MODULE T_RWCAS

EXTENDS $Integers,\ FiniteSets,\ TLAPS$

CONSTANT N

VARIABLES $pc,\ X,\ x,\ v,\ T$

ASSUME $NPosInt \triangleq N \in Nat \setminus \{0\}$

$$
\begin{aligned}
vars &\triangleq \langle pc,\ X,\ x,\ v,\ T\rangle\\
ProcSet &\triangleq 1\,..\,N\\
Bot &\triangleq -15\\
Ack &\triangleq -20
\end{aligned}
$$

$$
\begin{aligned}
Init \triangleq\ & \land\ pc \in [ProcSet \to \{1,\ 4\}]\\
& \land\ X \in Nat\\
& \land\ x \in [ProcSet \to Nat]\\
& \land\ v \in [ProcSet \to Nat]\\
& \land\ T = \{[State \mapsto X,\\
& \qquad\qquad Ret \mapsto [p \in ProcSet \mapsto Bot]]\}
\end{aligned}
$$

$$
\begin{aligned}
Inv01 &\triangleq T \neq \{\}\\
Inv02 &\triangleq \forall\, t \in T : t.State = X\\
Inv03 &\triangleq \exists\, t \in T : (\forall\, q \in ProcSet : pc[q] = 3 \Rightarrow t.Ret[q] = Ack)
\end{aligned}
$$

$$
Inv1 \triangleq \forall\, p \in ProcSet : pc[p] = 1 \Rightarrow (\forall\, t \in T : t.Ret[p] = Bot)
$$

$$
\begin{aligned}
L1(p) \triangleq\ & \land\ pc[p] = 1\\
& \land\ pc' = [pc \text{ EXCEPT } ![p] = 2]\\
& \land\ x' = [x \text{ EXCEPT } ![p] = X]\\
& \land\ \text{UNCHANGED } \langle X,\ v,\ T\rangle
\end{aligned}
$$

$$
\begin{aligned}
Inv21 &\triangleq \forall\, p \in ProcSet : pc[p] = 2 \Rightarrow (\exists\, t \in T : t.Ret[p] = Bot)\\
Inv22 &\triangleq \forall\, p \in ProcSet : pc[p] = 2 \Rightarrow (X \neq x[p] \Rightarrow (\exists\, t \in T : t.Ret[p] = Ack))\\
Inv25 &\triangleq \forall\, p \in ProcSet : pc[p] = 2 \Rightarrow (X \neq x[p]\\
&\qquad\qquad \Rightarrow (\forall\, t \in T : t.Ret[p] = Bot\\
&\qquad\qquad\qquad \Rightarrow (\exists\, u \in T : u = [State \mapsto t.State,\\
&\qquad\qquad\qquad\qquad Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = Ack]\\
Inv23 &\triangleq \forall\, p \in ProcSet : pc[p] = 2 \Rightarrow (\forall\, t \in T : t.Ret[p] \in \{Bot,\ Ack\})\\
Inv24 &\triangleq \forall\, p \in ProcSet : pc[p] = 2 \Rightarrow (\forall\, t \in T : t.Ret[p] = Ack\\
&\qquad\qquad \Rightarrow (\exists\, u \in T : u = [State \mapsto t.State,\\
&\qquad\qquad\qquad Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = Bot]]))
\end{aligned}
$$

$$
\begin{aligned}
L2(p) \triangleq\ & \lor\ (\ \land\ pc[p] = 2\\
& \qquad \land\ X = x[p]\\
& \qquad \land\ pc' = [pc \text{ EXCEPT } ![p] = 3]\\
& \qquad \land\ X' = v[p]\\
& \qquad \land\ T' = \{u \in [State : \{v[p]\},\\
& \qquad\qquad\qquad Ret : [ProcSet \to Nat \cup \{Bot,\ Ack\}]] :\\
& \qquad\qquad \land\ u.Ret[p] = Ack
\end{aligned}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad \land\ u.State = v[p] \\
\qquad\qquad\qquad\qquad \land\ (\exists\, t \in T : \land\ t.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ t.State = x[p] \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ (\forall\, q \in ProcSet : \land\ ((\lor\ pc[q] \neq 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \lor\ t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q]) \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ (\land\ pc[q] = 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}))\} \\
\qquad\qquad \land\ \textsc{unchanged}\ \langle x,\ v\rangle) \\
\qquad \lor\ (\land\ pc[p] = 2 \\
\qquad\qquad \land\ X \neq x[p] \\
\qquad\qquad \land\ pc' = [pc\ \textsc{except}\ ![p] = 3] \\
\qquad\qquad \land\ \textsc{unchanged}\ \langle X,\ x,\ v,\ T\rangle)
\end{array}
$$

$$
Inv3 \triangleq \forall\, p \in ProcSet : pc[p] = 3 \Rightarrow (\exists\, t \in T : t.Ret[p] = Ack)
$$

$$
\begin{array}{ll}
L3(p) \triangleq & \land\ pc[p] = 3 \\
& \land\ \exists\, LineNum \in \{1,\ 4\} : pc' = [pc\ \textsc{except}\ ![p] = LineNum] \\
& \land\ \exists\, vNew \in Nat : v' = [v\ \textsc{except}\ ![p] = vNew] \\
& \land\ T' = \{[State \mapsto t.State,\ Ret \mapsto [t.Ret\ \textsc{except}\ ![p] = Bot]] : t \in \{u \in T : u.Ret[p] = Ack\}\} \\
& \land\ \textsc{unchanged}\ \langle X,\ x\rangle
\end{array}
$$

$$
Inv4 \triangleq \forall\, p \in ProcSet : pc[p] = 4 \Rightarrow (\forall\, t \in T : t.Ret[p] = Bot)
$$

$$
\begin{array}{ll}
L4(p) \triangleq & \land\ pc[p] = 4 \\
& \land\ pc' = [pc\ \textsc{except}\ ![p] = 5] \\
& \land\ x'\ = [x\ \textsc{except}\ ![p] = X] \\
& \land\ T' = \{[State \mapsto t.State,\ Ret \mapsto [t.Ret\ \textsc{except}\ ![p] = X]] : t \in T\} \\
& \land\ \textsc{unchanged}\ \langle X,\ v\rangle
\end{array}
$$

$$
Inv5 \triangleq \forall\, p \in ProcSet : pc[p] = 5 \Rightarrow (\forall\, t \in T : t.Ret[p] = x[p])
$$

$$
\begin{array}{ll}
L5(p) \triangleq & \land\ pc[p] = 5 \\
& \land\ \exists\, LineNum \in \{1,\ 4\} : pc' = [pc\ \textsc{except}\ ![p] = LineNum] \\
& \land\ T' = \{[State \mapsto t.State,\ Ret \mapsto [t.Ret\ \textsc{except}\ ![p] = Bot]] : t \in T\} \\
& \land\ \textsc{unchanged}\ \langle X,\ x,\ v\rangle
\end{array}
$$

Algorithm

$$
\begin{array}{ll}
Step(p) \triangleq & \lor\ L1(p) \\
& \lor\ L2(p) \\
& \lor\ L3(p) \\
& \lor\ L4(p) \\
& \lor\ L5(p)
\end{array}
$$

$$
Next \triangleq \exists\, p \in ProcSet : Step(p)
$$

$$
\begin{array}{ll}
Spec \triangleq & \land\ Init \\
& \land\ \Box[Next]_{vars}
\end{array}
$$

Inductive Invariance

$$Lines \triangleq \{1, 2, 3, 4, 5\}$$

$$\begin{aligned} TypeOK \triangleq\ & \land pc \in [ProcSet \rightarrow Lines] \\ & \land X \in Nat \\ & \land x \in [ProcSet \rightarrow Nat] \\ & \land v \in [ProcSet \rightarrow Nat] \\ & \land T \in \text{SUBSET } [State : Nat, Ret : [ProcSet \rightarrow Nat \cup \{Bot, Ack\}]] \end{aligned}$$

$$\begin{aligned} IInv \triangleq\ & \land TypeOK \\ & \land Inv01 \\ & \land Inv02 \\ & \land Inv1 \\ & \land Inv21 \\ & \land Inv22 \\ & \land Inv23 \\ & \land Inv24 \\ & \land Inv3 \\ & \land Inv4 \\ & \land Inv5 \\ & \land Inv25 \\ & \land Inv03 \end{aligned}$$

$$\begin{aligned} ISpec \triangleq\ & \land IInv \\ & \land \Box[Next]_{vars} \end{aligned}$$

WARNING: Cannot feasibly model check, because $T \in$ SUBSET [...]

THEOREM $TypeCorrectness \triangleq Spec \Rightarrow \Box TypeOK$
⟨1⟩ USE $NPosInt$ DEFS $ProcSet, Lines, TypeOK, Bot, Ack$
⟨1⟩ SUFFICES $\land (Init \Rightarrow TypeOK)$
$\land (TypeOK \land [Next]\_vars \Rightarrow TypeOK')$
PROOF BY PTL DEF $Spec$
⟨1⟩1. $Init \Rightarrow TypeOK$
PROOF BY DEF $Init$
⟨1⟩2. $TypeOK \land [Next]\_vars \Rightarrow TypeOK'$
⟨2⟩ SUFFICES ASSUME $TypeOK$,
$[Next]\_vars$
PROVE $TypeOK'$
OBVIOUS
⟨2⟩1. ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $TypeOK'$
PROOF BY ⟨2⟩1 DEF $L1$
⟨2⟩2. ASSUME NEW $p \in ProcSet$,
$L2(p)$

PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 2$ DEF $L2$
$\langle 2 \rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 3$ DEF $L3$
$\langle 2 \rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 4$ DEF $L4$
$\langle 2 \rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $TypeOK'$
PROOF BY $\langle 2 \rangle 5$ DEF $L5$
$\langle 2 \rangle 6.$CASE UNCHANGED $vars$
PROOF BY $\langle 2 \rangle 6$ DEF $vars$
$\langle 2 \rangle 7.$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$ DEF $Next$, $Step$
$\langle 1 \rangle 3.$ QED
PROOF BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$

THEOREM $Spec \Rightarrow \Box TypeOK$
$\langle 1 \rangle$ USE $NPosInt$DEFS $ProcSet$, $Lines$, Bot, Ack, $TypeOK$
$\langle 1 \rangle 1.$ $Init \Rightarrow TypeOK$
BY DEF $Init$
$\langle 1 \rangle 2.$ $TypeOK \wedge [Next]_{vars} \Rightarrow TypeOK'$
$\langle 2 \rangle$ SUFFICES ASSUME $TypeOK$,
$[Next]_{vars}$
PROVE $TypeOK'$
OBVIOUS
$\langle 2 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $TypeOK'$
BY $\langle 2 \rangle 1$ DEF $L1$
$\langle 2 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $TypeOK'$
BY $\langle 2 \rangle 2$ DEF $L2$
$\langle 2 \rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $TypeOK'$
BY $\langle 2 \rangle 3$ DEF $L3$
$\langle 2 \rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $TypeOK'$

BY $\langle 2\rangle 4$ DEF $L4$

$\langle 2\rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $TypeOK'$

$\langle 3\rangle 1.$ SUFFICES ASSUME NEW $LineNum \in \{1, 4\}$,
$pc' = [pc$ EXCEPT $![p] = LineNum]$
PROVE $TypeOK'$

BY $\langle 2\rangle 5$ DEF $L5$

$\langle 3\rangle$ QED

BY $\langle 2\rangle 5$, $\langle 3\rangle 1$ DEF $L5$

$\langle 2\rangle 6.$CASE UNCHANGED $vars$

BY $\langle 2\rangle 6$ DEF $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$

