MODULE *Bakery*

The bakery algorithm originally appeared in:

Leslie *Lamport* A New Solution of *Dijkstra*'s Concurrent Programming Problem Communications of the *ACM* 17, 8 (August 1974), 453-455

The code for the algorithm given in that paper is :

```
begin integer j;
L1: choosing [i] := 1 ;
    number[i] := 1 + maximum (number[1],..., number[N]);
    choosing[i] := 0;
    for j = 1 step l until N do
       begin
         L2: if choosing[j] /= 0 then goto L2;
         L3: if number[j] /= 0 and (number [j], j) < (number[i],i)
               then goto L3;
       end;
    critical section;
    number[i] := 0;
    noncritical section;
    goto L1 ;
end
```

This *PlusCal* version of the Atomic *Bakery* algorithm is one in which variables whose initial values are not used are initialized to particular type-correct values. If the variables were left uninitialized, the *PlusCal* translation would initialize them to a particular unspecified value. This would complicate the proof because it would make the type-correctness invariant more complicated, but it would be efficient to model check. We could write a version that is more elegant and easy to prove, but less efficient to model check, by initializing the variables to arbitrarily chosen type-correct values.

EXTENDS $\mathit{Naturals}, \mathit{TLAPS}$

We first declare N to be the number of processes, and we assume that N is a natural number.

CONSTANT N

ASSUME $N \in \mathit{Nat}$

We define Procs to be the set $\{1, 2, \ldots, N\}$ of processes.

$$\mathit{Procs} \triangleq 1 \,..\, N$$

$\prec$ is defined to be the lexicographical less-than relation on pairs of numbers.

$$\begin{aligned} a \prec b \triangleq\ & \lor a[1] < b[1] \\ & \lor (a[1] = b[1]) \land (a[2] < b[2]) \end{aligned}$$

```
 ∗∗     this is a comment containing the PlusCal code *

{algorithm Bakery
{variables num = [i ∈ Procs ↦ 0], flag = [i ∈ Procs ↦ FALSE];
 fair process(p ∈ Procs)
   variables unchecked = {}, max = 0, nxt = 1 ;
   {ncs : − while(TRUE)
        {e1 : either{flag[self] := ¬flag[self];
                     goto e1}
              or    {flag[self] := TRUE;
```

```
                unchecked := Procs \ {self};
                max := 0
              };
      e2 : while(unchecked $\neq$ {})
             {with(i $\in$ unchecked)
                {unchecked := unchecked \ {i};
                 if (num[i] > max){max := num[i]}
                }
             };
      e3 : either{with(k $\in$ Nat){num[self] := k};
                goto e3}
           or   {with(i $\in$ {j $\in$ Nat : j > max})
                  {num[self] := i}
              };
      e4 : either{flag[self] := $\neg$flag[self];
                goto e4}
           or   {flag[self] := FALSE;
                unchecked := Procs \ {self}
              };
      w1 : while(unchecked $\neq$ {})
             {    with(i $\in$ unchecked){nxt := i};
                  await $\neg$flag[nxt];
               w2 : await $\vee$ num[nxt] = 0
                          $\vee$ $\langle$num[self], self$\rangle$ $\prec$ $\langle$num[nxt], nxt$\rangle$;
                  unchecked := unchecked \ {nxt};
             };
      cs : skip ; \* the critical section;
      exit : either{with(k $\in$ Nat){num[self] := k};
                goto exit}
           or   {num[self] := 0}
    }
  }
}
```

this ends the comment containing the *PlusCal* code
****

BEGIN TRANSLATION (this begins the translation of the *PlusCal* code)

VARIABLES $num, flag, pc, unchecked, max, nxt$

$$vars \triangleq \langle num, flag, pc, unchecked, max, nxt \rangle$$

$$ProcSet \triangleq (Procs)$$

$Init \triangleq$ Global variables

$$\land\ num = [i \in Procs \mapsto 0]$$
$$\land\ flag = [i \in Procs \mapsto \text{FALSE}]$$

