Proving R2 for the Handshake Algorithm

THEOREM $Inv_H \land Inv_H{}' \land Next_H \Rightarrow [\overline{Next_A}]_{\overline{vars_A}}$

1. $p1_H \Rightarrow$ UNCHANGED $\overline{vars_A}$

   PROOF: Obvious, since $p1_H$ implies that p, c, and box are unchanged.

2. ASSUME: $Inv_H \land p2_H$

   PROVE: $\overline{Producer_A}$

   2.1. $p \oplus c = 0$

   PROOF: $p2_H$ implies $p = c$, which by the first two conjuncts of Inv_H imply $p \oplus c = 0$.

   2.2. $box' = \overline{Put_A}(box)$

   PROOF: Follows from the definition of $p2_H$, since $\overline{Put_A}(box)$ equals $Put_H(box)$.

   2.3. $(p \oplus c)' = 1$

   PROOF: $p2_H$ implies $(p \oplus c)' = (p \oplus 1) \oplus c$, which by 2.1 and the first two conjuncts of Inv_H implies $(p \oplus c)' = 1$.

   2.4. Q.E.D.

   PROOF: By 2.1–2.3, which prove the three conjuncts of $\overline{Producer_A}$.

3. $c1_H \Rightarrow$ UNCHANGED $\overline{vars_A}$

   PROOF: Obvious, since $c1_H$ implies that p, c, and box are unchanged.

4. ASSUME: $Inv \land c2_H$

   PROVE: $\overline{Consumer_A}$

   PROOF: Similar to the proof of step 2.

5. Q.E.D.

   PROOF: By 1–4 and simple logic, because $Next_H$ equals

   $$p1_H \lor p2_H \lor c1_H \lor c2_H$$

   and $[\overline{Next_A}]_{\overline{vars_A}}$ equals

   $$\overline{Producer_A} \lor \overline{Consumer_A} \lor \text{UNCHANGED } \overline{vars_A}$$

CLOSE