j\rangle]' = \text{"test"}$

$\lor\ pc[\langle i\rangle]' \in \{\text{"ncs"}, \text{"M"}\}$

BY $\langle 3\rangle 4$ DEF $NumInv$, $OtherProcs$

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

$\langle 2\rangle 4.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$,
$L(\langle \mathit{self} \rangle)$
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 $j \in \mathit{OtherProcs}(i)$,
$\mathit{localNum}[j][i]' \neq \mathit{number}[i]'$
PROVE $\land\ \mathit{localNum}[j][i]' = \mathit{qm}$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}\}$
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 $\mathit{self} \in \mathit{Procs}$,
$cs(\langle \mathit{self} \rangle)$
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 $j \in \mathit{OtherProcs}(i)$,
$\mathit{localNum}[j][i]' \neq \mathit{number}[i]'$
PROVE $\land\ \mathit{localNum}[j][i]' = \mathit{qm}$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}\}$
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 $self \in Procs$,
$P(\langle self \rangle)$
PROVE $NumInv'$
$\langle 3 \rangle. \land pc[\langle self \rangle] = \text{"P"}$
$\land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"ncs"}]$
$\land number' = [number \text{ EXCEPT } ![self] = 0]$
$\land localNum' = [j \in Procs \mapsto$
$[i \in OtherProcs(j) \mapsto$
$\text{IF } i = self \text{ THEN } qm \text{ ELSE } localNum[j][i]]]$
$\land \text{UNCHANGED } localCh$
BY $\langle 2 \rangle 6$ DEF P
$\langle 3 \rangle 1. \forall i \in Procs : \forall j \in OtherProcs(i) : \text{UNCHANGED } pc[\langle i, j \rangle]$
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 $NumInv$, $ProcIds$
$\langle 3 \rangle 3.$ 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 $\land localNum[j][i]' = qm$
$\land \lor pc[\langle i \rangle]' = \text{"L"} \land pc[\langle i, j \rangle]' = \text{"test"}$
$\lor pc[\langle i \rangle]' \in \{\text{"ncs"}, \text{"M"}\}$
BY $\langle 3 \rangle 4$ DEF $NumInv$, $ProcIds$, $OtherProcs$
$\langle 3 \rangle.$QED BY ONLY $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $Zenon$ DEF $NumInv$
$\langle 2 \rangle 7.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$ch(\langle self, oth \rangle)$
PROVE $NumInv'$
$\langle 3 \rangle. \land pc[\langle self, oth \rangle] = \text{"ch"}$
$\land pc[\langle self \rangle] = \text{"M"}$
$\land pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{"test"}]$
$\land localCh' = [localCh \text{ EXCEPT } ![oth][self] = 1]$
$\land \text{UNCHANGED } \langle number, localNum \rangle$
BY $\langle 2 \rangle 7$ DEF ch
$\langle 3 \rangle 1.$ 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 $NumInv$, $OtherProcs$, $SubProcs$, POP, $PFunc$
$\langle 4 \rangle 2.$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 $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}\}$

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 $NumInv'$

$\langle 3 \rangle$. $\land\ pc[\langle self, oth \rangle] = \text{“test”}$
$\land\ pc[\langle self \rangle] = \text{“L”}$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{“Lb”}]$
$\land\ localNum' = [localNum \text{ EXCEPT } ![oth][self] = number[self]]$
$\land$ 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 $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i \rangle]' = \text{“L”} \land pc[\langle i, j \rangle]' = \text{“test”}$
$\lor\ pc[\langle i \rangle]' \in \{\text{“ncs”}, \text{“M”}\}$

$\langle 4 \rangle 1$.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 $NumInv'$

$\langle 3 \rangle$. $\land\ pc[\langle self, oth \rangle] = \text{“Lb”}$