Process p

$$\land\ unchecked = [self \in Procs \mapsto \{\}]$$
$$\land\ max = [self \in Procs \mapsto 0]$$
$$\land\ nxt\ \ = [self \in Procs \mapsto 1]$$

```
              $\land\ pc = [self \in ProcSet \mapsto \text{"ncs"}]$

$ncs(self) \triangleq$ $\land\ pc[self] = \text{"ncs"}$
                   $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e1"}]$
                   $\land\ \text{UNCHANGED}\ \langle num, flag, unchecked, max, nxt \rangle$

$e1(self) \triangleq$ $\land\ pc[self] = \text{"e1"}$
                 $\land\ \lor\ \land\ flag^{\theta} = [flag\ \text{EXCEPT}\ ![self] = \neg flag[self]]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e1"}]$
                          $\land\ \text{UNCHANGED}\ \langle unchecked, max \rangle$
                      $\lor\ \land\ flag^{\theta} = [flag\ \text{EXCEPT}\ ![self] = \text{TRUE}]$
                          $\land\ unchecked^{\theta} = [unchecked\ \text{EXCEPT}\ ![self] = Procs \setminus \{self\}]$
                          $\land\ max^{\theta} = [max\ \text{EXCEPT}\ ![self] = 0]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e2"}]$
                 $\land\ \text{UNCHANGED}\ \langle num, nxt \rangle$

$e2(self) \triangleq$ $\land\ pc[self] = \text{"e2"}$
                 $\land\ \text{IF}\ unchecked[self] \neq \{\}$
                         $\text{THEN}\ \land\ \exists\, i \in unchecked[self] :$
                                       $\land\ unchecked^{\theta} = [unchecked\ \text{EXCEPT}\ ![self] = unchecked[self] \setminus \{i\}]$
                                       $\land\ \text{IF}\ num[i] > max[self]$
                                               $\text{THEN}\ \land\ max^{\theta} = [max\ \text{EXCEPT}\ ![self] = num[i]]$
                                               $\text{ELSE}\ \land\ \text{TRUE}$
                                                     $\land\ max^{\theta} = max$
                                   $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e2"}]$
                         $\text{ELSE}\ \land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e3"}]$
                                   $\land\ \text{UNCHANGED}\ \langle unchecked, max \rangle$
                 $\land\ \text{UNCHANGED}\ \langle num, flag, nxt \rangle$

$e3(self) \triangleq$ $\land\ pc[self] = \text{"e3"}$
                 $\land\ \lor\ \land\ \exists\, k \in Nat :$
                                 $num^{\theta} = [num\ \text{EXCEPT}\ ![self] = k]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e3"}]$
                      $\lor\ \land\ \exists\, i \in \{j \in Nat : j > max[self]\} :$
                                 $num^{\theta} = [num\ \text{EXCEPT}\ ![self] = i]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e4"}]$
                 $\land\ \text{UNCHANGED}\ \langle flag, unchecked, max, nxt \rangle$

$e4(self) \triangleq$ $\land\ pc[self] = \text{"e4"}$
                 $\land\ \lor\ \land\ flag^{\theta} = [flag\ \text{EXCEPT}\ ![self] = \neg flag[self]]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"e4"}]$
                          $\land\ \text{UNCHANGED}\ unchecked$
                      $\lor\ \land\ flag^{\theta} = [flag\ \text{EXCEPT}\ ![self] = \text{FALSE}]$
                          $\land\ unchecked^{\theta} = [unchecked\ \text{EXCEPT}\ ![self] = Procs \setminus \{self\}]$
                          $\land\ pc^{\theta} = [pc\ \text{EXCEPT}\ ![self] = \text{"w1"}]$
                 $\land\ \text{UNCHANGED}\ \langle num, max, nxt \rangle$
```

```
$w1(self) \triangleq$ $\land\ pc[self] = \text{“w1”}$
            $\land$ IF $unchecked[self] \neq \{\}$
                  THEN $\land\ \exists\, i \in unchecked[self] :$
                             $nxt' = [nxt$ EXCEPT $![self] = i]$
                       $\land\ \neg flag[nxt'[self]]$
                       $\land\ pc' = [pc$ EXCEPT $![self] = \text{“w2”}]$
                  ELSE $\land\ pc' = [pc$ EXCEPT $![self] = \text{“cs”}]$
                       $\land\ nxt' = nxt$
            $\land$ UNCHANGED $\langle num, flag, unchecked, max\rangle$

$w2(self) \triangleq$ $\land\ pc[self] = \text{“w2”}$
            $\land\ \lor\ num[nxt[self]] = 0$
              $\lor\ \langle num[self], self\rangle \prec \langle num[nxt[self]], nxt[self]\rangle$
            $\land\ unchecked' = [unchecked$ EXCEPT $![self] = unchecked[self] \setminus \{nxt[self]\}]$
            $\land\ pc' = [pc$ EXCEPT $![self] = \text{“w1”}]$
            $\land$ UNCHANGED $\langle num, flag, max, nxt\rangle$

$cs(self) \triangleq$ $\land\ pc[self] = \text{“cs”}$
            $\land$ TRUE
            $\land\ pc' = [pc$ EXCEPT $![self] = \text{“exit”}]$
            $\land$ UNCHANGED $\langle num, flag, unchecked, max, nxt\rangle$

$exit(self) \triangleq$ $\land\ pc[self] = \text{“exit”}$
              $\land\ \lor\ \land\ \exists\, k \in Nat :$
                            $num' = [num$ EXCEPT $![self] = k]$
                       $\land\ pc' = [pc$ EXCEPT $![self] = \text{“exit”}]$
                  $\lor\ \land\ num' = [num$ EXCEPT $![self] = 0]$
                       $\land\ pc' = [pc$ EXCEPT $![self] = \text{“ncs”}]$
              $\land$ UNCHANGED $\langle flag, unchecked, max, nxt\rangle$

$p(self) \triangleq ncs(self) \lor e1(self) \lor e2(self) \lor e3(self) \lor e4(self)$
               $\lor\ w1(self) \lor w2(self) \lor cs(self) \lor exit(self)$

$Next \triangleq (\exists\, self \in Procs : p(self))$

$Spec \triangleq$ $\land\ Init \land 2[Next]_{vars}$
         $\land\ \forall\, self \in Procs : \mathrm{WF}_{vars}((pc[self] \neq \text{“ncs”}) \land p(self))$
```