$\langle 2\rangle 7.$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$ DEF $Next$, $Step$

$\langle 1\rangle 3.$ QED

BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, PTL DEF $Spec$

THEOREM $Spec \Rightarrow \Box IInv$

$\langle 1\rangle$ USE $NPosInt$DEFS $ProcSet$, $Lines$, Bot, Ack, $IInv$

$\langle 1\rangle$ SUFFICES $\wedge (Init \Rightarrow IInv)$
$\wedge (IInv \wedge [Next]_{vars} \Rightarrow IInv')$

PROOF BY PTL DEF $Spec$

$\langle 1\rangle 1.$ $Init \Rightarrow IInv$

$\langle 2\rangle$ SUFFICES ASSUME $Init$
PROVE $IInv$

OBVIOUS

$\langle 2\rangle 1.$ $TypeOK$

PROOF BY DEF $Init$, $TypeOK$

$\langle 2\rangle 2.$ $Inv01$

PROOF BY Isa DEF $Init$, $Inv01$

$\langle 2\rangle 3.$ $Inv02$

PROOF BY DEF $Init$, $Inv02$

$\langle 2\rangle 4.$ $Inv1$

PROOF BY DEF $Init$, $Inv1$

$\langle 2\rangle 5.$ $Inv21$

PROOF BY DEF $Init$, $Inv21$

$\langle 2\rangle 6.$ $Inv22$

PROOF BY DEF $Init$, $Inv22$

$\langle 2\rangle 7.$ $Inv23$

PROOF BY DEF $Init$, $Inv23$

$\langle 2\rangle 8.$ $Inv24$

PROOF BY DEF $Init$, $Inv24$

$\langle 2\rangle 9.$ $Inv3$

PROOF BY DEF $Init$, $Inv3$

$\langle 2 \rangle 10.$ $Inv4$

PROOF BY DEF $Init$, $Inv4$

$\langle 2 \rangle 11.$ $Inv5$

PROOF BY DEF $Init$, $Inv5$

$\langle 2 \rangle 12.$ $Inv03$

PROOF BY DEF $Init$, $Inv03$

$\langle 2 \rangle 13.$ $Inv25$

PROOF BY DEF $Init$, $Inv25$

$\langle 2 \rangle 14.$ QED

BY $\langle 2 \rangle 1$, $\langle 2 \rangle 10$, $\langle 2 \rangle 11$, $\langle 2 \rangle 12$, $\langle 2 \rangle 13$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, $\langle 2 \rangle 5$, $\langle 2 \rangle 6$, $\langle 2 \rangle 7$, $\langle 2 \rangle 8$, $\langle 2 \rangle 9$ DEF $IInv$

$\langle 1 \rangle 2.$ $IInv \wedge [Next]_{vars} \Rightarrow IInv'$

$\langle 2 \rangle$ SUFFICES ASSUME $IInv \wedge [Next]_{vars}$
PROVE $IInv'$

OBVIOUS

$\langle 2 \rangle$ USE DEF $Next$, $Step$, $vars$

$\langle 2 \rangle 1.$ $TypeOK'$

$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $TypeOK'$

PROOF BY $\langle 3 \rangle 1$ DEF $TypeOK$, $L1$

$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $TypeOK'$

PROOF BY $\langle 3 \rangle 2$ DEF $TypeOK$, $L2$

$\langle 3 \rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $TypeOK'$

PROOF BY $\langle 3 \rangle 3$ DEF $TypeOK$, $L3$

$\langle 3 \rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $TypeOK'$

PROOF BY $\langle 3 \rangle 4$ DEF $TypeOK$, $L4$

$\langle 3 \rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $TypeOK'$

PROOF BY $\langle 3 \rangle 5$ DEF $TypeOK$, $L5$

$\langle 3 \rangle 6.$CASE UNCHANGED $vars$

PROOF BY $\langle 3 \rangle 6$ DEF $TypeOK$, $vars$

$\langle 3 \rangle 7.$ QED

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF $Next$, $Step$

$\langle 2 \rangle 2.$ $Inv01'$

$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv01'$

PROOF BY $\langle 3 \rangle 1$ DEF $Inv01$, $L1$

$$
\begin{array}{l}
\langle 3\rangle 2.\ \textsc{assume new}\ p \in \mathit{ProcSet},\\
\qquad\qquad L2(p)\\
\quad\ \textsc{prove}\ \ \mathit{Inv}01'\\
\ \langle 4\rangle 1.\textsc{case}\ \ \land\ pc[p] = 2\\
\qquad\qquad\quad \land\ X = x[p]\\
\qquad\qquad\quad \land\ pc' = [pc\ \textsc{except}\ ![p] = 3]\\
\qquad\qquad\quad \land\ X' = v[p]\\
\qquad\qquad\quad \land\ T' = \{u \in [\mathit{State} : \{v[p]\},\\
\qquad\qquad\qquad\qquad\qquad \mathit{Ret} : [\mathit{ProcSet} \to \mathit{Nat} \cup \{\mathit{Bot},\ \mathit{Ack}\}]] :\\
\qquad\qquad\qquad\qquad \land\ u.\mathit{Ret}[p] = \mathit{Ack}\\
\qquad\qquad\qquad\qquad \land\ u.\mathit{State} = v[p]\\
\qquad\qquad\qquad\qquad \land\ (\exists\, t \in T :\ \land\ t.\mathit{Ret}[p] = \mathit{Bot}\\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ t.\mathit{State} = x[p]\\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ (\forall\, q \in \mathit{ProcSet} :\ \land\ ((\lor\ pc[q] \neq 2\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \lor\ t.\mathit{Ret}[q] = \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] = t.\mathit{Ret}[q])\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \land\ (\ \land\ pc[q] = 2\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ t.\mathit{Ret}[q] \neq \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] \in \{\mathit{Bot},\ \mathit{Ack}\})))\}\\
\qquad\qquad\quad \land\ \textsc{unchanged}\ \langle x,\ v\rangle\\
\quad \langle 5\rangle 1.\ \textsc{pick}\ t \in T : t.\mathit{Ret}[p] = \mathit{Bot} \land t.\mathit{State} = x[p]\\
\qquad \textsc{by}\ \langle 4\rangle 1\ \ \textsc{def}\ \mathit{Inv}02,\ \mathit{Inv}21\\
\quad \langle 5\rangle.\ \textsc{define}\ u \triangleq\ [\mathit{State} \mapsto v[p],\\
\qquad\qquad\qquad\qquad \mathit{Ret} \mapsto [[q \in \mathit{ProcSet} \mapsto \textsc{if}\ pc[q] = 2 \land t.\mathit{Ret}[q] \neq \mathit{Ack}\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textsc{then}\ \mathit{Bot}\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textsc{else}\ \ t.\mathit{Ret}[q]]\ \textsc{except}\ ![p] = \mathit{Ack}]]\\
\quad \langle 5\rangle 2.\ \land\ u \in [\mathit{State} : \{v[p]\},\ \mathit{Ret} : [\mathit{ProcSet} \to \mathit{Nat} \cup \{\mathit{Bot},\ \mathit{Ack}\}]]\\
\qquad\quad \land\ u.\mathit{State} = v[p]\\
\qquad\quad \land\ u.\mathit{Ret}[p] = \mathit{Ack}\\
\qquad \textsc{by}\ \ \textsc{def}\ \mathit{TypeOK}\\
\quad \langle 5\rangle 3.\ \forall\, q \in \mathit{ProcSet} :\ \land\ (q \neq p) \Rightarrow \textsc{if}\ pc[q] = 2 \land t.\mathit{Ret}[q] \neq \mathit{Ack}\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textsc{then}\ u.\mathit{Ret}[q] \in \{\mathit{Bot},\ \mathit{Ack}\}\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textsc{else}\ \ u.\mathit{Ret}[q] = t.\mathit{Ret}[q]\\
\qquad\qquad\qquad\qquad\quad \land\ (q = p) \Rightarrow u.\mathit{Ret}[q] = \mathit{Ack}\\
\qquad \textsc{obvious}\\
\quad \langle 5\rangle 4.\ \forall\, q \in \mathit{ProcSet} :\ \land\ ((\lor\ pc[q] \neq 2\\
\qquad\qquad\qquad\qquad\qquad\quad \lor\ t.\mathit{Ret}[q] = \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] = t.\mathit{Ret}[q])\\
\qquad\qquad\qquad\qquad\quad \land\ (\ \land\ pc[q] = 2\\
\qquad\qquad\qquad\qquad\qquad\quad \land\ t.\mathit{Ret}[q] \neq \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] \in \{\mathit{Bot},\ \mathit{Ack}\}\\
\qquad \textsc{by}\ \langle 4\rangle 1,\ \langle 5\rangle 2,\ \langle 5\rangle 3\\
\quad \langle 5\rangle 5.\ u \in T'\\
\qquad \textsc{by}\ \langle 4\rangle 1,\ \langle 5\rangle 1,\ \langle 5\rangle 2,\ \langle 5\rangle 4,\ \mathit{Zenon}\\
\quad \langle 5\rangle 6.\ \textsc{qed}\\
\qquad \textsc{by}\ \langle 5\rangle 5\ \ \textsc{def}\ \mathit{Inv}01\\
\ \langle 4\rangle 2.\textsc{case}\ \ \land\ pc[p] = 2\\
\qquad\qquad\quad \land\ X \neq x[p]\\
\qquad\qquad\quad \land\ pc' = [pc\ \textsc{except}\ ![p] = 3]
\end{array}
$$

$\wedge$ UNCHANGED $\langle X, x, v, T\rangle$
PROOF BY $\langle 4\rangle 2$ DEF $Inv01$
$\langle 4\rangle 3.$ QED
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L2$
$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv01'$
$\langle 4\rangle 1.$ PICK $t \in T : t.Ret[p] = Ack$
BY $\langle 3\rangle 3$ DEF $L3$, $Inv03$
$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p] = Bot]]$
$\langle 4\rangle 2.$ $u \in T'$
BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, $Zenon$ DEF $L3$
$\langle 4\rangle$ QED
BY $\langle 4\rangle 2$ DEF $Inv01$
$\langle 3\rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv01'$
PROOF BY $\langle 3\rangle 4$, Isa DEF $Inv01$, $L4$
$\langle 3\rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv01'$
PROOF BY $\langle 3\rangle 5$, Isa DEF $Inv01$, $L5$
$\langle 3\rangle 6.$CASE UNCHANGED $vars$
PROOF BY $\langle 3\rangle 6$ DEF $Inv01$, $vars$
$\langle 3\rangle 7.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF $Next$, $Step$
$\langle 2\rangle 3.$ $Inv02'$
$\langle 3\rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv02'$
PROOF BY $\langle 3\rangle 1$, Isa DEF $Inv02$, $L1$
$\langle 3\rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv02'$
PROOF BY $\langle 3\rangle 2$, Isa DEF $Inv02$, $L2$
$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv02'$
PROOF BY $\langle 3\rangle 3$, Isa DEF $Inv02$, $L3$
$\langle 3\rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv02'$
PROOF BY $\langle 3\rangle 4$, Isa DEF $Inv02$, $L4$
$\langle 3\rangle 5.$ ASSUME NEW $p \in ProcSet$,

