MODULE *T_SNAP*

EXTENDS *Integers*, *FiniteSets*, *TLAPS*

VARIABLES pc, X, A, B, v, a, b, T

$vars \triangleq \langle pc, X, A, B, v, a, b, T\rangle$
$ProcSet \triangleq \{\text{“S”}, \text{“W”}\}$
$Bot \triangleq -10$
$Ack \triangleq -15$

$$\begin{aligned}
Init \triangleq\ & \land pc = [p \in ProcSet \mapsto \text{IF } p = \text{“W”} \text{ THEN } 1 \text{ ELSE } 5] \\
& \land X = \text{FALSE} \\
& \land A \in Nat \\
& \land B \in Nat \cup \{Bot\} \\
& \land a \in Nat \\
& \land b \in Nat \cup \{Bot\} \\
& \land v \in Nat \\
& \land T = \{[State \mapsto A, \\
& \qquad RetW \mapsto Bot, \\
& \qquad RetS \mapsto Bot]\}
\end{aligned}$$

```
Original algorithm
write(v)
  A ← v
  if X
    B ← v
  return ack
scan()
  X ← true
  B ← ⊥
  a ← A
  X ← false
  b ← B
  if b = ⊥ return a else b
```

$$\begin{aligned}
Inv1A \triangleq\ & pc[\text{“W”}] = 1 \Rightarrow (\exists\, t \in T : \land t.State = A \\
& \qquad\qquad\qquad\qquad\qquad\qquad \land t.RetW = Bot) \\
Inv1B \triangleq\ & pc[\text{“W”}] = 1 \Rightarrow (\forall\, t \in T : \land t.State = A \\
& \qquad\qquad\qquad\qquad\qquad\qquad \land t.RetW = Bot)
\end{aligned}$$

$$\begin{aligned}
L1 \triangleq\ & \lor (\land pc[\text{“W”}] = 1 \\
& \quad \land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2] \\
& \quad \land A' = v \\
& \quad \land (\lor X = \text{FALSE} \\
& \qquad \lor pc[\text{“S”}] = 6 \\
& \qquad \lor (\land pc[\text{“S”}] = 7 \\
& \qquad\quad \land B = Bot)
\end{aligned}$$

$$
\begin{array}{l}
\quad \lor B = v \\
\quad \lor (\land pc[\text{“S”}] = 8 \\
\qquad \land B = Bot \\
\qquad \land a = v)) \\
\land T' = \{[State \mapsto v, \\
\qquad\quad RetW \mapsto Ack, \\
\qquad\quad RetS \mapsto t.RetS] : t \in T\} \\
\land \text{UNCHANGED } \langle X, B, v, a, b\rangle)
\end{array}
$$

$$
\begin{array}{l}
\lor (\land pc[\text{“W”}] = 1 \\
\quad \land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2] \\
\quad \land A' = v \\
\quad \land (\land X = \text{TRUE} \\
\qquad \land pc[\text{“S”}] \neq 6 \\
\qquad \land (\lor pc[\text{“S”}] \neq 7 \\
\qquad\quad \lor B \neq Bot) \\
\qquad \land B \neq v \\
\qquad \land (\lor pc[\text{“S”}] \neq 8 \\
\qquad\quad \lor B \neq Bot \\
\qquad\quad \lor a \neq v)) \\
\quad \land T' = \{[State \mapsto v, \\
\qquad\quad RetW \mapsto Ack, \\
\qquad\quad RetS \mapsto t.RetS] : t \in T\} \cup T \\
\quad \land \text{UNCHANGED } \langle X, B, v, a, b\rangle)
\end{array}
$$

