High-Level Proof of Inductive Invariance

$Inv \wedge Next \Rightarrow Inv'$

1. ASSUME: $Inv \wedge (i \in \{0,1\}) \wedge e1(i)$
   PROVE: Inv'
2. ASSUME: $Inv \wedge (i \in \{0,1\}) \wedge e2(i)$
   PROVE: Inv'
3. ASSUME: $Inv \wedge (i \in \{0,1\}) \wedge CS(i)$
   PROVE: Inv'
4. ASSUME: $Inv \wedge (i \in \{0,1\}) \wedge Rest(i)$
   PROVE: Inv'
5. Q.E.D.
   PROOF: By 1–4 and the assumption that $Next$ equals
   $\exists\, i \in \{0,1\} : e1(i) \vee e2(i) \vee CS(i) \vee Rest(i)$

   Click here if you don't understand why steps 1–4 imply the conclusion.

CLOSE