$L5(p)$
PROVE $Inv02'$
PROOF BY $\langle 3\rangle 5$, *Isa* DEF $Inv02$, $L5$
$\langle 3\rangle 6.$CASE UNCHANGED *vars*
PROOF BY $\langle 3\rangle 6$, *Isa* DEF $Inv02$, *vars*
$\langle 3\rangle 7.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF *Next*, *Step*
$\langle 2\rangle 4.$ $Inv1'$
$\langle 3\rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv1'$
PROOF BY $\langle 3\rangle 1$ DEF *TypeOK*, $Inv1$, $L1$
$\langle 3\rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv1'$
PROOF BY $\langle 3\rangle 2$ DEF *TypeOK*, $Inv1$, $L2$
$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv1'$
PROOF BY $\langle 3\rangle 3$ DEF *TypeOK*, $Inv1$, $L3$
$\langle 3\rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv1'$
PROOF BY $\langle 3\rangle 4$ DEF *TypeOK*, $Inv1$, $L4$
$\langle 3\rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv1'$
PROOF BY $\langle 3\rangle 5$ DEF *TypeOK*, $Inv1$, $L5$
$\langle 3\rangle 6.$CASE UNCHANGED *vars*
PROOF BY $\langle 3\rangle 6$ DEF *TypeOK*, $Inv1$, *vars*
$\langle 3\rangle 7.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF *Next*, *Step*
$\langle 2\rangle 5.$ $Inv21'$
$\langle 3\rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv21'$
PROOF BY $\langle 3\rangle 1$ DEF $L1$, $Inv01$, $Inv1$, $Inv21$
$\langle 3\rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv21'$
$\langle 4\rangle 1.$CASE $\land\ pc[p] = 2$
$\land\ X = x[p]$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = 3]$
$\land\ X' = v[p]$
$\land\ T' = \{u \in [State : \{v[p]\},$

$$
\begin{array}{l}
\qquad\qquad\qquad Ret : [ProcSet \rightarrow Nat \cup \{Bot,\ Ack\}]] : \\
\qquad\qquad \land\ u.Ret[p] = Ack \\
\qquad\qquad \land\ u.State = v[p] \\
\qquad\qquad \land\ (\exists\, t \in T :\ \land\ t.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad\quad \land\ t.State = x[p] \\
\qquad\qquad\qquad\qquad\quad \land\ (\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \lor\ t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q]) \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \land\ (\ \land\ pc[q] = 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \land\ t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}))\} \\
\qquad \land\ \text{UNCHANGED}\ \langle x,\ v\rangle \\
\langle 5\rangle\ \text{SUFFICES ASSUME NEW}\ p\_1 \in ProcSet', \\
\qquad\qquad\qquad\qquad (pc[p\_1] = 2)' \\
\qquad\qquad\qquad \text{PROVE}\quad (\exists\, t \in T : t.Ret[p\_1] = Bot)' \\
\quad \text{BY DEF}\ Inv21 \\
\langle 5\rangle 1.\ \text{PICK}\ t \in T :\ \land\ t.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad \land\ t.State = x[p] \\
\quad \text{BY}\ \langle 4\rangle 1\ \ \text{DEF}\ Inv02,\ Inv21 \\
\langle 5\rangle 2.\ \land\ pc[p\_1] = 2 \\
\qquad\ \land\ p\_1 \in ProcSet \\
\qquad\ \land\ p\_1 \neq p \\
\qquad\ \land\ t.Ret[p\_1] \in \{Bot,\ Ack\} \\
\quad \text{BY}\ \langle 4\rangle 1\ \ \text{DEF}\ L2,\ TypeOK,\ Inv23 \\
\langle 5\rangle\quad \text{DEFINE}\ t\_1 \triangleq [State \mapsto t.State, \\
\qquad\qquad\qquad\qquad Ret \mapsto [t.Ret\ \text{EXCEPT}\ ![p\_1] = Bot]] \\
\langle 5\rangle 3.\ t.Ret[p\_1] \neq Bot \Rightarrow\ \land\ t\_1 \in T \\
\qquad\qquad\qquad\qquad\qquad \land\ t\_1.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad\qquad \land\ t\_1.State = x[p] \\
\quad \text{BY}\ \langle 5\rangle 1,\ \langle 5\rangle 2\ \ \text{DEF}\ Inv24 \\
\langle 5\rangle 4.\ \exists\, t\_ \in T :\ \land\ t\_.Ret[p] = Bot \\
\qquad\qquad\qquad\quad \land\ t\_.Ret[p\_1] = Bot \\
\qquad\qquad\qquad\quad \land\ t\_.State = x[p] \\
\quad \text{BY}\ \langle 5\rangle 1,\ \langle 5\rangle 2,\ \langle 5\rangle 3\ \ \text{DEF}\ TypeOK \\
\langle 5\rangle\quad \text{PICK}\ t\_2 \in T :\ \land\ t\_2.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad \land\ t\_2.Ret[p\_1] = Bot \\
\qquad\qquad\qquad\qquad \land\ t\_2.State = x[p] \\
\quad \text{BY}\ \langle 5\rangle 4 \\
\langle 5\rangle\quad \text{DEFINE}\ u \triangleq [State \mapsto v[p], \\
\qquad\qquad\qquad Ret \mapsto [[q \in ProcSet \mapsto \text{IF}\ pc[q] = 2 \land t\_2.Ret[q] \neq Ack \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{THEN}\ Bot \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE}\ \ t\_2.Ret[q]]\ \text{EXCEPT}\ ![p] = Ack]] \\
\langle 5\rangle 5.\ \land\ u \in [State : \{v[p]\},\ Ret : [ProcSet \rightarrow Nat \cup \{Bot,\ Ack\}]] \\
\qquad\ \land\ u.State = v[p] \\
\qquad\ \land\ u.Ret[p] = Ack \\
\qquad\ \land\ u.Ret[p\_1] = Bot \\
\quad \text{BY}\ \langle 5\rangle 2\ \ \text{DEF}\ TypeOK
\end{array}
$$

$\langle 5\rangle 6.\ \forall\, q \in \mathit{ProcSet} :\ \wedge ((\vee\, pc[q] \neq 2$
$\qquad\qquad\qquad\qquad\vee\, t\_2.\mathit{Ret}[q] = \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] = t\_2.\mathit{Ret}[q])$
$\qquad\qquad\qquad\wedge (\wedge\, pc[q] = 2$
$\qquad\qquad\qquad\qquad\wedge\, t\_2.\mathit{Ret}[q] \neq \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] \in \{\mathit{Bot},\, \mathit{Ack}\}$

BY $\langle 4\rangle 1$

$\langle 5\rangle 7.\ u \in T'$

BY $\langle 4\rangle 1$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, *Zenon*

$\langle 5\rangle 8.$ QED

BY $\langle 5\rangle 5$, $\langle 5\rangle 7$ DEF *Inv*21

$\langle 4\rangle 2.$CASE $\wedge\, pc[p] = 2$
$\qquad\wedge\, X \neq x[p]$
$\qquad\wedge\, pc' = [pc \text{ EXCEPT } ![p] = 3]$
$\qquad\wedge$ UNCHANGED $\langle X,\, x,\, v,\, T\rangle$

PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF *L*2, *Inv*21

$\langle 4\rangle 3.$ QED

BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF *L*2

$\langle 3\rangle 3.$ ASSUME NEW $p \in \mathit{ProcSet}$,
$\qquad L3(p)$
PROVE $\mathit{Inv}21'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
$\qquad(pc[p\_1] = 2)'$
PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Bot})'$

BY DEF *Inv*21

$\langle 4\rangle 1.$ PICK $t \in T : t.\mathit{Ret}[p] = \mathit{Ack}$

BY $\langle 3\rangle 3$ DEF *L*3, *Inv*3

$\langle 4\rangle 2.\ t.\mathit{Ret}[p\_1] = \mathit{Ack} \Rightarrow \exists\, t\_ \in T : t\_ = [\mathit{State} \mapsto t.\mathit{State},$
$\qquad\qquad\mathit{Ret} \mapsto [t.\mathit{Ret} \text{ EXCEPT } ![p\_1] = \mathit{Bot}]]$

BY $\langle 3\rangle 3$ DEF *L*3, *Inv*24

$\langle 4\rangle 3.$ PICK $t\_ \in T :\ \wedge\, t\_.\mathit{Ret}[p] = \mathit{Ack}$
$\qquad\wedge\, t\_.\mathit{Ret}[p\_1] = \mathit{Bot}$

BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF *L*3, *Inv*23, *TypeOK*

$\langle 4\rangle$ DEFINE $u\_ \triangleq [\mathit{State} \mapsto t\_.\mathit{State},$
$\qquad\mathit{Ret} \mapsto [t\_.\mathit{Ret} \text{ EXCEPT } ![p] = \mathit{Bot}]]$