$$
\begin{array}{lcl}
Inv2A & \triangleq & pc[\text{“W”}] = 2 \Rightarrow A = v \\
Inv2B & \triangleq & pc[\text{“W”}] = 2 \Rightarrow (\exists\, t \in T : \land t.State = v \\
 & & \qquad\qquad\qquad\qquad \land t.RetW = Ack) \\
Inv2C & \triangleq & pc[\text{“W”}] = 2 \Rightarrow (X = \text{FALSE} \Rightarrow (\forall\, t \in T : \land t.State = v \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad \land t.RetW = Ack)) \\
Inv2D & \triangleq & pc[\text{“W”}] = 2 \Rightarrow (\exists\, t \in T : t.RetW = Bot \Rightarrow (\lor (\land pc[\text{“S”}] \in \{7, 8\} \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land B \neq Bot \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land B \neq v) \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \lor (\land pc[\text{“S”}] = 8 \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land A \neq a \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land B = Bot)))
\end{array}
$$

$$
\begin{array}{lcl}
L2 & \triangleq & \lor (\land pc[\text{“W”}] = 2 \\
 & & \quad \land X = \text{TRUE} \\
 & & \quad \land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 3] \\
 & & \quad \land \text{UNCHANGED } \langle X, A, B, v, a, b, T\rangle) \\
 & & \lor (\land pc[\text{“W”}] = 2 \\
 & & \quad \land X = \text{FALSE} \\
 & & \quad \land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 4] \\
 & & \quad \land \text{UNCHANGED } \langle X, A, B, v, a, b, T\rangle)
\end{array}
$$

$$
\begin{array}{lcl}
Inv3A & \triangleq & pc[\text{“W”}] = 3 \Rightarrow A = v \\
Inv3B & \triangleq & pc[\text{“W”}] = 3 \Rightarrow (\exists\, t \in T : \ \land\, t.State = v \\
 & & \qquad\qquad\qquad\qquad\quad \land\, t.RetW = Ack) \\
Inv3C & \triangleq & pc[\text{“W”}] = 3 \Rightarrow (pc[\text{“S”}] \in \{9, 10\} \Rightarrow (\exists\, t \in T : \ \land\, t.State = v \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, t.RetW = Ack \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, t.RetS \ = v)) \\
Inv3D & \triangleq & pc[\text{“W”}] = 3 \Rightarrow (\exists\, t \in T : t.RetW = Bot \Rightarrow (\ \lor\, (\ \land\, pc[\text{“S”}] \in \{7, 8\} \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, B \neq Bot \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, B \neq v) \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \lor\, (\ \land\, pc[\text{“S”}] = 8 \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, A \neq a \\
 & & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, B = Bot)))
\end{array}
$$

$$
\begin{array}{lcl}
L3 & \triangleq & \land\, pc[\text{“W”}] = 3 \\
 & & \land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 4] \\
 & & \land\, B' = v \\
 & & \land\, T' = \{t \in T : t.RetW = Ack\} \\
 & & \land \text{ UNCHANGED } \langle X,\, A,\, v,\, a,\, b\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Inv4A & \triangleq & pc[\text{“W”}] = 4 \Rightarrow A = v \\
Inv4B & \triangleq & pc[\text{“W”}] = 4 \Rightarrow (\exists\, t \in T : \ \land\, t.State = A \\
 & & \qquad\qquad\qquad\qquad\quad \land\, t.RetW = Ack) \\
Inv4C & \triangleq & pc[\text{“W”}] = 4 \Rightarrow (\forall\, t \in T : \ \land\, t.State = A \\
 & & \qquad\qquad\qquad\qquad\quad \land\, t.RetW = Ack)
\end{array}
$$

$$
\begin{array}{lcl}
L4 & \triangleq & \land\, pc[\text{“W”}] = 4 \\
 & & \land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 1] \\
 & & \land\, v' \ \in Nat \\
 & & \land\, T' = \{[State \ \mapsto t.State, \\
 & & \qquad\quad RetW \ \mapsto Bot, \\
 & & \qquad\quad RetS \ \mapsto t.RetS] : t \in T\} \\
 & & \land \text{ UNCHANGED } \langle X,\, A,\, B,\, a,\, b\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Inv5A & \triangleq & pc[\text{“S”}] = 5 \Rightarrow X = \text{FALSE} \\
Inv5B & \triangleq & pc[\text{“S”}] = 5 \Rightarrow (\forall\, t \in T : t.RetS = Bot) \\
Inv5C & \triangleq & pc[\text{“S”}] = 5 \Rightarrow (\forall\, t \in T : \ \land\, t.State = A \\
 & & \qquad\qquad\qquad\qquad\quad \land\, (pc[\text{“W”}] \neq 1 \Rightarrow t.RetW = Ack))
\end{array}
$$