$\land\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] = \text{"L2"}]$
$\land\ localCh' = [localCh$ EXCEPT $![oth][self] = 0]$
$\land$ UNCHANGED $\langle number, localNum\rangle$
BY $\langle 2\rangle 9$ DEF Lb
$\langle 3\rangle 1.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i\rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
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 $NumInv$, $OtherProcs$, $SubProcs$, POP, $PFunc$
$\langle 4\rangle 2.$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 $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i\rangle]' = \text{"L"} \land pc[\langle i, j\rangle]' = \text{"test"}$
$\lor\ pc[\langle i\rangle]' \in \{\text{"ncs"}, \text{"M"}\}$
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 $NumInv'$
$\langle 3\rangle.\ \land\ pc[\langle self, oth\rangle] = \text{"L2"}$
$\land\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] = \text{"L3"}]$
$\land$ UNCHANGED $\langle number, localNum, localCh\rangle$
BY $\langle 2\rangle 10$ DEF $L2$
$\langle 3\rangle 1.$ ASSUME NEW $i \in Procs$
PROVE $number[i]' \neq 0 \equiv pc[\langle i\rangle]' \in \{\text{"L"}, \text{"cs"}, \text{"P"}\}$
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 $\langle 3\rangle 2$, $\langle 4\rangle 1$, $pc'[\langle self, oth\rangle] = \text{"L3"}$, $Zenon$
DEF $NumInv$, $OtherProcs$, $SubProcs$
$\langle 4\rangle 2.$CASE $\neg(i = self \land j = oth)$
$\langle 5\rangle 1.$ 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  ∧ localNum[j][i]' = qm
               ∧ ∨ pc[⟨i⟩]' = "L" ∧ pc[⟨i, j⟩]' = "test"
                 ∨ pc[⟨i⟩]' ∈ {"ncs", "M"}
    BY ⟨3⟩3 DEF NumInv
  ⟨3⟩.QED BY ONLY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, Zenon DEF NumInv
⟨2⟩11. ASSUME NEW self ∈ Procs, NEW oth ∈ OtherProcs(self),
              L3(⟨self, oth⟩)
       PROVE  NumInv'
  ⟨3⟩. ∧ pc[⟨self, oth⟩] = "L3"
       ∧ pc' = [pc EXCEPT ![⟨self, oth⟩] = "ch"]
       ∧ UNCHANGED ⟨number, localNum, localCh⟩
    BY ⟨2⟩11 DEF L3
  ⟨3⟩1. ASSUME NEW i ∈ Procs
        PROVE  number[i]' ≠ 0 ≡ pc[⟨i⟩]' ∈ {"L", "cs", "P"}
    BY DEF NumInv
  ⟨3⟩2. ASSUME NEW i ∈ Procs, NEW j ∈ OtherProcs(i)
        PROVE  localCh[j][i]' = 1 ≡ pc[⟨i, j⟩]' ∈ {"test", "Lb"}
    ⟨4⟩1.CASE i = self ∧ j = oth
      BY ⟨3⟩2, ⟨4⟩1, pc'[⟨self, oth⟩] = "ch", Zenon
          DEF NumInv, OtherProcs, SubProcs
    ⟨4⟩2.CASE ¬(i = self ∧ j = oth)
      ⟨5⟩1. UNCHANGED pc[⟨i, j⟩]
        BY ⟨3⟩2, ⟨4⟩2
      ⟨5⟩.QED BY ONLY NumInv, UNCHANGED localCh, ⟨5⟩1, Zenon DEF NumInv
    ⟨4⟩.QED BY ⟨4⟩1, ⟨4⟩2
  ⟨3⟩3. ASSUME NEW i ∈ Procs, NEW j ∈ OtherProcs(i),
               localNum[j][i]' ≠ number[i]'
        PROVE  ∧ localNum[j][i]' = qm
               ∧ ∨ pc[⟨i⟩]' = "L" ∧ pc[⟨i, j⟩]' = "test"
                 ∨ pc[⟨i⟩]' ∈ {"ncs", "M"}
    BY ⟨3⟩3 DEF NumInv
  ⟨3⟩.QED BY ONLY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, Zenon DEF NumInv
⟨2⟩12. ASSUME NEW self ∈ Procs, NEW oth ∈ OtherProcs(self),
              wrp(⟨self, oth, "wr"⟩)
       PROVE  NumInv'
  ⟨3⟩. ∧ pc[⟨self⟩] ∈ {"ncs", "M"}
       ∧ localNum' = [localNum EXCEPT ![oth][self] = 0]
       ∧ UNCHANGED ⟨pc, number, localCh⟩
    BY ⟨2⟩12 DEF wrp, wr
  ⟨3⟩1. ASSUME NEW i ∈ Procs
        PROVE  number[i]' ≠ 0 ≡ pc[⟨i⟩]' ∈ {"L", "cs", "P"}
    BY DEF NumInv
  ⟨3⟩2. ASSUME NEW i ∈ Procs, NEW j ∈ OtherProcs(i)
        PROVE  localCh[j][i]' = 1 ≡ pc[⟨i, j⟩]' ∈ {"test", "Lb"}
    BY ONLY NumInv, UNCHANGED ⟨pc, localCh⟩, Zenon DEF NumInv
```

$\langle 3\rangle 3.$ ASSUME NEW $i \in Procs$, NEW $j \in OtherProcs(i)$,
$localNum[j][i]' \neq number[i]'$