END TRANSLATION (this ends the translation of the *PlusCal* code)

MutualExclusion asserts that no two distinct processes are in their critical sections.

```
$MutualExclusion \triangleq \forall\, i, j \in Procs : (i \neq j) \Rightarrow \neg \land\ pc[i] = \text{“cs”}$
                                                     $\land\ pc[j] = \text{“cs”}$
```

The Inductive Invariant

TypeOK is the type-correctness invariant.

$$
\begin{array}{ll}
\mathit{TypeOK} \triangleq & \land\ \mathit{num} \in [\mathit{Procs} \rightarrow \mathit{Nat}] \\
& \land\ \mathit{flag} \in [\mathit{Procs} \rightarrow \text{BOOLEAN}\ ] \\
& \land\ \mathit{unchecked} \in [\mathit{Procs} \rightarrow \text{SUBSET}\ \mathit{Procs}] \\
& \land\ \mathit{max} \in [\mathit{Procs} \rightarrow \mathit{Nat}] \\
& \land\ \mathit{nxt}\ \ \in [\mathit{Procs} \rightarrow \mathit{Procs}] \\
& \land\ \mathit{pc} \in [\mathit{Procs} \rightarrow \{\text{``ncs''},\ \text{``e1''},\ \text{``e2''},\ \text{``e3''}, \\
& \qquad\qquad\qquad\quad \text{``e4''},\ \text{``w1''},\ \text{``w2''},\ \text{``cs''},\ \text{``exit''}\}]
\end{array}
$$