$\langle 4\rangle 4.\ u\_ \in T'$

BY $\langle 3\rangle 3$, $\langle 4\rangle 3$ DEF *L*3

$\langle 4\rangle 5.\ u\_.\mathit{Ret}[p\_1] = \mathit{Bot}$

BY $\langle 3\rangle 3$, $\langle 4\rangle 3$ DEF *L*3

$\langle 4\rangle 6.$ QED

PROOF BY $\langle 4\rangle 4$, $\langle 4\rangle 5$, *Zenon*

$\langle 3\rangle 4.$ ASSUME NEW $p \in \mathit{ProcSet}$,
$\qquad L4(p)$
PROVE $\mathit{Inv}21'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
$\qquad(pc[p\_1] = 2)'$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad \textsc{prove}\ \ (\exists\, t \in T : t.Ret[p\_1] = Bot)' \\
\quad \textsc{by}\ \ \textsc{def}\ Inv21 \\
\quad \langle 4\rangle 1.\ \textsc{pick}\ t \in T : t.Ret[p\_1] = Bot \\
\quad\quad \textsc{by}\ \langle 3\rangle 4\ \ \textsc{def}\ L4,\ Inv21 \\
\quad \langle 4\rangle\quad \textsc{define}\ u \triangleq [State \mapsto t.State, \\
\qquad\qquad\qquad\qquad\quad Ret \mapsto [t.Ret\ \textsc{except}\ ![p] = X]] \\
\quad \langle 4\rangle 2.\ u \in T' \\
\quad\quad \textsc{by}\ \langle 3\rangle 4,\ Zenon\ \textsc{def}\ L4 \\
\quad \langle 4\rangle 3.\ u.Ret[p\_1] = Bot \\
\quad\quad \textsc{by}\ \langle 3\rangle 4,\ \langle 4\rangle 1\ \ \textsc{def}\ L4 \\
\quad \langle 4\rangle 4.\ \textsc{qed} \\
\quad\quad \textsc{proof by}\ \langle 4\rangle 2,\ \langle 4\rangle 3,\ Zenon \\
\langle 3\rangle 5.\ \textsc{assume new}\ p \in ProcSet, \\
\qquad\qquad\quad L5(p) \\
\qquad\quad \textsc{prove}\ \ Inv21' \\
\quad \langle 4\rangle\ \textsc{suffices assume new}\ p\_1 \in ProcSet', \\
\qquad\qquad\qquad\qquad\quad (pc[p\_1] = 2)' \\
\qquad\qquad\qquad\qquad \textsc{prove}\ \ (\exists\, t \in T : t.Ret[p\_1] = Bot)' \\
\quad\quad \textsc{by}\ \ \textsc{def}\ Inv21 \\
\quad \langle 4\rangle 1.\ \textsc{pick}\ t \in T : t.Ret[p\_1] = Bot \\
\quad\quad \textsc{by}\ \langle 3\rangle 5\ \ \textsc{def}\ L5,\ Inv21 \\
\quad \langle 4\rangle\quad \textsc{define}\ u \triangleq [State \mapsto t.State, \\
\qquad\qquad\qquad\qquad\quad Ret \mapsto [t.Ret\ \textsc{except}\ ![p] = Bot]] \\
\quad \langle 4\rangle 2.\ u \in T' \\
\quad\quad \textsc{by}\ \langle 3\rangle 5,\ Zenon\ \textsc{def}\ L5 \\
\quad \langle 4\rangle 3.\ u.Ret[p\_1] = Bot \\
\quad\quad \textsc{by}\ \langle 3\rangle 5,\ \langle 4\rangle 1\ \ \textsc{def}\ L5 \\
\quad \langle 4\rangle 4.\ \textsc{qed} \\
\quad\quad \textsc{proof by}\ \langle 4\rangle 2,\ \langle 4\rangle 3,\ Zenon \\
\langle 3\rangle 6. \textsc{case unchanged}\ vars \\
\quad \textsc{proof by}\ \langle 3\rangle 6\ \ \textsc{def}\ vars,\ Inv21 \\
\langle 3\rangle 7.\ \textsc{qed} \\
\quad \textsc{by}\ \langle 3\rangle 1,\ \langle 3\rangle 2,\ \langle 3\rangle 3,\ \langle 3\rangle 4,\ \langle 3\rangle 5,\ \langle 3\rangle 6\ \ \textsc{def}\ Next,\ Step \\
\langle 2\rangle 6.\ Inv22' \\
\quad \langle 3\rangle 1.\ \textsc{assume new}\ p \in ProcSet, \\
\qquad\qquad\quad L1(p) \\
\qquad\quad \textsc{prove}\ \ Inv22' \\
\quad\quad \textsc{proof by}\ \langle 3\rangle 1\ \ \textsc{def}\ L1,\ TypeOK,\ Inv22 \\
\quad \langle 3\rangle 2.\ \textsc{assume new}\ p \in ProcSet, \\
\qquad\qquad\quad L2(p) \\
\qquad\quad \textsc{prove}\ \ Inv22' \\
\quad\quad \langle 4\rangle 1. \textsc{case}\ \ \land pc[p] = 2 \\
\qquad\qquad\qquad\ \ \land X = x[p] \\
\qquad\qquad\qquad\ \ \land pc' = [pc\ \textsc{except}\ ![p] = 3] \\
\qquad\qquad\qquad\ \ \land X' = v[p]
\end{array}
$$

$$
\begin{array}{l}
\land\ T' = \{u \in [\mathit{State} : \{v[p]\},\\
\qquad\qquad \mathit{Ret} : [\mathit{ProcSet} \rightarrow \mathit{Nat} \cup \{\mathit{Bot}, \mathit{Ack}\}]] :\\
\qquad\quad \land\ u.\mathit{Ret}[p] = \mathit{Ack}\\
\qquad\quad \land\ u.\mathit{State} = v[p]\\
\qquad\quad \land\ (\exists\, t \in T :\ \land\ t.\mathit{Ret}[p] = \mathit{Bot}\\
\qquad\qquad\qquad\quad \land\ t.\mathit{State} = x[p]\\
\qquad\qquad\qquad\quad \land\ (\forall\, q \in \mathit{ProcSet} :\ \land\ ((\lor\ pc[q] \neq 2\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \lor\ t.\mathit{Ret}[q] = \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] = t.\mathit{Ret}[q])\\
\qquad\qquad\qquad\qquad\qquad\qquad \land\ (\land\ pc[q] = 2\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \land\ t.\mathit{Ret}[q] \neq \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] \in \{\mathit{Bot}, \mathit{Ack}\})))\}\\
\land\ \text{UNCHANGED}\ \langle x, v\rangle
\end{array}
$$

$\langle 5\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
$(pc[p\_1] = 2)'$,
$(X \neq x[p\_1])'$
PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack})'$

BY DEF $\mathit{Inv}22$

$\langle 5\rangle$ $p \neq p\_1$

BY $\langle 4\rangle 1$ DEF $L2$, TypeOK

$\langle 5\rangle$ $x[p\_1] \neq v[p]$

BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF $L2$, TypeOK

$\langle 5\rangle 1.$ PICK $t \in T :\ \land\ t.\mathit{Ret}[p] = \mathit{Bot}$
$\land\ t.\mathit{State} = x[p]$

BY $\langle 4\rangle 1$ DEF $\mathit{Inv}02$, $\mathit{Inv}21$

$\langle 5\rangle 2.$ $\land\ pc[p\_1] = 2$
$\land\ p\_1 \in \mathit{ProcSet}$
$\land\ p\_1 \neq p$
$\land\ t.\mathit{Ret}[p\_1] \in \{\mathit{Bot}, \mathit{Ack}\}$

BY $\langle 4\rangle 1$ DEF $L2$, TypeOK, $\mathit{Inv}23$

$\langle 5\rangle$ DEFINE $t\_1 \triangleq [\mathit{State} \mapsto t.\mathit{State}$,
$\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p\_1] = \mathit{Bot}]]$

$\langle 5\rangle 3.$ $t.\mathit{Ret}[p\_1] \neq \mathit{Bot} \Rightarrow\ \land\ t\_1 \in T$
$\land\ t\_1.\mathit{Ret}[p] = \mathit{Bot}$
$\land\ t\_1.\mathit{State} = x[p]$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF $\mathit{Inv}24$

$\langle 5\rangle 4.$ $\exists\, t\_ \in T :\ \land\ t\_.\mathit{Ret}[p] = \mathit{Bot}$
$\land\ t\_.\mathit{Ret}[p\_1] = \mathit{Bot}$
$\land\ t\_.\mathit{State} = x[p]$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF TypeOK

$\langle 5\rangle$ PICK $t\_2 \in T :\ \land\ t\_2.\mathit{Ret}[p] = \mathit{Bot}$
$\land\ t\_2.\mathit{Ret}[p\_1] = \mathit{Bot}$
$\land\ t\_2.\mathit{State} = x[p]$

BY $\langle 5\rangle 4$

$\langle 5\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto v[p]$,
$\mathit{Ret} \mapsto [[[q \in \mathit{ProcSet} \mapsto$ IF $pc[q] = 2 \land t\_2.\mathit{Ret}[q] \neq \mathit{Ack}$
THEN Bot

ELSE $t\_2.Ret[q]]$ EXCEPT $![p] = Ack]$ EXCEPT $![p\_1] =$

$\langle 5\rangle 5.\ \wedge u \in [State : \{v[p]\},\ Ret : [ProcSet \rightarrow Nat \cup \{Bot,\ Ack\}]]$
$\quad \wedge u.State = v[p]$
$\quad \wedge u.Ret[p] = Ack$
$\quad \wedge u.Ret[p\_1] = Ack$
BY $\langle 5\rangle 2$ DEF $TypeOK$, $Zenon$

$\langle 5\rangle 6.\ \forall q \in ProcSet : \wedge ((\vee pc[q] \neq 2$
$\qquad \vee t\_2.Ret[q] = Ack) \Rightarrow u.Ret[q] = t\_2.Ret[q])$
$\quad \wedge (\wedge pc[q] = 2$
$\qquad \wedge t\_2.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}$
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$ DEF $L2$, $TypeOK$

$\langle 5\rangle 7.\ u \in T'$
BY $\langle 4\rangle 1$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, $Zenon$

$\langle 5\rangle 8.$ QED
BY $\langle 5\rangle 5$, $\langle 5\rangle 7$ DEF $Inv22$

$\langle 4\rangle 2.$CASE $\wedge pc[p] = 2$
$\quad \wedge X \neq x[p]$
$\quad \wedge pc' = [pc$ EXCEPT $![p] = 3]$
$\quad \wedge$ UNCHANGED $\langle X,\ x,\ v,\ T\rangle$
PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $L2$, $TypeOK$, $Inv22$

$\langle 4\rangle 3.$ QED
BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L2$

$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$\quad L3(p)$
PROVE $Inv22'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$\quad (pc[p\_1] = 2)'$,
$\quad (X \neq x[p\_1])'$
PROVE $(\exists t \in T : t.Ret[p\_1] = Ack)'$
BY DEF $Inv22$

$\langle 4\rangle 1.$ PICK $t \in T : t.Ret[p] = Ack$
BY $\langle 3\rangle 3$ DEF $L3$, $Inv3$

$\langle 4\rangle 2.\ t.Ret[p\_1] = Bot \Rightarrow \exists t\_ \in T : t\_ = [State \mapsto t.State,$
$\qquad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Ack]]$
BY $\langle 3\rangle 3$ DEF $L3$, $Inv25$

$\langle 4\rangle 3.$ PICK $t\_ \in T : \wedge t\_.Ret[p] = Ack$
$\quad \wedge t\_.Ret[p\_1] = Ack$
BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L3$, $Inv23$, $TypeOK$

$\langle 4\rangle$ DEFINE $u\_ \triangleq [State \mapsto t\_.State,$
$\quad Ret \mapsto [t\_.Ret$ EXCEPT $![p] = Bot]]$

$\langle 4\rangle 4.\ u\_ \in T'$
BY $\langle 3\rangle 3$, $\langle 4\rangle 3$, $Zenon$ DEF $L3$

$\langle 4\rangle 5.\ u\_.Ret[p\_1] = Ack$
BY $\langle 3\rangle 3$, $\langle 4\rangle 3$ DEF $L3$

$\langle 4\rangle 6.$ QED
  PROOF BY $\langle 4\rangle 4$, $\langle 4\rangle 5$, *Zenon*
$\langle 3\rangle 4.$ ASSUME NEW $p \in \mathit{ProcSet}$,
  $L4(p)$
  PROVE $\mathit{Inv}22'$
  $\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
    $(pc[p\_1] = 2)'$,
    $(X \neq x[p\_1])'$
    PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack})'$
  BY DEF $\mathit{Inv}22$
  $\langle 4\rangle 1.$ PICK $t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack}$
    BY $\langle 3\rangle 4$ DEF $L4$, TypeOK, $\mathit{Inv}22$
  $\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
    $\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = X]]$
  $\langle 4\rangle 2.$ $u \in T'$
    BY $\langle 3\rangle 4$, *Zenon* DEF $L4$
  $\langle 4\rangle 3.$ $u.\mathit{Ret}[p\_1] = \mathit{Ack}$
    BY $\langle 3\rangle 4$, $\langle 4\rangle 1$ DEF $L4$
  $\langle 4\rangle 4.$ QED
    PROOF BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, *Zenon*
$\langle 3\rangle 5.$ ASSUME NEW $p \in \mathit{ProcSet}$,
  $L5(p)$
  PROVE $\mathit{Inv}22'$
  $\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
    $(pc[p\_1] = 2)'$,
    $(X \neq x[p\_1])'$
    PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack})'$
  BY DEF $\mathit{Inv}22$
  $\langle 4\rangle 1.$ PICK $t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack}$
    BY $\langle 3\rangle 5$ DEF $L5$, TypeOK, $\mathit{Inv}22$
  $\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
    $\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = \mathit{Bot}]]$
  $\langle 4\rangle 2.$ $u \in T'$
    BY $\langle 3\rangle 5$, *Zenon* DEF $L5$
  $\langle 4\rangle 3.$ $u.\mathit{Ret}[p\_1] = \mathit{Ack}$
    BY $\langle 3\rangle 5$, $\langle 4\rangle 1$ DEF $L5$
  $\langle 4\rangle 4.$ QED
    PROOF BY $\langle 4\rangle 2$, $\langle 4\rangle 3$, *Zenon*
$\langle 3\rangle 6.$CASE UNCHANGED *vars*
  PROOF BY $\langle 3\rangle 6$ DEF *vars*, TypeOK, $\mathit{Inv}22$
$\langle 3\rangle 7.$ QED
  BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF *Next*, *Step*
$\langle 2\rangle 7.$ $\mathit{Inv}23'$
  $\langle 3\rangle 1.$ ASSUME NEW $p \in \mathit{ProcSet}$,
    $L1(p)$