PROVE $\land\ localNum[j][i]' = qm$
$\land\ \lor\ pc[\langle i\rangle]' = \text{“L”} \land pc[\langle i, j\rangle]' = \text{“test”}$
$\lor\ pc[\langle i\rangle]' \in \{\text{“ncs”}, \text{“M”}\}$
BY $\langle 3\rangle 3$, POP_except DEF $NumInv$, $OtherProcs$
$\langle 3\rangle$.QED BY ONLY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $Zenon$ DEF $NumInv$
$\langle 2\rangle 13.$CASE UNCHANGED $vars$
BY $\langle 2\rangle 13$, Isa DEF $vars$, $NumInv$
$\langle 2\rangle 14.$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 2\rangle 9$, $\langle 2\rangle 10$, $\langle 2\rangle 11$, $\langle 2\rangle 12$, $\langle 2\rangle 13$
DEF $Next$, $main$, sub, $ProcIds$, $SubProcs$, $WrProcs$, $OtherProcs$
$\langle 1\rangle$.QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, $Typing$, 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 $Invariance \triangleq Spec \Rightarrow \Box I$
$\langle 1\rangle 1.$ $Init \Rightarrow I$
BY $Zenon$
DEF $Init$, I, $OtherProcs$, Inv, $inBakery$, $passed$,
$ProcSet$, $ProcIds$, $SubProcs$, $WrProcs$
$\langle 1\rangle 2.$ $FullTypeOK \land SyncInv \land NumInv \land I \land [Next]_{vars} \Rightarrow I'$
$\langle 2\rangle$ SUFFICES ASSUME $FullTypeOK$, $SyncInv$, $NumInv$,
I,
$[Next]_{vars}$
PROVE I'
OBVIOUS
$\langle 2\rangle$.USE DEF $FullTypeOK$
$\langle 2\rangle 1.$ ASSUME NEW $self \in Procs$,
$ncs(\langle self\rangle)$
PROVE I'

$\langle 3 \rangle. \land pc[\langle self \rangle] = \text{"ncs"}$
$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"M"}]$
$\quad \land \text{UNCHANGED } number$
$\text{BY } \langle 2 \rangle 1 \ \text{ DEF } ncs$
$\langle 3 \rangle 1. \ \forall i, j \in Procs : inBakery(i, j)' \equiv inBakery(i, j)$
$\text{BY DEF } inBakery$
$\langle 3 \rangle 2. \ \forall i, j \in Procs : \forall w \in Nat : inDoorwayVal(i, j, w)' \equiv inDoorwayVal(i, j, w)$
$\text{BY DEF } inDoorwayVal$
$\langle 3 \rangle 3. \ \forall i, j \in Procs : inDoorway(i, j)' \equiv inDoorway(i, j)$
$\text{BY DEF } inDoorway$
$\langle 3 \rangle 4. \ \forall i, j \in Procs :$
$\quad \land passed(i, j, \text{"L2"})' \equiv passed(i, j, \text{"L2"})$
$\quad \land passed(i, j, \text{"L3"})' \equiv passed(i, j, \text{"L3"})$
$\text{BY DEF } passed$
$\langle 3 \rangle 5. \ \forall i, j \in Procs : Before(i, j)' \equiv Before(i, j)$
$\text{BY } \langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4 \ \text{ DEF } Before, Outside$
$\langle 3 \rangle.\text{QED}$
$\text{BY } \langle 3 \rangle 1, \langle 3 \rangle 3, \langle 3 \rangle 4, \langle 3 \rangle 5 \ \text{ DEF } I, Inv, OtherProcs$
$\langle 2 \rangle 2. \ \text{ASSUME NEW } self \in Procs,$
$\qquad M(\langle self \rangle)$
$\quad \text{PROVE } \ I'$
$\langle 3 \rangle.\text{PICK } v \in Nat \setminus \{0\} :$
$\quad \land pc[\langle self \rangle] = \text{"M"}$
$\quad \land \forall oth \in OtherProcs(self) : pc[\langle self, oth \rangle] = \text{"test"}$
$\quad \land \forall oth \in OtherProcs(self) :$
$\qquad \lor localNum[self][oth] = qm$
$\qquad \lor v \quad > localNum[self][oth]$
$\quad \land number' = [number \text{ EXCEPT } ![self] = v]$
$\quad \land localNum' = [j \in Procs \mapsto$
$\qquad [i \in OtherProcs(j) \mapsto$
$\qquad\quad \text{IF } i = self \text{ THEN } qm$
$\qquad\qquad \text{ELSE } localNum[j][i]]]$
$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"L"}]$
$\text{BY } \langle 2 \rangle 2, SubProcsOfEquality, Isa \text{ DEF } M, OtherProcs$
$\langle 3 \rangle 1. \ \text{ASSUME NEW } p \in Procs, \text{NEW } q \in OtherProcs(p)$