$$
\begin{array}{lcl}
L5 & \triangleq & \land\, pc[\text{“S”}] = 5 \\
 & & \land\, pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 6] \\
 & & \land\, X' = \text{TRUE} \\
 & & \land \text{ UNCHANGED } \langle A,\, B,\, v,\, a,\, b,\, T\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Inv6A & \triangleq & pc[\text{“S”}] = 6 \Rightarrow X = \text{TRUE} \\
Inv6B & \triangleq & pc[\text{“S”}] = 6 \Rightarrow (\forall\, t \in T : t.RetS = Bot)
\end{array}
$$

$$
L6 \quad \triangleq \quad \land\, pc[\text{“S”}] = 6
$$

$\land\ pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 7]$
$\land\ B' = Bot$
$\land$ UNCHANGED $\langle A,\ X,\ v,\ a,\ b,\ T\rangle$

$Inv7A \triangleq pc[\text{“S”}] = 7 \Rightarrow X = \text{TRUE}$
$Inv7B \triangleq pc[\text{“S”}] = 7 \Rightarrow (\forall\, t \in T : t.RetS = Bot)$
$Inv7C \triangleq pc[\text{“S”}] = 7 \Rightarrow (B \neq Bot \Rightarrow \exists\, t\ \in T : t.State = B)$
$Inv7D \triangleq pc[\text{“S”}] = 7 \Rightarrow (B = Bot \Rightarrow (\exists\, t \in T : t.State = A))$

$L7 \triangleq \land\ pc[\text{“S”}] = 7$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 8]$
$\land\ a' = A$
$\land$ UNCHANGED $\langle A,\ B,\ X,\ v,\ b,\ T\rangle$

$Inv8A \triangleq pc[\text{“S”}] = 8 \Rightarrow X = \text{TRUE}$
$Inv8B \triangleq pc[\text{“S”}] = 8 \Rightarrow (\forall\, t \in T : t.RetS = Bot)$
$Inv8C \triangleq pc[\text{“S”}] = 8 \Rightarrow (B \neq Bot \Rightarrow (\exists\, t \in T : t.State = B))$
$Inv8D \triangleq pc[\text{“S”}] = 8 \Rightarrow (B = Bot \Rightarrow (\exists\, t \in T : t.State = a))$

$L8 \triangleq \land\ pc[\text{“S”}] = 8$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 9]$
$\land\ X' = \text{FALSE}$
$\land\ T' = \{u \in [State\ : Nat,$
$RetW\ : \{Bot,\ Ack\},$
$RetS\ : Nat \cup \{Bot\}] : \exists\, t \in T : (\lor (\land\ t.RetW = Bot$
$\land\ pc[\text{“W”}] \neq 1$
$\land\ u.RetW = Ack$
$\land\ u.RetS\ = t.State$
$\land\ u.State = v)$
$\lor (\land\ t.RetW = Bot$
$\land\ pc[\text{“W”}] = 1$
$\land\ u.RetW = Bot$
$\land\ u.State = t.State$
$\land\ u.RetS\ = t.State)$
$\lor (\land\ t.RetW\ = Ack$
$\land\ u.RetW = Ack$
$\land\ u.State = t.State$
$\land\ u.RetS = t.State))\}$
$\land$ UNCHANGED $\langle A,\ B,\ v,\ a,\ b\rangle$

