

High-Level Proof of Step 2

2. ASSUME: $Inv \wedge (i \in \{0, 1\}) \wedge e2(i)$

PROVE: Inv'

2.1. $TypeOK'$

2.2. $MutualExclusion'$

2.3. ASSUME: $j \in \{0, 1\}$

PROVE: $InCS(j)' \vee (pc'[j] = \text{"e2"}) \Rightarrow x'[j]$

2.4. Q.E.D.

PROOF: By 2.1–2.3 and the definition of Inv .

CLOSE