$\quad \text{PROVE } \ inBakery(p, q)' \equiv inBakery(p, q)$
$\text{BY DEF } inBakery$
$\langle 3 \rangle 2. \ \text{ASSUME NEW } p \in Procs, \text{NEW } q \in OtherProcs(p)$
$\quad \text{PROVE } \ inDoorway(p, q)' \equiv inDoorway(p, q) \lor p = self$
$\text{BY DEF } inDoorway, ProcIds$
$\langle 3 \rangle 3. \ \text{ASSUME NEW } p \in Procs, \text{NEW } q \in OtherProcs(p), \text{NEW } w \in Nat$
$\quad \text{PROVE } \ inDoorwayVal(p, q, w) \Rightarrow inDoorwayVal(p, q, w)'$
Here we only have an implication.
$\text{BY DEF } inDoorwayVal$
$\langle 3 \rangle 4. \ \text{ASSUME NEW } p \in OtherProcs(self), inBakery(p, self)$

PROVE $inDoorwayVal(self, p, number[p])'$

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

$\quad \land localNum[self][p] \neq qm$

BY $\langle 3 \rangle 4$, $inBakeryNum$, $qmNotNat$, $Zenon$ DEF $OtherProcs$

$\langle 4 \rangle$.QED

BY DEF $inDoorwayVal$, $ProcIds$, $OtherProcs$

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

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

$\quad \land passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$

BY DEF $passed$

$\langle 3 \rangle 6.$ $\forall p \in OtherProcs(self) : \neg inBakery(self, p)$

BY DEF $inBakery$, $SyncInv$

$\langle 3 \rangle 7.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$

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

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF $Before$, $Outside$, $OtherProcs$

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

$\langle 2 \rangle 4.$ ASSUME NEW $self \in Procs$,

$\quad L(\langle self \rangle)$

PROVE I'

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

$\quad \land \forall p \in Procs \setminus \{self\} : pc[\langle self, p \rangle] = \text{"ch"}$

$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"cs"}]$

$\quad \land$ UNCHANGED $number$

BY $\langle 2 \rangle 4$ DEF L, $SubProcsOf$, $SubProcs$

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

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

BY DEF $inBakery$

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

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

BY DEF $inDoorway$, $SubProcsOf$, $SubProcs$, $OtherProcs$

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

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

BY DEF $inDoorwayVal$, $OtherProcs$

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

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

$\quad \land passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$

BY DEF $passed$, $OtherProcs$, $ProcIds$

$\langle 3 \rangle$.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 $self \in Procs$,

$\quad cs(\langle self \rangle)$

PROVE I'

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

$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{"P"}]$

$\quad \land$ UNCHANGED $number$

BY $\langle 2 \rangle 5$ DEF cs

⟨3⟩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 $inBakery$, $SyncInv$, $ProcIds$, $SubProcs$, $OtherProcs$

⟨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 $p \in Procs \setminus \{self\}$, 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 $passed$

⟨3⟩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 $passed$, $SyncInv$, $ProcIds$

⟨3⟩6. ASSUME NEW $p \in Procs \setminus \{self\}$, NEW $q \in OtherProcs(p) \setminus \{self\}$
PROVE $Before(p, q) \Rightarrow Before(p, q)'$
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4 DEF $Before$, $Outside$, $OtherProcs$

⟨3⟩7. $\forall q \in OtherProcs(self) : inBakery(q, self)' \Rightarrow Before(q, self)'$