PROVE $Inv23'$
PROOF BY $\langle 3 \rangle 1$ DEF $TypeOK$, $Inv1$, $Inv23$, $L1$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv23'$
PROOF BY $\langle 3 \rangle 2$ DEF $TypeOK$, $Inv23$, $L2$
$\langle 3 \rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv23'$
PROOF BY $\langle 3 \rangle 3$ DEF $TypeOK$, $Inv23$, $L3$
$\langle 3 \rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv23'$
PROOF BY $\langle 3 \rangle 4$ DEF $TypeOK$, $Inv23$, $L4$
$\langle 3 \rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv23'$
PROOF BY $\langle 3 \rangle 5$ DEF $TypeOK$, $Inv23$, $L5$
$\langle 3 \rangle 6.$CASE UNCHANGED $vars$
PROOF BY $\langle 3 \rangle 6$ DEF $TypeOK$, $Inv23$, $vars$
$\langle 3 \rangle 7.$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF $Next$, $Step$
$\langle 2 \rangle 8.$ $Inv24'$
$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv24'$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$(pc[p\_1] = 2)'$,
NEW $t \in T'$,
$(t.Ret[p\_1] = Ack)'$
PROVE $(\exists\, u \in T : u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]])'$
BY DEF $Inv24$
$\langle 4 \rangle 1.$ $\land\ T = T'$
$\land\ pc[p\_1] = 2$
BY $\langle 3 \rangle 1$ DEF $L1$, $TypeOK$, $Inv1$
$\langle 4 \rangle 2.$ PICK $u \in T : u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 4 \rangle 1$ DEF $Inv24$
$\langle 4 \rangle 4.$ QED
BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv24'$
$\langle 4 \rangle 1.$CASE $\land\ pc[p] = 2$

$$
\begin{array}{l}
\quad\quad \land\ X = x[p] \\
\quad\quad \land\ pc' = [pc \text{ EXCEPT } ![p] = 3] \\
\quad\quad \land\ X' = v[p] \\
\quad\quad \land\ T' = \{u \in [State : \{v[p]\}, \\
\quad\quad\quad\quad\quad\quad Ret : [ProcSet \to Nat \cup \{Bot,\ Ack\}]] : \\
\quad\quad\quad\quad\quad \land\ u.Ret[p] = Ack \\
\quad\quad\quad\quad\quad \land\ u.State = v[p] \\
\quad\quad\quad\quad\quad \land\ (\exists\, t \in T :\ \land\ t.Ret[p] = Bot \\
\quad\quad\quad\quad\quad\quad\quad\quad \land\ t.State = x[p] \\
\quad\quad\quad\quad\quad\quad\quad\quad \land\ (\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \lor\ t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q]) \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\ (\ \land\ pc[q] = 2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \land\ t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\})))\} \\
\quad\quad \land\ \text{UNCHANGED } \langle x,\ v\rangle
\end{array}
$$

$\langle 5\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$(pc[p\_1] = 2)'$,
NEW $t\_pr \in T'$,
$(t\_pr.Ret[p\_1] = Ack)'$
PROVE $\exists\, u \in T' : u = [State \mapsto t\_pr.State,$
$Ret \mapsto [t\_pr.Ret \text{ EXCEPT } ![p\_1] = Bot]]$

BY DEF $Inv24$

$\langle 5\rangle$ DEFINE $u \triangleq [State \mapsto t\_pr.State,$
$Ret \mapsto [t\_pr.Ret \text{ EXCEPT } ![p\_1] = Bot]]$

$\langle 5\rangle 1.$ PICK $t\_ \in T :$

$$
\begin{array}{l}
\land\ t\_.Ret[p] = Bot \\
\land\ t\_.State = x[p] \\
\land\ (\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2 \\
\quad\quad\quad \lor\ t\_.Ret[q] = Ack) \Rightarrow t\_pr.Ret[q] = t\_.Ret[q]) \\
\quad\quad \land\ (\ \land\ pc[q] = 2 \\
\quad\quad\quad \land\ t\_.Ret[q] \neq Ack) \Rightarrow t\_pr.Ret[q] \in \{Bot,\ Ack\})
\end{array}
$$

BY $\langle 4\rangle 1$

$\langle 5\rangle 2.$ $\land\ t\_.Ret[p\_1] \in \{Bot,\ Ack\}$
$\land\ t\_.Ret[p\_1] = Ack \Rightarrow \exists\, t\_1 \in T : t\_1 = [State \mapsto t\_.State,$
$Ret \mapsto [t\_.Ret \text{ EXCEPT } ![p\_1] = Bot]]$

BY $\langle 4\rangle 1$ DEF $L2$, $Inv23$, $Inv24$

$\langle 5\rangle$ DEFINE $u\_ \triangleq [State \mapsto t\_.State,$
$Ret \mapsto [t\_.Ret \text{ EXCEPT } ![p\_1] = Bot]]$

$\langle 5\rangle 3.$ $\land\ u\_ \in T$
$\land\ u\_.Ret[p] = Bot$
$\land\ u\_.State = x[p]$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF $L2$, $Inv24$, $TypeOK$

$\langle 5\rangle 4.$ $\land\ u \in [State : \{v[p]\},\ Ret : [ProcSet \to Nat \cup \{Bot,\ Ack\}]]$
$\land\ u.State = v[p]$
$\land\ u.Ret[p] = Ack$

BY $\langle 4\rangle 1$ DEF $L2$, $TypeOK$

$\langle 5\rangle 5.$ $\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2$

$\lor\ u\_.Ret[q] = Ack) \Rightarrow u.Ret[q] = u\_.Ret[q])$
$\land\ (\ \land\ pc[q] = 2$
$\land\ u\_.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}$

BY $\langle 5\rangle 1$, $\langle 5\rangle 4$ DEF $TypeOK$

$\langle 5\rangle 6.$ $\land\ u\_ \in T$
$\land\ u\_.Ret[p] = Bot$
$\land\ u\_.State = x[p]$
$\land\ (\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2$
$\lor\ u\_.Ret[q] = Ack) \Rightarrow u.Ret[q] = u\_.Ret[q])$
$\land\ (\ \land\ pc[q] = 2$
$\land\ u\_.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\})$

BY $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$

$\langle 5\rangle 7.$ $(\exists\, t \in T :\ \land\ t.Ret[p] = Bot$
$\land\ t.State = x[p]$
$\land\ (\forall\, q \in ProcSet :\ \land\ ((\ \lor\ pc[q] \neq 2$
$\lor\ t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])$
$\land\ (\ \land\ pc[q] = 2$
$\land\ t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}))$

BY $\langle 5\rangle 6$

$\langle 5\rangle 8.$ $u \in T'$

BY $\langle 4\rangle 1$, $\langle 5\rangle 4$, $\langle 5\rangle 7$, Isa DEF $TypeOK$, $L2$

$\langle 5\rangle$ QED

BY $\langle 5\rangle 8$ DEF $Inv24$

$\langle 4\rangle 2.$CASE $\land\ pc[p] = 2$
$\land\ X \neq x[p]$
$\land\ pc' = [pc$ EXCEPT $![p] = 3]$
$\land$ UNCHANGED $\langle X,\ x,\ v,\ T\rangle$

PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv24$, $L2$

$\langle 4\rangle 3.$ QED

BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L2$

$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv24'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$(pc[p\_1] = 2)'$,
NEW $t \in T'$,
$(t.Ret[p\_1] = Ack)'$
PROVE $(\exists\, u \in T : u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]])'$

BY DEF $Inv24$

$\langle 4\rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p] = Ack]]$

$\langle 4\rangle 1.$ $t\_ \in T$

BY $\langle 3\rangle 3$, $Z3$ DEF $L3$, $TypeOK$

$\langle 4 \rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State,$
$\quad Ret \mapsto [t\_.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 3 \rangle 3$, $\langle 4 \rangle 1$ DEF $L3$, $Inv24$
$\langle 4 \rangle 3.$ $u\_ \in \{u \in T : u.Ret[p] = Ack\}$
BY $\langle 4 \rangle 2$ DEF $TypeOK$
$\langle 4 \rangle 4.$ PICK $u \in T' : u = [State \mapsto u\_.State,$
$\quad Ret \mapsto [u\_.Ret$ EXCEPT $![p] = Bot]]$
BY $\langle 3 \rangle 3$, $\langle 4 \rangle 3$, $Zenon$ DEF $L3$
$\langle 4 \rangle 5.$ QED
BY $\langle 4 \rangle 2$, $\langle 4 \rangle 4$
$\langle 3 \rangle 4.$ ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv24'$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$(pc[p\_1] = 2)'$,
NEW $t \in T'$,
$(t.Ret[p\_1] = Ack)'$
PROVE $(\exists\, u \in T : u = [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]])'$
BY DEF $Inv24$
$\langle 4 \rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p] = Bot]]$
$\langle 4 \rangle 1.$ $t\_ \in T$
BY $\langle 3 \rangle 4$, $Z3$ DEF $TypeOK$, $Inv4$, $L4$
$\langle 4 \rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State,$
$\quad Ret \mapsto [t\_.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 3 \rangle 4$, $\langle 4 \rangle 1$ DEF $Inv24$, $L4$
$\langle 4 \rangle$ DEFINE $u \triangleq [State \mapsto u\_.State,$
$\quad Ret \mapsto [u\_.Ret$ EXCEPT $![p] = X]]$
$\langle 4 \rangle 3.$ $u \in T'$
BY $\langle 3 \rangle 4$, $\langle 4 \rangle 1$, $Zenon$ DEF $L4$
$\langle 4 \rangle 4.$ $u = [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF $TypeOK$
$\langle 4 \rangle 5.$ QED
BY $\langle 4 \rangle 3$, $\langle 4 \rangle 4$
$\langle 3 \rangle 5.$ ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv24'$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$(pc[p\_1] = 2)'$,
NEW $t \in T'$,
$(t.Ret[p\_1] = Ack)'$
PROVE $(\exists\, u \in T : u = [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]])'$