$Inv9A \triangleq pc[\text{“S”}] = 9 \Rightarrow X = \text{FALSE}$
$Inv9B \triangleq pc[\text{“S”}] = 9 \Rightarrow (\forall\, t \in T : t.RetS \neq Bot)$
$Inv9C \triangleq pc[\text{“S”}] = 9 \Rightarrow (B \neq Bot \Rightarrow (\exists\, t \in T : t.RetS = B))$
$Inv9D \triangleq pc[\text{“S”}] = 9 \Rightarrow (B = Bot \Rightarrow (\exists\, t \in T : t.RetS = a))$
$Inv9E \triangleq pc[\text{“S”}] = 9 \Rightarrow (\forall\, t \in T : \land\ t.State = A$
$\land\ (pc[\text{“W”}] \neq 1 \Rightarrow t.RetW = Ack))$

$$
\begin{array}{lcl}
L9 & \triangleq & \land\ pc[\text{“S”}] = 9 \\
 & & \land\ pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 10] \\
 & & \land\ b' = B \\
 & & \land \text{ UNCHANGED } \langle X,\ A,\ B,\ v,\ a,\ T\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Inv10A & \triangleq & pc[\text{“S”}] = 10 \Rightarrow X = \text{FALSE} \\
Inv10B & \triangleq & pc[\text{“S”}] = 10 \Rightarrow (\forall\, t \in T : t.RetS \neq Bot) \\
Inv10C & \triangleq & pc[\text{“S”}] = 10 \Rightarrow (b \neq Bot \Rightarrow (\exists\, t \in T : t.RetS = b)) \\
Inv10D & \triangleq & pc[\text{“S”}] = 10 \Rightarrow (b = Bot \Rightarrow (\exists\, t \in T : t.RetS = a)) \\
Inv10E & \triangleq & pc[\text{“S”}] = 10 \Rightarrow (\forall\, t \in T :\ \land\ t.State = A \\
 & & \qquad\qquad\qquad\qquad\qquad \land\ (pc[\text{“W”}] \neq 1 \Rightarrow t.RetW = Ack))
\end{array}
$$

$$
\begin{array}{lcl}
L10 & \triangleq & \land\ pc[\text{“S”}] = 10 \\
 & & \land\ pc' = [pc \text{ EXCEPT } ![\text{“S”}] = 5] \\
 & & \land\ T' = \{[State\ \mapsto t.State, \\
 & & \qquad\quad RetW\ \mapsto t.RetW, \\
 & & \qquad\quad RetS\ \mapsto Bot] : t \in \{t\_1 \in T : t\_1.RetS \neq Bot\}\} \\
 & & \qquad RetS \mapsto Bot] : t \in T\} \\
 & & \land \text{ UNCHANGED } \langle X,\ A,\ B,\ v,\ a,\ b\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Next & \triangleq & \lor\ L1 \\
 & & \lor\ L2 \\
 & & \lor\ L3 \\
 & & \lor\ L4 \\
 & & \lor\ L5 \\
 & & \lor\ L6 \\
 & & \lor\ L7 \\
 & & \lor\ L8 \\
 & & \lor\ L9 \\
 & & \lor\ L10
\end{array}
$$

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

$$
\begin{array}{lcl}
TypeOK & \triangleq & \land\ pc \in [ProcSet \to \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}] \\
 & & \land\ pc[\text{“W”}] \in \{1,\ 2,\ 3,\ 4\} \\
 & & \land\ pc[\text{“S”}]\ \in \{5,\ 6,\ 7,\ 8,\ 9,\ 10\} \\
 & & \land\ X\ \in \text{ BOOLEAN} \\
 & & \land\ A\ \in Nat \\
 & & \land\ B\ \in Nat \cup \{Bot\} \\
 & & \land\ a\ \in Nat \\
 & & \land\ b\ \in Nat \cup \{Bot\} \\
 & & \land\ v\ \in Nat \\
 & & \land\ T \in \text{ SUBSET } [State\ : Nat, \\
 & & \qquad\qquad\qquad\qquad RetW\ : \{Bot,\ Ack\}, \\
 & & \qquad\qquad\qquad\qquad RetS\ : Nat \cup \{Bot\}]
\end{array}
$$

$$Inv0A \triangleq \land \forall\, t1,\, t2,\, t3 \in T : \neg(\land\, t1 \neq t2 \land\, t1 \neq t3 \land\, t2 \neq t3)$$

