MODULE *ParReachProofs*

This module contains *TLAPS* checked proofs of the safety properties asserted in module *ParReach*–namely, the invariance of *Inv* and that the parallel algorithm implements the safety part of *Misra*'s algorithm under the refinement mapping defined there.

```
EXTENDS $ParReach, Integers, TLAPS$

LEMMA $TypeInvariant \triangleq Spec \Rightarrow \Box Inv$
$\langle 1 \rangle 1.$ $Init \Rightarrow Inv$
    BY $RootAssump$ DEF $Init, Inv, ProcSet$
$\langle 1 \rangle 2.$ $Inv \land [Next]_{vars} \Rightarrow Inv'$
   BY $SuccAssump$ DEF $Inv, Next, Terminating, vars, ProcSet, p, a, b, c$
$\langle 1 \rangle 3.$ QED
  BY $\langle 1 \rangle 1, \langle 1 \rangle 2, PTL$ DEF $Spec$

THEOREM $Spec \Rightarrow R!Init \land \Box[R!Next]_{R!vars}$
$\langle 1 \rangle 1.$ $Init \Rightarrow R!Init$
    BY $ProcsAssump$ DEF $Init, R!Init, pcBar, vrootBar, ProcSet$
$\langle 1 \rangle 2.$ $Inv \land [Next]_{vars} \Rightarrow [R!Next]_{R!vars}$
  $\langle 2 \rangle$ SUFFICES ASSUME $Inv$,
                             $[Next]_{vars}$
                    PROVE   $[R!Next]_{R!vars}$
    OBVIOUS
  $\langle 2 \rangle$ USE DEF $Inv, Next, Terminating, vars, R!Next, R!vars, vrootBar, pcBar$
  $\langle 2 \rangle 1.$ ASSUME NEW $self \in Procs$,
                    $a(self)$
        PROVE  $[R!Next]_{R!vars}$
    $\langle 3 \rangle 1.$ ASSUME $vroot \neq \{\}$
          PROVE  UNCHANGED $R!vars$
      BY $\langle 2 \rangle 1, \langle 3 \rangle 1$ DEF $a$
    $\langle 3 \rangle 2.$ ASSUME $vroot = \{\}$
          PROVE  $[R!Next]_{R!vars}$
      $\langle 4 \rangle 1.$ ASSUME $vrootBar = \{\}$
            PROVE  $[R!Next]_{R!vars}$
        BY $\langle 2 \rangle 1, \langle 3 \rangle 2, \langle 4 \rangle 1$ DEF $a, R!a$
      $\langle 4 \rangle 2.$ ASSUME $vrootBar \neq \{\}$
            PROVE UNCHANGED $R!vars$
        $\langle 5 \rangle 1.$ $\exists q \in Procs \setminus \{self\} : pc[q] \neq$ "Done"
          BY $\langle 4 \rangle 2, \langle 3 \rangle 2, \langle 2 \rangle 1$ DEF $a$
        $\langle 5 \rangle 2.$ $pcBar' \neq$ "Done"
          BY $\langle 5 \rangle 1, \langle 3 \rangle 2, \langle 2 \rangle 1$ DEF $a$
        $\langle 5 \rangle$.QED
          BY $\langle 5 \rangle 2, \langle 3 \rangle 2, \langle 2 \rangle 1$ DEF $a$
      $\langle 4 \rangle 3.$ QED
        BY $\langle 4 \rangle 1, \langle 4 \rangle 2$
    $\langle 3 \rangle 3.$ QED
      BY $\langle 3 \rangle 1, \langle 3 \rangle 2$ DEF $R!Next$
  ⟨2⟩2. ASSUME NEW $self \in Procs$,
                   $b(self)$
        PROVE  $[R!Next]_R!vars$
    BY ⟨2⟩2  DEF $b$, $R!a$
  ⟨2⟩3. ASSUME NEW $self \in Procs$,
                   $c(self)$
        PROVE   $[R!Next]_R!vars$
    BY ⟨2⟩3  DEF $c$
  ⟨2⟩4.CASE UNCHANGED $vars$
    BY ⟨2⟩4
  ⟨2⟩5. QED
    BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4  DEF $Next$, $Terminating$, $p$
⟨1⟩3. QED
  BY ⟨1⟩1, ⟨1⟩2, $TypeInvariant$, $PTL$ DEF $Spec$
```

* Modification History
* Last modified Sun *Apr* 14 16:55:36 *PDT* 2019 by *lamport*
* Created Sat *Apr* 13 14:37:54 *PDT* 2019 by *lamport*