$\mathit{Before}(i, j)$ is a condition that implies that $\mathit{num}[i] > 0$ and, if j is trying to enter its critical section and i does not change $\mathit{num}[i]$, then j either has or will choose a value of $\mathit{num}[j]$ for which

$$\langle \mathit{num}[i],\ i\rangle \prec \langle \mathit{num}[j],\ j\rangle$$

is true.

$$
\begin{array}{ll}
\mathit{Before}(i,\ j) \triangleq & \land\ \mathit{num}[i] > 0 \\
& \land\ \lor\ \mathit{pc}[j] \in \{\text{``ncs''},\ \text{``e1''},\ \text{``exit''}\} \\
& \quad \lor\ \land\ \mathit{pc}[j] = \text{``e2''} \\
& \qquad\ \ \land\ \lor\ i \in \mathit{unchecked}[j] \\
& \qquad\qquad\ \lor\ \mathit{max}[j] \geq \mathit{num}[i] \\
& \quad \lor\ \land\ \mathit{pc}[j] = \text{``e3''} \\
& \qquad\ \ \land\ \mathit{max}[j] \geq \mathit{num}[i] \\
& \quad \lor\ \land\ \mathit{pc}[j] \in \{\text{``e4''},\ \text{``w1''},\ \text{``w2''}\} \\
& \qquad\ \ \land\ \langle \mathit{num}[i],\ i\rangle \prec \langle \mathit{num}[j],\ j\rangle \\
& \qquad\ \ \land\ (\mathit{pc}[j] \in \{\text{``w1''},\ \text{``w2''}\}) \Rightarrow (i \in \mathit{unchecked}[j])
\end{array}
$$

Inv is the complete inductive invariant.

$$
\begin{array}{ll}
\mathit{Inv} \triangleq & \land\ \mathit{TypeOK} \\
& \land\ \forall\, i \in \mathit{Procs} : \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{``ncs''},\ \text{``e1''},\ \text{``e2''}\}) \Rightarrow (\mathit{num}[i] = 0) \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{``e4''},\ \text{``w1''},\ \text{``w2''},\ \text{``cs''}\}) \Rightarrow (\mathit{num}[i] \neq 0) \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{``e2''},\ \text{``e3''}\}) \Rightarrow \mathit{flag}[i] \\
& \qquad \land\ (\mathit{pc}[i] = \text{``w2''}) \Rightarrow (\mathit{nxt}[i] \neq i) \\
& \qquad \land\ \mathit{pc}[i] \in \{\ \text{``e2''},\text{``w1''},\ \text{``w2''}\} \Rightarrow i \notin \mathit{unchecked}[i] \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{``w1''},\ \text{``w2''}\}) \Rightarrow \\
& \qquad\qquad\quad \forall\, j \in (\mathit{Procs} \setminus \mathit{unchecked}[i]) \setminus \{i\} : \mathit{Before}(i,\ j) \\
& \qquad \land\ \land\ (\mathit{pc}[i] = \text{``w2''}) \\
& \qquad\quad\ \ \land\ \lor\ (\mathit{pc}[\mathit{nxt}[i]] = \text{``e2''}) \land (i \notin \mathit{unchecked}[\mathit{nxt}[i]]) \\
& \qquad\qquad\quad\ \lor\ \mathit{pc}[\mathit{nxt}[i]] = \text{``e3''} \\
& \qquad\quad\ \ \Rightarrow \mathit{max}[\mathit{nxt}[i]] \geq \mathit{num}[i] \\
& \qquad \land\ (\mathit{pc}[i] = \text{``cs''}) \Rightarrow \forall\, j \in \mathit{Procs} \setminus \{i\} : \mathit{Before}(i,\ j)
\end{array}
$$