BY DEF $Inv24$
$\langle 4 \rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p] = x[p]]]$
$\langle 4 \rangle 1.$ $t\_ \in T$
BY $\langle 3 \rangle 5$, $Z3$ DEF $TypeOK$, $Inv5$, $L5$
$\langle 4 \rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State,$
$\quad Ret \mapsto [t\_.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 3 \rangle 5$, $\langle 4 \rangle 1$ DEF $Inv24$, $L5$
$\langle 4 \rangle$ DEFINE $u \triangleq [State \mapsto u\_.State,$
$\quad Ret \mapsto [u\_.Ret$ EXCEPT $![p] = Bot]]$
$\langle 4 \rangle 3.$ $u \in T'$
BY $\langle 3 \rangle 5$, $\langle 4 \rangle 1$, $Zenon$ DEF $L5$
$\langle 4 \rangle 4.$ $u = [State \mapsto t.State,$
$\quad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Bot]]$
BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF $TypeOK$
$\langle 4 \rangle 5.$ QED
BY $\langle 4 \rangle 3$, $\langle 4 \rangle 4$
$\langle 3 \rangle 6.$CASE UNCHANGED $vars$
PROOF BY $\langle 3 \rangle 6$ DEF $TypeOK$, $Inv24$, $L1$
$\langle 3 \rangle 7.$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF $Next$, $Step$
$\langle 2 \rangle 9.$ $Inv3'$
$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$\quad L1(p)$
PROVE $Inv3'$
PROOF BY $\langle 3 \rangle 1$ DEF $Inv3$, $L1$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$\quad L2(p)$
PROVE $Inv3'$
$\langle 4 \rangle 1.$CASE $\land\ pc[p] = 2$
$\quad \land\ X = x[p]$
$\quad \land\ pc' = [pc$ EXCEPT $![p] = 3]$
$\quad \land\ X' = v[p]$
$\quad \land\ T' = \{u \in [State : \{v[p]\},$
$\qquad Ret : [ProcSet \to Nat \cup \{Bot,\ Ack\}]] :$
$\qquad \land\ u.Ret[p] = Ack$
$\qquad \land\ u.State = v[p]$
$\qquad \land\ (\exists\, t \in T : \land\ t.Ret[p] = Bot$
$\qquad\qquad \land\ t.State = x[p]$
$\qquad\qquad \land\ (\forall\, q \in ProcSet : \land\ ((\lor\ pc[q] \neq 2$
$\qquad\qquad\qquad \lor\ t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])$
$\qquad\qquad\qquad \land\ (\land\ pc[q] = 2$
$\qquad\qquad\qquad\quad \land\ t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}))\}$
$\quad \land$ UNCHANGED $\langle x,\ v \rangle$
$\langle 5 \rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,

$(pc[p\_1] = 3)'$
PROVE $(\exists\, t \in T : t.Ret[p\_1] = Ack)'$
BY DEF $Inv3$
$\langle 5 \rangle 1.$ CASE $p = p\_1$
$\langle 6 \rangle 1.$ PICK $t \in T : \land\, t.State = x[p]$
$\land\, t.Ret[p] = Bot$
$\land\, t.Ret[p\_1] = Bot$
BY $\langle 4 \rangle 1$, $\langle 5 \rangle 1$ DEF $Inv02$, $Inv21$
$\langle 6 \rangle$ DEFINE $u \triangleq [State \mapsto v[p],$
$Ret \mapsto [[q \in ProcSet \mapsto$ IF $pc[q] = 2 \land t.Ret[q] \neq Ack$
THEN Bot
ELSE $t.Ret[q]]$ EXCEPT $![p] = Ack]]$
$\langle 6 \rangle 2.$ $\land\, u \in [State : \{v[p]\},\ Ret : [ProcSet \rightarrow Nat \cup \{Bot,\ Ack\}]]$
$\land\, u.State = v[p]$
$\land\, u.Ret[p] = Ack$
$\land\, u.Ret[p\_1] = Ack$
BY $\langle 5 \rangle 1$ DEF $TypeOK$
$\langle 6 \rangle 3.$ $\forall\, q \in ProcSet : \land\, ((\lor\, pc[q] \neq 2$
$\lor\, t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])$
$\land\, (\land\, pc[q] = 2$
$\land\, t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\}$
BY $\langle 4 \rangle 1$
$\langle 6 \rangle 4.$ $u \in T'$
BY $\langle 3 \rangle 2$, $\langle 4 \rangle 1$, $\langle 5 \rangle 1$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$ DEF $TypeOK$, $L2$, $Zenon$
$\langle 6 \rangle 5.$ QED
BY $\langle 6 \rangle 2$, $\langle 6 \rangle 4$
$\langle 5 \rangle 2.$ CASE $p \neq p\_1$
$\langle 6 \rangle 1.$ PICK $t\_ \in T : \land\, t\_.State = x[p]$
$\land\, t\_.Ret[p\_1] = Ack$
BY $\langle 4 \rangle 1$, $\langle 5 \rangle 2$ DEF $L2$, $TypeOK$, $Inv02$, $Inv3$
$\langle 6 \rangle 2.$ $t\_.Ret[p] = Ack \Rightarrow \exists\, u \in T : u = [State \mapsto t\_.State,$
$Ret \mapsto [t\_.Ret$ EXCEPT $![p] = Bot]]$
BY $\langle 4 \rangle 1$ DEF $L2$, $Inv24$, $TypeOK$
$\langle 6 \rangle 3.$ PICK $t \in T : \land\, t.State = x[p]$
$\land\, t.Ret[p] = Bot$
$\land\, t.Ret[p\_1] = Ack$
BY $\langle 4 \rangle 1$, $\langle 5 \rangle 2$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$ DEF $Inv23$, $TypeOK$
$\langle 6 \rangle$ DEFINE $u \triangleq [State \mapsto v[p],$
$Ret \mapsto [[q \in ProcSet \mapsto$ IF $pc[q] = 2 \land t.Ret[q] \neq Ack$
THEN Bot
ELSE $t.Ret[q]]$ EXCEPT $![p] = Ack]]$
$\langle 6 \rangle 4.$ $\land\, u \in [State : \{v[p]\},\ Ret : [ProcSet \rightarrow Nat \cup \{Bot,\ Ack\}]]$
$\land\, u.State = v[p]$
$\land\, u.Ret[p] = Ack$
BY DEF $TypeOK$

$\langle 6\rangle 5.\ \forall\, q \in \mathit{ProcSet} : \wedge\, ((\vee\, pc[q] \neq 2$
$\qquad \vee\, t.\mathit{Ret}[q] = \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] = t.\mathit{Ret}[q])$
$\quad \wedge\, (\wedge\, pc[q] = 2$
$\qquad \wedge\, t.\mathit{Ret}[q] \neq \mathit{Ack}) \Rightarrow u.\mathit{Ret}[q] \in \{\mathit{Bot}, \mathit{Ack}\}$

BY $\langle 4\rangle 1$

$\langle 6\rangle 6.\ u \in T'$

BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 3$, $\langle 6\rangle 4$, $\langle 6\rangle 5$ DEF *TypeOK*, *L2*, *Zenon*

$\langle 6\rangle$ QED

BY $\langle 6\rangle 3$, $\langle 6\rangle 6$ DEF *Inv3*, *Zenon*

$\langle 5\rangle 3.$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$

$\langle 4\rangle 2.$CASE $\wedge\, pc[p] = 2$
$\wedge\, X \neq x[p]$
$\wedge\, pc' = [pc$ EXCEPT $![p] = 3]$
$\wedge$ UNCHANGED $\langle X, x, v, T\rangle$

BY $\langle 4\rangle 2$ DEF *Inv22*, *Inv3*

$\langle 4\rangle 3.$ QED

BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF *L2*

$\langle 3\rangle 3.$ ASSUME NEW $p \in \mathit{ProcSet}$,
$L3(p)$
PROVE $\mathit{Inv3}'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
$(pc[p\_1] = 3)'$
PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack})'$

BY DEF *Inv3*

$\langle 4\rangle 1.$ PICK $t \in T : \wedge\, t.\mathit{Ret}[p] = \mathit{Ack}$
$\wedge\, t.\mathit{Ret}[p\_1] = \mathit{Ack}$

BY $\langle 3\rangle 3$ DEF *L3*, *Inv03*

$\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
$\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = \mathit{Bot}]]$

$\langle 4\rangle 2.\ u \in T'$

BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, *Zenon* DEF *L3*

$\langle 4\rangle 3.\ p\_1 \neq p$

BY $\langle 3\rangle 3$ DEF *L3*, *TypeOK*

$\langle 4\rangle 4.\ u.\mathit{Ret}[p\_1] = \mathit{Ack}$

BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEF *L3*

$\langle 4\rangle 5.$ QED

PROOF BY $\langle 4\rangle 2$, $\langle 4\rangle 4$, *Zenon*

$\langle 3\rangle 4.$ ASSUME NEW $p \in \mathit{ProcSet}$,
$L4(p)$
PROVE $\mathit{Inv3}'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in \mathit{ProcSet}'$,
$(pc[p\_1] = 3)'$
PROVE $(\exists\, t \in T : t.\mathit{Ret}[p\_1] = \mathit{Ack})'$

BY DEF *Inv3*

$\langle 4 \rangle 1.$ PICK $t \in T : t.Ret[p\_1] = Ack$
  BY $\langle 3 \rangle 4$ DEF $L4$, $Inv3$
$\langle 4 \rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
  $Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = X]]$
$\langle 4 \rangle 2.$ $u \in T'$
  BY $\langle 3 \rangle 4$, *Zenon* DEF $L4$
$\langle 4 \rangle 3.$ $u.Ret[p\_1] = Ack$
  BY $\langle 3 \rangle 4$, $\langle 4 \rangle 1$ DEF $L4$
$\langle 4 \rangle 4.$ QED
  PROOF BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$, *Zenon*
$\langle 3 \rangle 5.$ ASSUME NEW $p \in ProcSet$,
  $L5(p)$
  PROVE $Inv3'$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
  $(pc[p\_1] = 3)'$
  PROVE $(\exists\, t \in T : t.Ret[p\_1] = Ack)'$
  BY DEF $Inv3$
$\langle 4 \rangle 1.$ PICK $t \in T : t.Ret[p\_1] = Ack$
  BY $\langle 3 \rangle 5$ DEF $L5$, $Inv3$
$\langle 4 \rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
  $Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = Bot]]$
$\langle 4 \rangle 2.$ $u \in T'$
  BY $\langle 3 \rangle 5$, *Zenon* DEF $L5$
$\langle 4 \rangle 3.$ $u.Ret[p\_1] = Ack$
  BY $\langle 3 \rangle 5$, $\langle 4 \rangle 1$ DEF $L5$
$\langle 4 \rangle 4.$ QED
  PROOF BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$, *Zenon*
$\langle 3 \rangle 6.$CASE UNCHANGED *vars*
  PROOF BY $\langle 3 \rangle 6$ DEF $L4$, $Inv3$, *vars*
$\langle 3 \rangle 7.$ QED
  BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF *Next*, *Step*
$\langle 2 \rangle 10.$ $Inv4'$
$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
  $L1(p)$
  PROVE $Inv4'$
  PROOF BY $\langle 3 \rangle 1$ DEF $Inv4$, $L1$
$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
  $L2(p)$
  PROVE $Inv4'$
  PROOF BY $\langle 3 \rangle 2$ DEF *TypeOK*, $Inv4$, $L2$
$\langle 3 \rangle 3.$ ASSUME NEW $p \in ProcSet$,
  $L3(p)$
  PROVE $Inv4'$
  PROOF BY $\langle 3 \rangle 3$ DEF *TypeOK*, $Inv4$, $L3$
$\langle 3 \rangle 4.$ ASSUME NEW $p \in ProcSet$,

