MODULE *Peterson*

EXTENDS *Integers*, *TLAPS*

$Not(i) \triangleq$ IF $i = 0$ THEN 1 ELSE 0

```
**************************************************************************
--algorithm Peterson{
    variables flag = [i ∈ {0, 1} ↦ FALSE], turn = 0 ;
    process ( proc ∈ {0, 1} ) {
        a0:  while ( TRUE ) {
        a1:      flag[self] := TRUE ;
        a2:      turn := Not(self) ;
        a3a:     if ( flag[Not(self)] ) { goto a3b } else { goto cs } ;
        a3b:     if ( turn = Not(self) ) { goto a3a } else { goto cs } ;
        cs:      skip ;
        a4:      flag[self] := FALSE ;
             }
    }
}
**************************************************************************
```

BEGIN TRANSLATION

VARIABLES *flag*, *turn*, *pc*

$vars \triangleq \langle flag, turn, pc \rangle$

$ProcSet \triangleq (\{0, 1\})$

$Init \triangleq$ Global variables
$\land\ flag = [i \in \{0, 1\} \mapsto \text{FALSE}]$
$\land\ turn = 0$
$\land\ pc = [self \in ProcSet \mapsto \text{“a0”}]$

$a0(self) \triangleq \land\ pc[self] = \text{“a0”}$
$\land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“a1”}]$
$\land$ UNCHANGED $\langle flag, turn \rangle$

$a1(self) \triangleq \land\ pc[self] = \text{“a1”}$
$\land\ flag' = [flag \text{ EXCEPT } ![self] = \text{TRUE}]$
$\land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“a2”}]$
$\land\ turn' = turn$

$a2(self) \triangleq \land\ pc[self] = \text{“a2”}$
$\land\ turn' = Not(self)$
$\land\ pc' = [pc \text{ EXCEPT } ![self] = \text{“a3a”}]$
$\land\ flag' = flag$

$a3a(self) \triangleq \land\ pc[self] = \text{“a3a”}$

$\land$ IF $flag[Not(self)]$
THEN $\land\ pc' = [pc$ EXCEPT $![self] =$ "a3b"$]$
ELSE $\land\ pc' = [pc$ EXCEPT $![self] =$ "cs"$]$
$\land$ UNCHANGED $\langle flag,\ turn\rangle$

$a3b(self) \triangleq$ $\land\ pc[self] =$ "a3b"
$\land$ IF $turn = Not(self)$
THEN $\land\ pc' = [pc$ EXCEPT $![self] =$ "a3a"$]$
ELSE $\land\ pc' = [pc$ EXCEPT $![self] =$ "cs"$]$
$\land$ UNCHANGED $\langle flag,\ turn\rangle$

$cs(self) \triangleq$ $\land\ pc[self] =$ "cs"
$\land$ TRUE
$\land\ pc' = [pc$ EXCEPT $![self] =$ "a4"$]$
$\land$ UNCHANGED $\langle flag,\ turn\rangle$

$a4(self) \triangleq$ $\land\ pc[self] =$ "a4"
$\land\ flag' = [flag$ EXCEPT $![self] =$ FALSE$]$
$\land\ pc' = [pc$ EXCEPT $![self] =$ "a0"$]$
$\land\ turn' = turn$

$proc(self) \triangleq\ a0(self) \lor a1(self) \lor a2(self) \lor a3a(self) \lor a3b(self)$
$\lor\ cs(self) \lor a4(self)$

$Next \triangleq\ (\exists\, self \in \{0, 1\} : proc(self))$

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

END TRANSLATION

$MutualExclusion \triangleq\ (pc[0] \neq$ "cs"$) \lor (pc[1] \neq$ "cs"$)$

$TypeOK \triangleq$ $\land\ pc \in [\{0, 1\} \to \{$"a0", "a1", "a2", "a3a", "a3b", "cs", "a4"$\}]$
$\land\ turn \in \{0, 1\}$
$\land\ flag\ \in [\{0, 1\} \to$ BOOLEAN $]$