$$Inv0B \triangleq \land \forall\, t \in T : t.RetW = Ack \Rightarrow t.State = A$$

$$\begin{array}{l} IInv \triangleq \land\ TypeOK \\ \quad \land\ Inv0A \\ \quad \land\ Inv0B \\ \quad \land\ Inv1A \\ \quad \land\ Inv1B \\ \quad \land\ Inv2A \\ \quad \land\ Inv2B \\ \quad \land\ Inv2C \\ \quad \land\ Inv2D \\ \quad \land\ Inv3A \\ \quad \land\ Inv3B \\ \quad \land\ Inv3C \\ \quad \land\ Inv3D \\ \quad \land\ Inv4A \\ \quad \land\ Inv4B \\ \quad \land\ Inv4C \\ \quad \land\ Inv5A \\ \quad \land\ Inv5B \\ \quad \land\ Inv5C \\ \quad \land\ Inv6A \\ \quad \land\ Inv6B \\ \quad \land\ Inv7A \\ \quad \land\ Inv7B \\ \quad \land\ Inv7C \\ \quad \land\ Inv7D \quad \text{NEW} \\ \quad \land\ Inv8A \\ \quad \land\ Inv8B \\ \quad \land\ Inv8C \\ \quad \land\ Inv8D \\ \quad \land\ Inv9A \\ \quad \land\ Inv9B \\ \quad \land\ Inv9C \\ \quad \land\ Inv9D \\ \quad \land\ Inv9E \\ \quad \land\ Inv10A \\ \quad \land\ Inv10B \\ \quad \land\ Inv10C \\ \quad \land\ Inv10D \\ \quad \land\ Inv10E \end{array}$$

$ISpec \triangleq \land IInv$
$\land \Box[Next]_{vars}$

THEOREM $TypeCorrectness \triangleq Spec \Rightarrow \Box TypeOK$
⟨1⟩ USE DEFS $ProcSet$, Bot, Ack, $TypeOK$
⟨1⟩1. $Init \Rightarrow TypeOK$
⟨2⟩ SUFFICES ASSUME $Init$
PROVE $TypeOK$
OBVIOUS
⟨2⟩1. $pc \in [ProcSet \to \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}]$
PROOF BY DEF $Init$
⟨2⟩2. $pc[\text{“W”}] \in \{1, 2, 3, 4\}$
PROOF BY DEF $Init$
⟨2⟩3. $pc[\text{“S”}] \in \{5, 6, 7, 8, 9, 10\}$
PROOF BY DEF $Init$
⟨2⟩4. $X \in$ BOOLEAN
PROOF BY DEF $Init$
⟨2⟩5. $A \in Nat$
PROOF BY DEF $Init$
⟨2⟩6. $B \in Nat \cup \{Bot\}$
PROOF BY DEF $Init$
⟨2⟩7. $a \in Nat$
PROOF BY DEF $Init$
⟨2⟩8. $b \in Nat \cup \{Bot\}$
PROOF BY DEF $Init$
⟨2⟩9. $v \in Nat$
PROOF BY DEF $Init$
⟨2⟩10. $T \in$ SUBSET $[State : Nat,$
$RetW : \{Bot, Ack\},$
$RetS : Nat \cup \{Bot\}]$
PROOF BY DEF $Init$
⟨2⟩11. QED
BY ⟨2⟩1, ⟨2⟩10, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5, ⟨2⟩6, ⟨2⟩7, ⟨2⟩8, ⟨2⟩9 DEF $TypeOK$
⟨1⟩2. $TypeOK \land [Next]_{vars} \Rightarrow TypeOK'$
⟨2⟩1. QED
⟨3⟩ SUFFICES ASSUME $TypeOK$, $[Next]_{vars}$
PROVE $TypeOK'$
OBVIOUS
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $Next$, $vars$, $L1$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $Next$, $vars$, $L2$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $Next$, $vars$, $L3$

⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $Next$, $vars$, $L4$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $Next$, $vars$, $L5$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $Next$, $vars$, $L6$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $Next$, $vars$, $L7$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $Next$, $vars$, $L8$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $Next$, $vars$, $L9$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $Next$, $vars$, $L10$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $Next$, $vars$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$
⟨1⟩3. QED
BY ⟨1⟩1, ⟨1⟩2, PTL DEF $Spec$

THEOREM $Spec \Rightarrow \Box IInv$
⟨1⟩ USE DEFS $ProcSet$, Bot, Ack, $TypeOK$
⟨1⟩1. $Init \Rightarrow IInv$
⟨2⟩ SUFFICES ASSUME $Init$
PROVE $IInv$
OBVIOUS
⟨2⟩1. $TypeOK$
BY Isa DEF $Init$
⟨2⟩2. $Inv0A$
BY DEF $Init$, $Inv0A$
⟨2⟩3. $Inv0B$
BY DEF $Init$, $Inv0B$
⟨2⟩4. $Inv1A$
BY DEF $Init$, $Inv1A$
⟨2⟩5. $Inv1B$
BY DEF $Init$, $Inv1B$
⟨2⟩6. $Inv2A$
BY DEF $Init$, $Inv2A$
⟨2⟩7. $Inv2B$
BY DEF $Init$, $Inv2B$
⟨2⟩8. $Inv2C$
BY DEF $Init$, $Inv2C$
⟨2⟩9. $Inv2D$
BY DEF $Init$, $Inv2D$

⟨2⟩10. $Inv3A$
BY DEF $Init$, $Inv3A$
⟨2⟩11. $Inv3B$
BY DEF $Init$, $Inv3B$
⟨2⟩12. $Inv3C$
BY DEF $Init$, $Inv3C$
⟨2⟩13. $Inv3D$
BY DEF $Init$, $Inv3D$
⟨2⟩14. $Inv4A$
BY DEF $Init$, $Inv4A$
⟨2⟩15. $Inv4B$
BY DEF $Init$, $Inv4B$
⟨2⟩16. $Inv4C$
BY DEF $Init$, $Inv4C$
⟨2⟩17. $Inv5A$
BY DEF $Init$, $Inv5A$
⟨2⟩18. $Inv5B$
BY DEF $Init$, $Inv5B$
⟨2⟩19. $Inv5C$
BY DEF $Init$, $Inv5C$
⟨2⟩20. $Inv6A$
BY DEF $Init$, $Inv6A$
⟨2⟩21. $Inv6B$
BY DEF $Init$, $Inv6B$
⟨2⟩22. $Inv7A$
BY DEF $Init$, $Inv7A$
⟨2⟩23. $Inv7B$
BY DEF $Init$, $Inv7B$
⟨2⟩24. $Inv7C$
BY DEF $Init$, $Inv7C$
⟨2⟩25. $Inv8A$
BY DEF $Init$, $Inv8A$
⟨2⟩26. $Inv8B$
BY DEF $Init$, $Inv8B$
⟨2⟩27. $Inv8C$
BY DEF $Init$, $Inv8C$
⟨2⟩28. $Inv8D$
BY DEF $Init$, $Inv8D$
⟨2⟩29. $Inv9A$
BY DEF $Init$, $Inv9A$
⟨2⟩30. $Inv9B$
BY DEF $Init$, $Inv9B$
⟨2⟩31. $Inv9C$
BY DEF $Init$, $Inv9C$
⟨2⟩32. $Inv9D$