BY ⟨3⟩1 DEF $Before$, $Outside$, $inDoorway$ have $Outside(self, q)'$

⟨3⟩.QED
BY $passedInBakery$, ⟨3⟩1, ⟨3⟩2, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7 DEF $OtherProcs$, I, Inv

⟨2⟩6. ASSUME NEW $self \in Procs$,
$P(\langle self \rangle)$
PROVE I'

⟨3⟩. $\land\ pc[\langle self \rangle] = \text{“P”}$
$\land\ number' = [number \text{ EXCEPT } ![self] = 0]$
$\land\ pc' = [pc \text{ EXCEPT } ![\langle self \rangle] = \text{“ncs”}]$
BY ⟨2⟩6 DEF P

⟨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⟩5. $\forall q \in OtherProcs(self) : \neg inBakery(self, q)$

BY DEF $inBakery$, $SyncInv$

$\langle 3\rangle 9.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $Before(p, q) \Rightarrow Before(p, q)'$

$\langle 4\rangle 1.$CASE $q = self$ follows from $Outside(self, p)'$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 5$, $\langle 3\rangle 9$, $\langle 4\rangle 1$ DEF $Before$, $inDoorway$, $Outside$, $OtherProcs$

$\langle 4\rangle 2.$CASE $q \neq self$
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 9$, $\langle 4\rangle 2$ DEF $Before$, $OtherProcs$, $Outside$

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

$\langle 3\rangle.$QED BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 4$, $\langle 3\rangle 9$ DEF I, Inv, $OtherProcs$

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

$\langle 3\rangle.$ $\land\ pc[\langle self, oth\rangle] =$ "ch"
$\land\ pc[\langle self\rangle] =$ "M"
$\land\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] =$ "test"$]$
$\land$ UNCHANGED $number$
BY $\langle 2\rangle 7$ DEF ch

$\langle 3\rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$

$\langle 3\rangle 2.$ 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 $\land\ passed(p, q,$ "L2"$)' \equiv passed(p, q,$ "L2"$)$
$\land\ passed(p, q,$ "L3"$)' \equiv passed(p, q,$ "L3"$)$
BY DEF $passed$

$\langle 3\rangle.$QED BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEF I, Inv, $Before$, $OtherProcs$, $Outside$

$\langle 2\rangle 8.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$test(\langle self, oth\rangle)$
PROVE I'

$\langle 3\rangle.$ $\land\ pc[\langle self, oth\rangle] =$ "test"
$\land\ pc[\langle self\rangle] =$ "L"
$\land\ pc' = [pc$ EXCEPT $![\langle self, oth\rangle] =$ "Lb"$]$
$\land$ UNCHANGED $number$
BY $\langle 2\rangle 8$ DEF $test$

$\langle 3\rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q) \lor (p = self \land q = oth)$
BY DEF $inBakery$, $ProcIds$, $SubProcs$, $OtherProcs$

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

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

PROVE $\mathit{inDoorwayVal}(p, q, w)' \equiv \mathit{inDoorwayVal}(p, q, w) \land \neg(p = \mathit{self} \land q = \mathit{oth})$

BY DEF $\mathit{inDoorwayVal}$, $\mathit{ProcIds}$, $\mathit{SubProcs}$, $\mathit{OtherProcs}$

$\langle 3\rangle 4.$ ASSUME NEW $p \in \mathit{Procs}$, NEW $q \in \mathit{OtherProcs}(p)$

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

$\land\ \mathit{passed}(p, q, \text{"L3"})' \equiv \mathit{passed}(p, q, \text{"L3"})$

BY DEF passed

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

PROVE $\mathit{Before}(p, q)'$

$\langle 4\rangle 1.$CASE $p = \mathit{oth} \land q = \mathit{self}$

$\langle 5\rangle 1.$ $\mathit{inBakery}(\mathit{oth}, \mathit{self})' \land \mathit{inBakery}(\mathit{self}, \mathit{oth})'$

BY $\langle 3\rangle 5$, $\langle 3\rangle 1$, $\langle 4\rangle 1$ DEF Before, $\mathit{OtherProcs}$