Proof of Mutual Exclusion

This is a standard invariance proof, where $<1>2$ asserts that any step of the algorithm (including a stuttering step) starting in a state in which Inv is true leaves Inv true. Step $<1>4$ follows easily from $<1>1$- $<1>3$ by simple temporal reasoning.

```
THEOREM $Spec \Rightarrow 2\,MutualExclusion$
$<1>$ $USEN \in NatDEFSProcs,\ TypeOK,\ Before,\ \prec,\ ProcSet$
$<1>$ $1.Init \Rightarrow Inv$
    $BYDEFInit,\ Inv$
$<1>$ $2.Inv \wedge [Next]_{vars} \Rightarrow Inv^{\theta}$
    $<2>$ $SUFFICES$ ASSUME $Inv,$
                               $[Next]_{vars}$
                   $PROVE\ Inv^{\theta}$
        $OBVIOUS$
    $<2>$ 1.ASSUME $NEWself \in Procs,$
                   $ncs(self)$
            $PROVE\ Inv^{\theta}$
        $BY <2> 1DEFncs,\ Inv$
    $<2>$ 2.ASSUME $NEWself \in Procs,$
                   $e1(self)$
            $PROVE\ Inv^{\theta}$
        $<3>$ . $\wedge\ pc[self] = $ “e1”
                $\wedge$ UNCHANGED $\langle num,\ nxt \rangle$
            $BY <2> 2DEFe1$
        $<3>$ 1.CASE $\wedge\ flag^{\theta} = [flag$ EXCEPT $![self] = \neg flag[self]]$
                     $\wedge\ pc^{\theta} = [pc$ EXCEPT $![self] = $ “e1”$]$
                     $\wedge$ UNCHANGED $\langle unchecked,\ max \rangle$
            $BY <3> 1DEFInv$
        $<3>$ 2.CASE $\wedge\ flag^{\theta} = [flag$ EXCEPT $![self] =$ TRUE$]$
                     $\wedge\ unchecked^{\theta} = [unchecked$ EXCEPT $![self] = Procs \setminus \{self\}]$
                     $\wedge\ max^{\theta} = [max$ EXCEPT $![self] = 0]$
                     $\wedge\ pc^{\theta} = [pc$ EXCEPT $![self] = $ “e2”$]$
            $BY <3> 2DEFInv$
        $<3>$ $.QED\ \ BY <3> 1,\ <3> 2,\ <2> 2DEFe1$
    $<2>$ 3.ASSUME $NEWself \in Procs,$
                   $e2(self)$
            $PROVE\ Inv^{\theta}$
        $<3>$ . $\wedge\ pc[self] = $ “e2”
                $\wedge$ UNCHANGED $\langle num,\ flag,\ nxt \rangle$
            $BY <2> 3DEFe2$
        $<3>$ 1.ASSUME $NEWi \in unchecked[self],$
                       $unchecked^{\theta} = [unchecked$ EXCEPT $![self] = unchecked[self] \setminus \{i\}],$
                       $num[i] > max[self],$
                       $max^{\theta} = [max$ EXCEPT $![self] = num[i]],$
                       $pc^{\theta} = [pc$ EXCEPT $![self] = $ “e2”$]$
                $PROVE\ Inv^{\theta}$
            $BY <3> 1,\ Z3T(10)DEFInv$
        $<3>$ 2.ASSUME $NEWi \in unchecked[self],$
                       $unchecked^{\theta} = [unchecked$ EXCEPT $![self] = unchecked[self] \setminus \{i\}],$
                       $\neg(num[i] > max[self]),$
```

```
                    $max^{\theta} = max,$
                    $pc^{\theta} = [pc \text{ EXCEPT } ![self] = \text{“e2”}]$
              $PROVE\ Inv^{\theta}$
            $< 4 > .TypeOK^{\theta}\ BY < 3 > 2DEFInv$
            $< 4 > 1.\forall\, ii \in Procs : (pc^{\theta}[ii] \in \{\text{“e4”}, \text{“w1”}, \text{“w2”}, \text{“cs”}\}) \Rightarrow (num^{\theta}[ii] \neq 0)$
                $BY < 3 > 2DEFInv$
            $< 4 > 2.\forall\, ii \in Procs : (pc^{\theta}[ii] \in \{\text{“e2”}, \text{“e3”}\}) \Rightarrow flag^{\theta}[ii]$
                $BY < 3 > 2DEFInv$
            $< 4 > 3.\forall\, ii \in Procs : (pc^{\theta}[ii] = \text{“w2”}) \Rightarrow (nxt^{\theta}[ii] \neq ii)$
                $BY < 3 > 2DEFInv$
            $< 4 > 4.\forall\, ii \in Procs : pc^{\theta}[ii] \in \{\ \text{“e2”,}\text{“w1”}, \text{“w2”}\} \Rightarrow ii \notin unchecked^{\theta}[ii]$
                $BY < 3 > 2DEFInv$
            $< 4 > 5.\forall\, ii \in Procs : (pc^{\theta}[ii] \in \{\text{“w1”}, \text{“w2”}\}) \Rightarrow$
                       $\forall\, j \in (Procs \setminus unchecked^{\theta}[ii]) \setminus \{ii\} : Before(ii, j)^{\theta}$
                $BY < 3 > 2DEFInv$
            $< 4 > 6.\forall\, ii \in Procs :$
                      $\wedge\ (pc^{\theta}[ii] = \text{“w2”})$
                      $\wedge\ \vee\ (pc^{\theta}[nxt^{\theta}[ii]] = \text{“e2”}) \wedge (ii \notin unchecked^{\theta}[nxt^{\theta}[ii]])$
                         $\vee\ pc^{\theta}[nxt^{\theta}[ii]] = \text{“e3”}$