$L4(p)$
PROVE $Inv4'$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv4$, $L4$
⟨3⟩5. ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv4'$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv4$, $L5$
⟨3⟩6.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩6 DEF $Inv4$, $vars$
⟨3⟩7. QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6 DEF $Next$, $Step$
⟨2⟩11. $Inv5'$
⟨3⟩1. ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv5'$
PROOF BY ⟨3⟩1 DEF $Inv5$, $L1$
⟨3⟩2. ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv5'$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv5$, $L2$
⟨3⟩3. ASSUME NEW $p \in ProcSet$,
$L3(p)$
PROVE $Inv5'$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv5$, $L3$
⟨3⟩4. ASSUME NEW $p \in ProcSet$,
$L4(p)$
PROVE $Inv5'$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv5$, $L4$
⟨3⟩5. ASSUME NEW $p \in ProcSet$,
$L5(p)$
PROVE $Inv5'$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv5$, $L5$
⟨3⟩6.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩6 DEF $Inv5$, $vars$
⟨3⟩7. QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6 DEF $Next$, $Step$
⟨2⟩12. $Inv25'$
⟨3⟩1. ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv25'$
BY ⟨3⟩1 DEF $TypeOK$, $Inv25$, $L1$
⟨3⟩2. ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv25'$
⟨4⟩1.CASE $\land\, pc[p] = 2$

$$
\begin{array}{l}
\quad \land X = x[p] \\
\quad \land pc' = [pc \text{ EXCEPT } ![p] = 3] \\
\quad \land X' = v[p] \\
\quad \land T' = \{u \in [State : \{v[p]\}, \\
\qquad\qquad\qquad Ret : [ProcSet \to Nat \cup \{Bot,\ Ack\}]] : \\
\qquad\qquad \land u.Ret[p] = Ack \\
\qquad\qquad \land u.State = v[p] \\
\qquad\qquad \land (\exists\, t \in T :\ \land t.Ret[p] = Bot \\
\qquad\qquad\qquad\qquad \land t.State = x[p] \\
\qquad\qquad\qquad\qquad \land (\forall\, q \in ProcSet :\ \land ((\lor pc[q] \neq 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \lor t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q]) \\
\qquad\qquad\qquad\qquad\qquad\qquad \land (\land pc[q] = 2 \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \land t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\ Ack\})))\} \\
\quad \land \text{UNCHANGED } \langle x,\ v\rangle
\end{array}
$$

$$
\begin{array}{l}
\langle 5\rangle \text{ SUFFICES ASSUME NEW } p\_1 \in ProcSet', \\
\qquad\qquad\qquad (pc[p\_1] = 2)', \\
\qquad\qquad\qquad (X \neq x[p\_1])', \\
\qquad\qquad\qquad \text{NEW } t\_pr \in T', \\
\qquad\qquad\qquad (t\_pr.Ret[p\_1] = Bot)' \\
\qquad\quad \text{PROVE } (\exists\, u \in T : u = [State \mapsto t\_pr.State, \\
\qquad\qquad\qquad\qquad Ret \mapsto [t\_pr.Ret \text{ EXCEPT } ![p\_1] = Ack]])' \\
\quad \text{BY DEF } Inv25 \\
\langle 5\rangle \quad \text{DEFINE } u \triangleq [State \mapsto t\_pr.State, \\
\qquad\qquad\qquad Ret \mapsto [t\_pr.Ret \text{ EXCEPT } ![p\_1] = Ack]] \\
\langle 5\rangle 1.\ \text{PICK } t\_1 \in T :\ \land t\_1.Ret[p] = Bot \\
\qquad\qquad \land t\_1.State = x[p] \\
\qquad\qquad \land (\forall\, q \in ProcSet :\ \land ((\lor pc[q] \neq 2 \\
\qquad\qquad\qquad\qquad \lor t\_1.Ret[q] = Ack) \Rightarrow t\_pr.Ret[q] = t\_1.Ret[q]) \\
\qquad\qquad\qquad \land (\land pc[q] = 2 \\
\qquad\qquad\qquad\quad \land t\_1.Ret[q] \neq Ack) \Rightarrow t\_pr.Ret[q] \in \{Bot,\ Ack\}) \\
\quad \text{BY } \langle 4\rangle 1 \\
\langle 5\rangle 2.\ \land t\_1.Ret[p\_1] \in \{Bot,\ Ack\} \\
\qquad \land t\_1.Ret[p\_1] = Ack \Rightarrow \exists\, t\_ \in T : t\_ = [State \mapsto t\_1.State, \\
\qquad\qquad\qquad\qquad Ret \mapsto [t\_1.Ret \text{ EXCEPT } ![p\_1] = Bot]] \\
\quad \text{BY } \langle 4\rangle 1 \text{ DEF } L2,\ TypeOK,\ Inv23,\ Inv24 \\
\langle 5\rangle 3.\ \text{PICK } u\_ \in T :\ \land u\_.Ret[p] = Bot \\
\qquad\qquad \land u\_.Ret[p\_1] = Bot \\
\qquad\qquad \land u\_.State = x[p] \\
\qquad\qquad \land (\forall\, q \in ProcSet :\ \land ((\lor pc[q] \neq 2 \\
\qquad\qquad\qquad\qquad \lor u\_.Ret[q] = Ack) \Rightarrow t\_pr.Ret[q] = u\_.Ret[q]) \\
\qquad\qquad\qquad \land (\land pc[q] = 2 \\
\qquad\qquad\qquad\quad \land u\_.Ret[q] \neq Ack) \Rightarrow t\_pr.Ret[q] \in \{Bot,\ Ack\}) \\
\quad \text{BY } \langle 5\rangle 1,\ \langle 5\rangle 2 \\
\langle 5\rangle 4.\ pc[p\_1] = 2 \\
\quad \text{BY } \langle 4\rangle 1 \text{ DEF } L2,\ TypeOK
\end{array}
$$

$\langle 5\rangle 4.\ \ \land u\_ \in T$
$\quad\quad \land u\_.Ret[p] = Bot$
$\quad\quad \land u\_.State = x[p]$
$\quad\quad \land (\forall q \in ProcSet : \land ((\lor pc[q] \neq 2$
$\quad\quad\quad\quad\quad\quad\quad\quad \lor u\_.Ret[q] = Ack) \Rightarrow u.Ret[q] = u\_.Ret[q])$
$\quad\quad\quad\quad\quad\quad\quad \land (\land pc[q] = 2$
$\quad\quad\quad\quad\quad\quad\quad\quad \land u\_.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot, Ack\})$
$\quad$ BY $\langle 4\rangle 1$, $\langle 5\rangle 3$ DEF $L2$, $TypeOK$
$\langle 5\rangle 5.\ \land u \in [State : \{v[p]\}, Ret : [ProcSet \to Nat \cup \{Bot, Ack\}]]$
$\quad\quad \land u.State = v[p]$
$\quad\quad \land u.Ret[p] = Ack$
$\quad$ BY $\langle 4\rangle 1$ DEF $L2$, $TypeOK$
$\langle 5\rangle 6.\ (\exists t \in T : \land t.Ret[p] = Bot$
$\quad\quad\quad\quad \land t.State = x[p]$
$\quad\quad\quad\quad \land (\forall q \in ProcSet : \land ((\lor pc[q] \neq 2$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad \lor t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])$
$\quad\quad\quad\quad\quad\quad\quad\quad \land (\land pc[q] = 2$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad \land t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot, Ack\}))$
$\quad$ BY $\langle 5\rangle 3$, $\langle 5\rangle 4$
$\langle 5\rangle 7.\ u \in T'$
$\quad$ BY $\langle 4\rangle 1$, $\langle 5\rangle 4$, $\langle 5\rangle 6$ DEF $TypeOK$, $L2$
$\langle 5\rangle 8.$ QED
$\quad$ BY $\langle 5\rangle 7$ DEF $Inv25$
$\langle 4\rangle 2.$CASE $\land pc[p] = 2$
$\quad\quad \land X \neq x[p]$
$\quad\quad \land pc' = [pc$ EXCEPT $![p] = 3]$
$\quad\quad \land$ UNCHANGED $\langle X, x, v, T\rangle$
$\quad$ BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv25$, $L2$
$\langle 4\rangle 3.$ QED
$\quad$ BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L2$

$\langle 3\rangle 3.$ ASSUME NEW $p \in ProcSet$,
$\quad\quad L3(p)$
$\quad$ PROVE $Inv25'$
$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$,
$\quad\quad (pc[p\_1] = 2)'$,
$\quad\quad (X \neq x[p\_1])'$,
$\quad\quad$ NEW $t \in T'$,
$\quad\quad (t.Ret[p\_1] = Bot)'$
$\quad$ PROVE $(\exists u \in T : u = [State \mapsto t.State,$
$\quad\quad\quad Ret \mapsto [t.Ret$ EXCEPT $![p\_1] = Ack]])'$
$\quad$ BY DEF $Inv25$
$\langle 4\rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State,$
$\quad\quad Ret \mapsto [t.Ret$ EXCEPT $![p] = Ack]]$
$\langle 4\rangle 1.\ t\_ \in T$

BY $\langle 3\rangle 3$, $Z3$ DEF $L3$, $TypeOK$

$\langle 4\rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State, Ret \mapsto [t\_.Ret \text{ EXCEPT } ![p\_1] = Ack]]$

BY $\langle 3\rangle 3$, $\langle 4\rangle 1$ DEF $L3$, $Inv25$

$\langle 4\rangle 3.$ $u\_ \in \{u \in T : u.Ret[p] = Ack\}$

BY $\langle 4\rangle 2$ DEF $TypeOK$

$\langle 4\rangle 4.$ PICK $u \in T' : u = [State \mapsto u\_.State, Ret \mapsto [u\_.Ret \text{ EXCEPT } ![p] = Bot]]$

BY $\langle 3\rangle 3$, $\langle 4\rangle 3$, $Zenon$ DEF $L3$

$\langle 4\rangle 5.$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 4$

$\langle 3\rangle 4.$ ASSUME NEW $p \in ProcSet$, $L4(p)$
PROVE $Inv25'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$, $(pc[p\_1] = 2)'$, $(X \neq x[p\_1])'$, NEW $t \in T'$, $(t.Ret[p\_1] = Bot)'$
PROVE $(\exists\, u \in T : u = [State \mapsto t.State, Ret \mapsto [t.Ret \text{ EXCEPT } ![p\_1] = Ack]])'$

BY DEF $Inv25$

$\langle 4\rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State, Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = Bot]]$

$\langle 4\rangle 1.$ $t\_ \in T$

BY $\langle 3\rangle 4$, $Z3$ DEF $TypeOK$, $Inv4$, $L4$

$\langle 4\rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State, Ret \mapsto [t\_.Ret \text{ EXCEPT } ![p\_1] = Ack]]$

BY $\langle 3\rangle 4$, $\langle 4\rangle 1$ DEF $Inv25$, $L4$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto u\_.State, Ret \mapsto [u\_.Ret \text{ EXCEPT } ![p] = X]]$

$\langle 4\rangle 3.$ $u \in T'$

BY $\langle 3\rangle 4$, $\langle 4\rangle 1$, $Zenon$ DEF $L4$

$\langle 4\rangle 4.$ $u = [State \mapsto t.State, Ret \mapsto [t.Ret \text{ EXCEPT } ![p\_1] = Ack]]$

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $TypeOK$

$\langle 4\rangle 5.$ QED

BY $\langle 4\rangle 3$, $\langle 4\rangle 4$

$\langle 3\rangle 5.$ ASSUME NEW $p \in ProcSet$, $L5(p)$
PROVE $Inv25'$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p\_1 \in ProcSet'$, $(pc[p\_1] = 2)'$, $(X \neq x[p\_1])'$, NEW $t \in T'$,

$(t.Ret[p\_1] = Bot)'$

PROVE $(\exists\, u \in T : u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret \text{ EXCEPT } ![p\_1] = Ack]])'$