$\langle 5\rangle 2.$ $\mathit{inDoorway}(\mathit{self}, \mathit{oth}) \land \neg \mathit{inBakery}(\mathit{self}, \mathit{oth})$

BY DEF $\mathit{inDoorway}$, $\mathit{inBakery}$

$\langle 5\rangle 3.$ $\mathit{inDoorwayVal}(\mathit{self}, \mathit{oth}, \mathit{number}[\mathit{oth}])$

BY $\langle 3\rangle 5$, $\langle 4\rangle 1$, $\langle 5\rangle 2$ DEF Before, $\mathit{Outside}$

$\langle 5\rangle 4.$ $\langle \mathit{number}[\mathit{oth}], \mathit{oth}\rangle \ll \langle \mathit{number}[\mathit{self}], \mathit{self}\rangle$

BY $\langle 5\rangle 3$ DEF $\mathit{inDoorwayVal}$, $\ll$, $\mathit{OtherProcs}$

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

$\langle 4\rangle 2.$CASE $p \neq \mathit{oth} \lor q \neq \mathit{self}$

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, $\mathit{Outside}$, $\mathit{OtherProcs}$

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

$\langle 3\rangle 6.$ ASSUME $\mathit{inBakery}(\mathit{oth}, \mathit{self})$

PROVE $\mathit{Before}(\mathit{self}, \mathit{oth})' \lor \mathit{Before}(\mathit{oth}, \mathit{self})'$

$\langle 4\rangle 1.$ $\mathit{inBakery}(\mathit{self}, \mathit{oth})' \land \mathit{inBakery}(\mathit{oth}, \mathit{self})'$

BY $\langle 3\rangle 6$, $\langle 3\rangle 1$ DEF $\mathit{OtherProcs}$

$\langle 4\rangle 2.$ $\neg \mathit{passed}(\mathit{self}, \mathit{oth}, \text{"L3"})'$

BY DEF passed

$\langle 4\rangle 3.$CASE $\mathit{passed}(\mathit{oth}, \mathit{self}, \text{"L3"})$ $\mathit{Before}(\mathit{oth}, \mathit{self})$, hence $\mathit{Before}(\mathit{oth}, \mathit{self})'$

BY $\langle 4\rangle 3$, $\langle 3\rangle 5$ DEF I, Inv, $\mathit{OtherProcs}$

$\langle 4\rangle 4.$CASE $\neg \mathit{passed}(\mathit{oth}, \mathit{self}, \text{"L3"})$ $\mathit{Before}(\mathit{self}, \mathit{oth})' \lor \mathit{Before}(\mathit{oth}, \mathit{self})'$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 4$, $\langle 3\rangle 4$, $\mathit{TotalOrder}$ DEF Before, $\mathit{OtherProcs}$

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

$\langle 3\rangle 7.$ $\mathit{Before}(\mathit{self}, \mathit{oth})' \lor \mathit{Before}(\mathit{oth}, \mathit{self})' \lor \mathit{inDoorway}(\mathit{oth}, \mathit{self})'$

$\langle 4\rangle 1.$CASE $\mathit{Outside}(\mathit{oth}, \mathit{self})$ $\mathit{inBakery}(\mathit{self}, \mathit{oth})' \land \mathit{Outside}(\mathit{oth}, \mathit{self})'$

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

$\langle 4\rangle 2.$CASE $\mathit{inDoorway}(\mathit{oth}, \mathit{self})$ $\mathit{inDoorway}(\mathit{oth}, \mathit{self})'$

BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $\mathit{OtherProcs}$

$\langle 4\rangle 3.$CASE $\mathit{inBakery}(\mathit{oth}, \mathit{self})$

BY $\langle 4\rangle 3$, $\langle 3\rangle 6$

$\langle 4\rangle$.QED BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $\mathit{Outside}$

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

$\langle 2\rangle 9.$ ASSUME NEW $\mathit{self} \in \mathit{Procs}$, NEW $\mathit{oth} \in \mathit{OtherProcs}(\mathit{self})$,

$\mathit{Lb}(\langle \mathit{self}, \mathit{oth}\rangle)$

PROVE I'

$\langle 3 \rangle. \land pc[\langle self, oth \rangle] = \text{"Lb"}$
$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{"L2"}]$
$\quad \land \text{UNCHANGED } number$
BY $\langle 2 \rangle 9$ DEF Lb
$\langle 3 \rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$
$\langle 3 \rangle 2.$ 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 $\land passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"})$