BY DEF $Init$, $Inv9D$
⟨2⟩33. $Inv9E$
BY DEF $Init$, $Inv9E$
⟨2⟩34. $Inv10A$
BY DEF $Init$, $Inv10A$
⟨2⟩35. $Inv10B$
BY DEF $Init$, $Inv10B$
⟨2⟩36. $Inv10C$
BY DEF $Init$, $Inv10C$
⟨2⟩37. $Inv10D$
BY DEF $Init$, $Inv10D$
⟨2⟩38. $Inv10E$
BY DEF $Init$, $Inv10E$
⟨2⟩39. QED
BY ⟨2⟩1, ⟨2⟩10, ⟨2⟩11, ⟨2⟩12, ⟨2⟩13, ⟨2⟩14, ⟨2⟩15, ⟨2⟩16, ⟨2⟩17, ⟨2⟩18, ⟨2⟩19, ⟨2⟩2, ⟨2⟩20, ⟨2⟩21, ⟨2⟩22, ⟨2⟩23,
⟨1⟩2. $IInv \wedge [Next]_{vars} \Rightarrow IInv'$
⟨2⟩ SUFFICES ASSUME $IInv \wedge [Next]_{vars}$
PROVE $IInv'$
OBVIOUS
⟨2⟩ USE DEF $IInv$, $Next$, $vars$, $L1$, $L2$, $L3$, $L4$, $L5$, $L6$, $L7$, $L8$, $L9$, $L10$
⟨2⟩1. $TypeOK'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩2. $Inv0A'$
OMITTED
⟨2⟩3. $Inv0B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv0B$, $Inv1B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv0B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv0B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv0B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv0B$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv0B$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv0B$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv0B$, $Inv2A$, $Inv3A$, $Inv4A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv0B$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv0B$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv0B$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩4. $Inv1A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv1A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv1A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv1A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4, Isa DEF $TypeOK$, $Inv1A$, $Inv4A$, $Inv4B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv1A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv1A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv1A$
⟨3⟩8.CASE $L8$
⟨4⟩ USE DEF $L8$

⟨4⟩ SUFFICES ASSUME $pc[\text{“W”}] = 1$
PROVE $\exists\, t \in T' : \wedge\, t.State = A'$
$\wedge\, t.RetW = Bot$
BY ⟨3⟩8 DEF $L8$, $Inv1A$
⟨4⟩1. PICK $t \in T : \wedge\, t.State = A$
$\wedge\, t.RetW = Bot$
BY DEF $Inv1A$
⟨4⟩2. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Bot,$
$RetS \mapsto t.State]$
⟨4⟩3. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1
⟨4⟩4. QED
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩3

⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv1A$
⟨3⟩10.CASE $L10$
⟨4⟩ SUFFICES ASSUME $(pc[\text{“W”}] = 1)'$
PROVE $(\exists\, t \in T : \wedge\, t.State = A$
$\wedge\, t.RetW = Bot)'$
BY DEF $Inv1A$
⟨4⟩1. PICK $t \in T : \wedge\, t.State = A$
$\wedge\, t.RetW = Bot$
BY ⟨3⟩10 DEF $L10$, $Inv1A$
⟨4⟩2. $t.RetS \neq Bot$
BY ⟨3⟩10 DEF $L10$, $Inv10B$
⟨4⟩ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$
⟨4⟩3. $u \in T'$
BY ⟨3⟩10, ⟨4⟩1, ⟨4⟩2 DEF $L10$
⟨4⟩4. QED
BY ⟨4⟩1, ⟨4⟩3
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv1A$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩5. $Inv1B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv1B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv1B$
⟨3⟩3.CASE $L3$