BY DEF $Inv25$

$\langle 4 \rangle$ DEFINE $t\_ \triangleq [State \mapsto t.State,$
$Ret \mapsto [t.Ret \text{ EXCEPT } ![p] = x[p]]]$

$\langle 4 \rangle 1.$ $t\_ \in T$

BY $\langle 3 \rangle 5$, $Z3$ DEF $TypeOK$, $Inv5$, $L5$

$\langle 4 \rangle 2.$ PICK $u\_ \in T : u\_ = [State \mapsto t\_.State,$
$Ret \mapsto [t\_.Ret \text{ EXCEPT } ![p\_1] = Bot]]$

BY $\langle 3 \rangle 5$, $\langle 4 \rangle 1$ DEF $Inv25$, $L5$

$\langle 4 \rangle$ DEFINE $u \triangleq [State \mapsto u\_.State,$
$Ret \mapsto [u\_.Ret \text{ EXCEPT } ![p] = Bot]]$

$\langle 4 \rangle 3.$ $u \in T'$

BY $\langle 3 \rangle 5$, $\langle 4 \rangle 1$, $Zenon$ DEF $L5$

$\langle 4 \rangle 4.$ $u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret \text{ EXCEPT } ![p\_1] = Ack]]$

BY $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF $TypeOK$

$\langle 4 \rangle 5.$ QED

BY $\langle 4 \rangle 3$, $\langle 4 \rangle 4$

$\langle 3 \rangle 6.$CASE UNCHANGED $vars$

BY $\langle 3 \rangle 6$ DEF $TypeOK$, $Inv25$

$\langle 3 \rangle 7.$ QED

BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$, $\langle 3 \rangle 5$, $\langle 3 \rangle 6$ DEF $Next$, $Step$

$\langle 2 \rangle 13.$ $Inv03'$

$\langle 3 \rangle 1.$ ASSUME NEW $p \in ProcSet$,
$L1(p)$
PROVE $Inv03'$

BY $\langle 3 \rangle 1$ DEF $TypeOK$, $Inv03$, $L1$

$\langle 3 \rangle 2.$ ASSUME NEW $p \in ProcSet$,
$L2(p)$
PROVE $Inv03'$

$\langle 4 \rangle 1.$CASE
$$
\begin{aligned}
&\land pc[p] = 2\\
&\land X = x[p]\\
&\land pc' = [pc \text{ EXCEPT } ![p] = 3]\\
&\land X' = v[p]\\
&\land T' = \{u \in [State : \{v[p]\},\\
&\qquad\qquad Ret : [ProcSet \to Nat \cup \{Bot, Ack\}]] :\\
&\qquad \land u.Ret[p] = Ack\\
&\qquad \land u.State = v[p]\\
&\qquad \land (\exists\, t \in T : \land t.Ret[p] = Bot\\
&\qquad\qquad \land t.State = x[p]\\
&\qquad\qquad \land (\forall\, q \in ProcSet : \land ((\lor pc[q] \neq 2\\
&\qquad\qquad\qquad \lor t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])\\
&\qquad\qquad\qquad \land (\land pc[q] = 2
\end{aligned}
$$

$\wedge\, t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\, Ack\})) \}$

$\wedge$ UNCHANGED $\langle x,\, v \rangle$

BY $\langle 4 \rangle 1$, $\langle 3 \rangle 2$ DEF *TypeOK*, *Inv*03, *L*2

$\langle 5 \rangle 1.$ PICK $t\_1 \in T : (\forall\, q \in ProcSet : pc[q] = 3 \Rightarrow t\_1.Ret[q] = Ack)$

BY $\langle 3 \rangle 2$ DEF *Inv*03

$\langle 5 \rangle 2.$ $\wedge\, t\_1.Ret[p] \in \{Bot,\, Ack\}$
$\wedge\, t\_1.Ret[p] = Ack \Rightarrow \exists\, u \in T : u = [State \mapsto t\_1.State,$
$Ret \mapsto [t\_1.Ret$ EXCEPT $![p] = Bot]]$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 1$ DEF *Inv*23, *Inv*24, *TypeOK*

$\langle 5 \rangle 3.$ PICK $t \in T :$ $\wedge\, (\forall\, q \in ProcSet : pc[q] = 3 \Rightarrow t.Ret[q] = Ack)$
$\wedge\, t.Ret[p] = Bot$
$\wedge\, t.State = x[p]$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 1$, $\langle 5 \rangle 2$ DEF *TypeOK*, *Inv*02

$\langle 5 \rangle$ DEFINE $u \triangleq [State \mapsto v[p],$
$Ret \mapsto [t.Ret$ EXCEPT $![p] = Ack]]$

$\langle 5 \rangle 4.$ $\forall\, q \in ProcSet :$ $\wedge\, ((\vee\, pc[q] \neq 2$
$\vee\, t.Ret[q] = Ack) \Rightarrow u.Ret[q] = t.Ret[q])$
$\wedge\, (\wedge\, pc[q] = 2$
$\wedge\, t.Ret[q] \neq Ack) \Rightarrow u.Ret[q] \in \{Bot,\, Ack\}$

BY $\langle 4 \rangle 1$ DEF *Inv*23

$\langle 5 \rangle 5.$ $\wedge\, u \in [State : \{v[p]\},\, Ret : [ProcSet \to Nat \cup \{Bot,\, Ack\}]]$
$\wedge\, u.State = v[p]$
$\wedge\, u.Ret[p] = Ack$

BY $\langle 4 \rangle 1$ DEF *TypeOK*

$\langle 5 \rangle 6.$ $u \in T'$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 3$, $\langle 5 \rangle 4$, $\langle 5 \rangle 5$

$\langle 5 \rangle 7.$ $\forall\, q \in ProcSet : pc'[q] = 3 \Rightarrow u.Ret[q] = Ack$

BY $\langle 4 \rangle 1$, $\langle 5 \rangle 3$ DEF *TypeOK*

$\langle 5 \rangle 8.$ QED

BY $\langle 5 \rangle 6$, $\langle 5 \rangle 7$ DEF *Inv*03

$\langle 4 \rangle 2.$CASE $\wedge\, pc[p] = 2$
$\wedge\, X \neq x[p]$
$\wedge\, pc' = [pc$ EXCEPT $![p] = 3]$
$\wedge$ UNCHANGED $\langle X,\, x,\, v,\, T \rangle$

$\langle 5 \rangle 1.$ PICK $t \in T : (\forall\, q \in ProcSet : pc[q] = 3 \Rightarrow t.Ret[q] = Ack)$

BY $\langle 3 \rangle 2$ DEF *Inv*03

$\langle 5 \rangle 2.$ $\wedge\, t.Ret[p] \in \{Bot,\, Ack\}$
$\wedge\, t.Ret[p] = Bot \Rightarrow \exists\, u \in T : u = [State \mapsto t.State,$
$Ret \mapsto [t.Ret$ EXCEPT $![p] = Ack]]$

BY $\langle 4 \rangle 2$ DEF *Inv*23, *Inv*25

$\langle 5 \rangle 3.$ PICK $u \in T :$ $\wedge\, (\forall\, q \in ProcSet : pc[q] = 3 \Rightarrow u.Ret[q] = Ack)$
$\wedge\, u.Ret[p] = Ack$

BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$ DEF *TypeOK*

$\langle 5 \rangle 4.$ $u \in T'$

BY $\langle 4 \rangle 2$

$\langle 5\rangle 5.\ \forall\, q \in \mathit{ProcSet} : pc'[q] = 3 \Rightarrow u.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 4\rangle 2$, $\langle 5\rangle 3$ DEF TypeOK
$\langle 5\rangle 6.$ QED
  BY $\langle 5\rangle 4$, $\langle 5\rangle 5$ DEF $\mathit{Inv}03$
$\langle 4\rangle 3.$ QED
  BY $\langle 3\rangle 2$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L2$
$\langle 3\rangle 3.$ ASSUME NEW $p \in \mathit{ProcSet}$,
    $L3(p)$
  PROVE $\mathit{Inv}03'$
$\langle 4\rangle 1.$ PICK $t \in T : \forall\, q \in \mathit{ProcSet} : pc[q] = 3 \Rightarrow t.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 3$ DEF $\mathit{Inv}03$
$\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
    $\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = \mathit{Bot}]]$
$\langle 4\rangle 2.\ u \in T'$
  BY $\langle 3\rangle 3$, $\langle 4\rangle 1$, *Zenon* DEF $L3$
$\langle 4\rangle 3.\ \forall\, q \in \mathit{ProcSet} : pc'[q] = 3 \Rightarrow u.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 3$, $\langle 4\rangle 1$ DEF $L3$, TypeOK
$\langle 4\rangle$ QED
  BY $\langle 3\rangle 3$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, *Zenon* DEF $\mathit{Inv}03$, $L3$
$\langle 3\rangle 4.$ ASSUME NEW $p \in \mathit{ProcSet}$,
    $L4(p)$
  PROVE $\mathit{Inv}03'$
$\langle 4\rangle 1.$ PICK $t \in T : \forall\, q \in \mathit{ProcSet} : pc[q] = 3 \Rightarrow t.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 4$ DEF $\mathit{Inv}03$
$\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
    $\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = X]]$
$\langle 4\rangle 2.\ u \in T'$
  BY $\langle 3\rangle 4$, *Zenon* DEF $L4$
$\langle 4\rangle 3.\ \forall\, q \in \mathit{ProcSet} : pc'[q] = 3 \Rightarrow u.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 4$, $\langle 4\rangle 1$ DEF $L4$
$\langle 4\rangle$ QED
  BY $\langle 3\rangle 4$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, *Zenon* DEF $\mathit{Inv}03$, $L4$
$\langle 3\rangle 5.$ ASSUME NEW $p \in \mathit{ProcSet}$,
    $L5(p)$
  PROVE $\mathit{Inv}03'$
$\langle 4\rangle 1.$ PICK $t \in T : \forall\, q \in \mathit{ProcSet} : pc[q] = 3 \Rightarrow t.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 5$ DEF $\mathit{Inv}03$
$\langle 4\rangle$ DEFINE $u \triangleq [\mathit{State} \mapsto t.\mathit{State},$
    $\mathit{Ret} \mapsto [t.\mathit{Ret}$ EXCEPT $![p] = \mathit{Bot}]]$
$\langle 4\rangle 2.\ u \in T'$
  BY $\langle 3\rangle 5$, *Zenon* DEF $L5$
$\langle 4\rangle 3.\ \forall\, q \in \mathit{ProcSet} : pc'[q] = 3 \Rightarrow u.\mathit{Ret}[q] = \mathit{Ack}$
  BY $\langle 3\rangle 5$, $\langle 4\rangle 1$ DEF $L5$
$\langle 4\rangle 4.$ QED
  BY $\langle 3\rangle 5$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, *Zenon* DEF $\mathit{Inv}03$, $L5$

$\langle 3\rangle 6.$CASE UNCHANGED *vars*

BY $\langle 3\rangle 6$ DEF *TypeOK*, *Inv*03, *vars*

$\langle 3\rangle 7.$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$ DEF *Next*, *Step*

$\langle 2\rangle 14.$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 10$, $\langle 2\rangle 11$, $\langle 2\rangle 12$, $\langle 2\rangle 13$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 2\rangle 9$ DEF *IInv*

$\langle 1\rangle 3.$ QED

PROOF BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

* Modification History

* Last modified *Fri* May 14 11:33:08 *EDT* 2021 by *uguryavuz*

* Created *Thu* May 06 15:11:18 *EDT* 2021 by *uguryavuz*