$\quad \land passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$
BY DEF $passed$
$\langle 3 \rangle.$QED BY $\langle 3 \rangle 1, \langle 3 \rangle 2, \langle 3 \rangle 3, \langle 3 \rangle 4$ DEF I, Inv, $Before$, $Outside$, $OtherProcs$
$\langle 2 \rangle 10.$ ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$L2(\langle self, oth \rangle)$
PROVE I'
$\langle 3 \rangle. \land pc[\langle self, oth \rangle] = \text{"L2"}$
$\quad \land localCh[self][oth] = 0$
$\quad \land pc' = [pc \text{ EXCEPT } ![\langle self, oth \rangle] = \text{"L3"}]$
$\quad \land \text{UNCHANGED } number$
BY $\langle 2 \rangle 10$ DEF $L2$
$\langle 3 \rangle 1.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inBakery(p, q)' \equiv inBakery(p, q)$
BY DEF $inBakery$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in Procs$, NEW $q \in OtherProcs(p)$
PROVE $inDoorway(p, q)' \equiv inDoorway(p, q)$
BY DEF $inDoorway$
$\langle 3 \rangle 3.$ $\neg inDoorway(oth, self)$
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 $\land passed(p, q, \text{"L2"})' \equiv passed(p, q, \text{"L2"}) \lor (p = self \land q = oth)$
$\quad \land passed(p, q, \text{"L3"})' \equiv passed(p, q, \text{"L3"})$
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 *number*

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

BY DEF *passed*, *SyncInv*, *ProcIds*, *SubProcs*, *OtherProcs*

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

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 $q \in OtherProcs(p)$, $q \neq self \vee p \neq oth$
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 $\langle pc, number \rangle$
BY $\langle 2 \rangle$X, *Isa*
DEF *I*, *Inv*, *Before*, *Outside*, *inBakery*, *inDoorway*, *inDoorwayVal*, *passed*, *OtherProcs*
$\langle 2 \rangle 12$. ASSUME NEW $self \in Procs$, NEW $oth \in OtherProcs(self)$,
$wrp(\langle self, oth, \text{"wr"} \rangle)$
PROVE I'
BY $\langle 2 \rangle 12$, $\langle 2 \rangle$X DEF *wr*, *wrp*
$\langle 2 \rangle 13$.CASE UNCHANGED *vars*
BY $\langle 2 \rangle 13$, $\langle 2 \rangle$X DEF *vars*
$\langle 2 \rangle 14$. QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, $\langle 2 \rangle 8$, $\langle 2 \rangle 9$, $\langle 2 \rangle 10$, $\langle 2 \rangle 11$, $\langle 2 \rangle 12$, $\langle 2 \rangle 13$
DEF *Next*, *main*, *sub*, *ProcIds*, *SubProcs*, *WrProcs*, *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 $Spec \Rightarrow \Box MutualExclusion$
$\langle 1 \rangle 1$. $FullTypeOK \wedge SyncInv \wedge I \Rightarrow MutualExclusion$
$\langle 2 \rangle$.SUFFICES ASSUME *FullTypeOK*, *SyncInv*, *I*,
NEW $p \in Procs$, NEW $q \in Procs$, $q \neq p$,
$pc[\langle p \rangle] = \text{"cs"}$, $pc[\langle q \rangle] = \text{"cs"}$
PROVE FALSE
BY DEF *MutualExclusion*, *ProcIds*
$\langle 2 \rangle 1$. $passed(p, q, \text{"L3"}) \wedge passed(q, p, \text{"L3"})$
BY DEF *passed*, *SyncInv*, *OtherProcs*
$\langle 2 \rangle 2$. $Before(p, q) \wedge Before(q, p)$
BY $\langle 2 \rangle 1$ DEF *I*, *Inv*, *OtherProcs*
$\langle 2 \rangle 3$. $\neg Outside(p, q) \wedge \neg Outside(q, p)$
BY DEF *Outside*, *inBakery*, *SyncInv*, *OtherProcs*
$\langle 2 \rangle 4$. $\neg inDoorwayVal(p, q, number[q]) \wedge \neg inDoorwayVal(q, p, number[p])$
BY DEF *inDoorwayVal*
$\langle 2 \rangle 5$. $\wedge \langle number[p], p \rangle \ll \langle number[q], q \rangle$
$\wedge \langle number[q], q \rangle \ll \langle number[p], p \rangle$
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 *Tue Nov* 16 19:42:11 *CET* 2021 by *merz*

* Created *Thu Jul* 01 12:26:36 *CEST* 2021 by *merz*