                      $\Rightarrow max^{\theta}[nxt^{\theta}[ii]] \geq num^{\theta}[ii]$
                $BY < 3 > 2DEFInv$
            $< 4 > 7.\forall\, ii \in Procs : (pc^{\theta}[ii] = \text{“cs”}) \Rightarrow \forall\, j \in Procs \setminus \{ii\} : Before(ii, j)^{\theta}$
                $BY < 3 > 2DEFInv$
            $< 4 > .QED\ \ BY\ \ < 4 > 0, < 4 > 1,\ < 4 > 2,\ < 4 > 3,\ < 4 > 4,\ < 4 > 5,\ < 4 > 6,\ < 4 > 7.$
      $< 3 > 3.\text{CASE}\ \ \wedge\ unchecked[self] = \{\}$
                      $\wedge\ pc^{\theta} = [pc \text{ EXCEPT } ![self] = \text{“e3”}]$
                      $\wedge\ \text{UNCHANGED}\ \langle unchecked, max\rangle$
           $BY < 3 > 3DEFInv$
      $< 3 > .QED\ \ BY < 3 > 1,\ < 3 > 2,\ < 3 > 3,\ < 2 > 3DEFe2$
  $< 2 > 4.\text{ASSUME}\ NEWself \in Procs,$
                 $e3(self)$
          $PROVE\ Inv^{\theta}$
      $< 3 > .\wedge\ pc[self] = \text{“e3”}$
              $\wedge\ \text{UNCHANGED}\ \langle flag, unchecked, max, nxt\rangle$
          $BY < 2 > 4DEFe3$
      $< 3 > 1.\text{CASE}\ \ \wedge\ \exists\, k \in Nat :$
                           $num^{\theta} = [num \text{ EXCEPT } ![self] = k]$
                      $\wedge\ pc^{\theta} = [pc \text{ EXCEPT } ![self] = \text{“e3”}]$
          $BY < 3 > 1DEFInv$
      $< 3 > 2.\text{CASE}\ \ \wedge\ \exists\, i \in \{j \in Nat : j > max[self]\} :$
                          $num^{\theta} = [num \text{ EXCEPT } ![self] = i]$
                      $\wedge\ pc^{\theta} = [pc \text{ EXCEPT } ![self] = \text{“e4”}]$
          $BY < 3 > 2,\ Z3DEFInv$
      $< 3 > 3.QED\ \ BY < 3 > 1,\ < 3 > 2,\ < 2 > 4DEFe3$
  $< 2 > 5.\text{ASSUME}\ NEWself\ \ \ \ \ \ \ \ \in Procs,$
```

```
                  $e4(self)$
              $PROVE\ Inv'$
          $< 3 > .\ \land pc[self] = \text{“e4”}$
                  $\land \text{UNCHANGED } \langle num, max, nxt \rangle$
              $BY < 2 > 5DEFe4$
          $< 3 > 1.\text{CASE } \land flag' = [flag \text{ EXCEPT } ![self] = \neg flag[self]]$
                           $\land pc' = [pc \text{ EXCEPT } ![self] = \text{“e4”}]$
                           $\land \text{UNCHANGED } unchecked$
              $BY < 3 > 1DEFInv$
          $< 3 > 2.\text{CASE } \land flag' = [flag \text{ EXCEPT } ![self] = \text{FALSE}]$
                           $\land unchecked' = [unchecked \text{ EXCEPT } ![self] = Procs \setminus \{self\}]$
                           $\land pc' = [pc \text{ EXCEPT } ![self] = \text{“w1”}]$
              $BY < 3 > 2,\ Z3T(30)DEFInv$
          $< 3 > .QED\ \ BY < 3 > 1,\ < 3 > 2,\ < 2 > 5DEFe4$
      $< 2 > 6.\text{ASSUME } NEWself \in Procs,$
                  $w1(self)$
              $PROVE\ Inv'$
          $< 3 > .\ \land pc[self] = \text{“w1”}$
                  $\land \text{UNCHANGED } \langle num, flag, unchecked, max \rangle$
              $BY < 2 > 6DEFw1$
          $< 3 > 1.\text{CASE } \land unchecked[self] \neq \{\}$
                           $\land \exists\, i \in unchecked[self] :$
                                   $nxt' = [nxt \text{ EXCEPT } ![self] = i]$
                           $\land \neg flag[nxt'[self]]$
                           $\land pc' = [pc \text{ EXCEPT } ![self] = \text{“w2”}]$
              $BY < 3 > 1,\ Z3DEFInv$
          $< 3 > 2.\text{CASE } \land unchecked[self] = \{\}$
                           $\land pc' = [pc \text{ EXCEPT } ![self] = \text{“cs”}]$
                           $\land nxt' = nxt$
              $BY < 3 > 2,\ Z3DEFInv$
          $< 3 > .QED\ \ BY < 3 > 1,\ < 3 > 2,\ < 2 > 6DEFw1$
      $< 2 > 7.\text{ASSUME } NEWself \in Procs,$
                  $w2(self)$
              $PROVE\ Inv'$
          $BY < 2 > 7,\ Z3DEFw2,\ Inv$
      $< 2 > 8.\text{ASSUME } NEWself \in Procs,$
                  $cs(self)$
              $PROVE\ Inv'$
          $BY < 2 > 8,\ Z3DEFcs,\ Inv$
      $< 2 > 9.\text{ASSUME } NEWself \in Procs,$
                  $exit(self)$
              $PROVE\ Inv'$
          $< 3 > .\ \land pc[self] = \text{“exit”}$
                  $\land \text{UNCHANGED } \langle flag, unchecked, max, nxt \rangle$
              $BY < 2 > 9DEFexit$
```