$I \triangleq\ \forall\, i \in \{0, 1\} :$
$\land\ pc[i] \in \{$"a2", "a3a", "a3b", "cs", "a4"$\} \Rightarrow flag[i]$
$\land\ pc[i] \in \{$"cs", "a4"$\} \Rightarrow$ $\land\ pc[Not(i)] \notin \{$"cs", "a4"$\}$
$\land\ pc[Not(i)] \in \{$"a3a", "a3b"$\} \Rightarrow turn = i$

$Inv \triangleq\ TypeOK \land I$

THEOREM $Spec \Rightarrow \Box MutualExclusion$
$\langle 1 \rangle 1$. $Init \Rightarrow Inv$
BY *Zenon*, *Isa*DEFS *Init*, *Inv*, *TypeOK*, *I*, *ProcSet*
$\langle 1 \rangle 2$. $Inv \wedge [Next]_{vars} \Rightarrow Inv'$
BY DEFS *Inv*, *Next*, *TypeOK*, *I*, *Not*, *proc*, *a*0, *a*1, *a*2, *a*3*a*, *a*3*b*, *cs*, *a*4, *vars*
$\langle 2 \rangle 1$. SUFFICES ASSUME *Inv*, *Next*
PROVE *Inv*′
BY *Zenon*, *Isa*DEFS *Inv*, *TypeOK*, *I*, *vars*
$\langle 2 \rangle 2$. *TypeOK*′
BY *Zenon*, *Isa*, $\langle 2 \rangle 1$
DEFS *Inv*, *TypeOK*, *Next*, *proc*, *a*0, *a*1, *a*2, *a*3*a*, *a*3*b*, *cs*, *a*4, *Not*
$\langle 2 \rangle 3$. *I*′
$\langle 3 \rangle 1$. SUFFICES ASSUME NEW $j \in \{0, 1\}$
PROVE $I\,!\,(j)'$
BY *Zenon*, *Isa*DEFS *I*
$\langle 3 \rangle 2$. PICK $i \in \{0, 1\} : proc(i)$
BY *Zenon*, *Isa*, $\langle 2 \rangle 1$
DEFS *Next*, *I*, *TypeOK*, *Next*, *proc*, *a*0, *a*1, *a*2, *a*3*a*, *a*3*b*, *cs*, *a*4, *Not*
$\langle 3 \rangle 3$.CASE $i = j$
BY *Zenon*, *Isa*, $\langle 2 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$
DEFS *Inv*, *I*, *TypeOK*, *proc*, *a*0, *a*1, *a*2, *a*3*a*, *a*3*b*, *cs*, *a*4, *Not*
$\langle 3 \rangle 4$.CASE $i \neq j$
BY *Zenon*, *Isa*, $\langle 2 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 4$
DEFS *Inv*, *I*, *TypeOK*, *proc*, *a*0, *a*1, *a*2, *a*3*a*, *a*3*b*, *cs*, *a*4, *Not*
$\langle 3 \rangle 5$. QED
BY *Zenon*, *Isa*, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$
$\langle 2 \rangle 4$. QED
BY *Zenon*, *Isa*, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$ DEFS *Inv*
$\langle 1 \rangle 3$. $Inv \Rightarrow MutualExclusion$
BY *Zenon*, *Isa*DEFS *MutualExclusion*, *Inv*, *I*, *Not*
$\langle 1 \rangle 4$. QED
BY *Zenon*, *Isa*, $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, *PTL* DEF *Spec*

* Modification History
* Last modified *Tue Jan* 15 12:40:02 *GMT*+08:00 2019 by *pure_*
* Last modified *Mon Jan* 14 22:22:59 *CST* 2019 by *stary*
* Created *Fri Jan* 11 10:38:09 *CST* 2019 by *stary*