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 alorithm implements the safety part of *Misra*'s algorithm under the refinement mapping defined there.

EXTENDS *ParReach*, *Integers*, *TLAPS*

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

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