$< 3 > 1.$CASE $\land \exists\, k \in Nat :$
$\qquad num^{\theta} = [num \text{ EXCEPT } ![self] = k]$
$\land\, pc^{\theta} = [pc \text{ EXCEPT } ![self] =$ “exit”$]$
$BY < 3 > 1 DEFInv$
$< 3 > 2.$CASE $\land\, num^{\theta} = [num \text{ EXCEPT } ![self] = 0]$
$\land\, pc^{\theta} = [pc \text{ EXCEPT } ![self] =$ “ncs”$]$
$BY < 3 > 2 DEFInv$
$< 3 > .QED\ \ BY < 3 > 1,\ < 3 > 2,\ < 2 > 9 DEFexit$
$< 2 > 10.$CASE UNCHANGED $vars$
$BY < 2 > 10 DEFvars,\ Inv$
$< 2 > 11.QED$
$BY < 2 > 1,\ < 2 > 10,\ < 2 > 2,\ < 2 > 3,\ < 2 > 4,\ < 2 > 5,\ < 2 > 6,\ < 2 > 7,\ < 2 > 8,\ < 2 > 9$
$< 1 > 3.Inv \Rightarrow MutualExclusion$
$BYSMTDEFMutualExclusion,\ Inv$
$< 1 > 4.QED$
$BY < 1 > 1,\ < 1 > 2,\ < 1 > 3,\ PTLDEFSpec$

$Trying(i) \triangleq pc[i] =$ “e1”
$InCS(i) \triangleq pc[i] =$ “cs”
$DeadlockFree \triangleq (\exists\, i \in Procs : Trying(i))\ \leadsto\ (\exists\, i \in Procs : InCS(i))$
$StarvationFree \triangleq \forall\, i \in Procs : Trying(i)\ \leadsto\ InCS(i)$

$II \triangleq \forall\, i \in Procs :$
$\land\ (pc[i] \in \{$“ncs”, “e1”, “e2”$\}) \Rightarrow (num[i] = 0)$ * not found Test 1 (21993 states)
$\land\, (pc[i] \in \{$“e4”, “w1”, “w2”, “cs”$\}) \Rightarrow (num[i] \neq 0)$ found Test 1
$\land\, (pc[i] \in \{$“e2”, “e3”$\}) \Rightarrow flag[i]$ found Test 1
$\land\, (pc[i] =$ “w2”$) \Rightarrow (nxt[i] \neq i)$ not found Test 1 (12115 states) or with N = 2
$\land\, pc[i] \in \{$“e2”, “w1”, “w2”$\} \Rightarrow i \notin unchecked[i]$ found Test 1
$\land\, (pc[i] \in \{$“w1”, “w2”$\}) \Rightarrow$ found Test 1
$\qquad \forall\, j \in (Procs \setminus unchecked[i]) \setminus \{i\} : Before(i, j)$
$\land\ \land\, (pc[i] =$ “w2”$)$ found Test 1
$\quad \land\ \lor\, (pc[nxt[i]] =$ “e2”$) \land (i \notin unchecked[nxt[i]])$
$\qquad \lor\, pc[nxt[i]] =$ “e3”
$\quad \Rightarrow max[nxt[i]] \geq num[i]$
$\land\, (pc[i] =$ “cs”$) \Rightarrow \forall\, j \in Procs \setminus \{i\} : Before(i, j)$ found Test 1

$IInit \triangleq \land\, num \in [Procs \rightarrow Nat]$
$\land\, flag \in [Procs \rightarrow \text{BOOLEAN}]$
$\land\, unchecked \in [Procs \rightarrow \text{SUBSET } Procs]$
$\land\, max \in [Procs \rightarrow Nat]$
$\land\, nxt \in [Procs \rightarrow Procs]$
$\land\, pc \in [Procs \rightarrow \{$“ncs”, “e1”, “e2”, “e3”,
“e4”, “w1”, “w2”, “cs”, “exit”$\}]$
$\land\, II$

$ISpec \triangleq IInit \land 2[Next]_{vars}$

* Modification History
* Last modified Sat Mar 07 08:41:02 CET 2020 by $merz$
* Last modified Tue Aug 27 12:23:10 PDT 2019 by $loki$
* Last modified Sat May 19 16:40:23 $CEST$ 2018 by $merz$
* Last modified Thu May 17 07:02:45 PDT 2018 by $lamport$
* Created Thu Nov 21 15:54:32 PST 2013 by $lamport$

Test 1: 5248 distinct initial states 151056 full initial states
$IInit \triangleq \land\, num \in [Procs \to Nat]$
$\quad\quad \land\, flag \in [Procs \to \text{BOOLEAN}]$
$\quad\quad \land\, unchecked \in [Procs \to \text{SUBSET } Procs]$
$\quad\quad \land\, max \in [Procs \to \{0\}]$ * $Nat]$
$\quad\quad \land\, nxt \in [Procs \to \{1\}]$
$\quad\quad \land\, pc \in [Procs \to \{$“ncs”, “e1”, “e2”, “e3”, “e4”, “w1”, “w2”, “cs”$\}]$
$\quad\quad \land\, II$