PROOF BY ⟨3⟩3 DEF *TypeOK*, *Inv*1*B*
⟨3⟩4.CASE *L*4
PROOF BY ⟨3⟩4 DEF *TypeOK*, *Inv*1*B*, *Inv*4*A*, *Inv*4*B*, *Inv*4*C*
⟨3⟩5.CASE *L*5
PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*1*B*
⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*1*B*
⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*1*B*
⟨3⟩8.CASE *L*8
PROOF BY ⟨3⟩8 DEF *TypeOK*, *Inv*1*B*
⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*1*B*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*1*B*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*1*B*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩6. *Inv*2*A*′
⟨3⟩1.CASE *L*1
PROOF BY ⟨3⟩1 DEF *TypeOK*, *Inv*2*A*
⟨3⟩2.CASE *L*2
PROOF BY ⟨3⟩2 DEF *TypeOK*, *Inv*2*A*
⟨3⟩3.CASE *L*3
PROOF BY ⟨3⟩3 DEF *TypeOK*, *Inv*2*A*
⟨3⟩4.CASE *L*4
PROOF BY ⟨3⟩4 DEF *TypeOK*, *Inv*2*A*
⟨3⟩5.CASE *L*5
PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*2*A*
⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*2*A*
⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*2*A*
⟨3⟩8.CASE *L*8
PROOF BY ⟨3⟩8 DEF *TypeOK*, *Inv*2*A*
⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*2*A*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*2*A*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*2*A*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩7. $Inv2B'$
⟨3⟩1.CASE $L1$
⟨4⟩1.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
PROOF BY ⟨4⟩1, ⟨3⟩1, *Isa* DEF $TypeOK$, $Inv1A$, $Inv1B$, $Inv2B$
⟨4⟩2.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \land\ X = \text{TRUE}$
$\land\ pc[\text{“S”}] \neq 6$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 7$
$\lor\ B \neq Bot)$
$\land\ B \neq v$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 8$
$\lor\ B \neq Bot$
$\lor\ a\ \neq v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
PROOF BY ⟨4⟩2, ⟨3⟩1, $IsaT(60)$ DEF $TypeOK$, $Inv1A$, $Inv1B$, $Inv2B$
⟨4⟩3. QED
BY ⟨3⟩1, ⟨4⟩1, ⟨4⟩2 DEF $L1$

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv2B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv2B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv2B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv2B$

⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv2B$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv2B$
⟨3⟩8.CASE $L8$
⟨4⟩ SUFFICES ASSUME $pc[\text{"W"}] = 2$
PROVE $\exists\, t \in T' : \wedge\, t.State = v'$
$\wedge\, t.RetW = Ack$
BY ⟨3⟩8 DEF $L8$, $Inv2B$
⟨4⟩1. PICK $t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack$
BY DEF $Inv2B$
⟨4⟩2. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$
⟨4⟩3. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1
⟨4⟩4. QED
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩3
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv2B$
⟨3⟩10.CASE $L10$
⟨4⟩ SUFFICES ASSUME $(pc[\text{"W"}] = 2)'$
PROVE $(\exists\, t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack)'$
BY DEF $Inv2B$
⟨4⟩1. PICK $t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack$
BY ⟨3⟩10 DEF $L10$, $Inv2B$
⟨4⟩2. $t.RetS \neq Bot$
BY ⟨3⟩10 DEF $L10$, $Inv10B$
⟨4⟩ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$
⟨4⟩3. $u \in T'$
BY ⟨3⟩10, ⟨4⟩1, ⟨4⟩2 DEF $L10$
⟨4⟩4. QED
BY ⟨4⟩1, ⟨4⟩3

⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv2B$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩8. $Inv2C'$

⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv2C$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv2C$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv2C$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv2C$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv2C$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv2C$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv2C$
⟨3⟩8.CASE $L8$
⟨4⟩ SUFFICES ASSUME $pc'[\text{“W”}] = 2$,
$X' = \text{FALSE}$,
NEW $t\_pr \in T'$
PROVE $(\land t\_pr.State = v$
$\land t\_pr.RetW = Ack)'$
BY DEF $Inv2C$
⟨4⟩1. $t\_pr.State = v'$
PROOF BY ⟨3⟩8 DEF $Inv2A$, $Inv0B$
⟨4⟩2. $t\_pr.RetW = Ack$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv2C$
⟨4⟩3. QED
BY ⟨4⟩1, ⟨4⟩2
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv2C$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv2C$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv2C$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩9. $Inv2D'$
⟨3⟩1.CASE $L1$
⟨4⟩1.CASE $\land pc[\text{“W”}] = 1$
$\land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land A' = v$
$\land (\lor X = \text{FALSE}$
$\lor pc[\text{“S”}] = 6$
$\lor (\land pc[\text{“S”}] = 7$
$\land B = Bot)$

$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$

$\langle 5\rangle 1$. PICK $t \in T$: TRUE
BY $\langle 3\rangle 1$ DEF $Inv1A$

$\langle 5\rangle$ DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS]$

$\langle 5\rangle 2$. $u \in T'$
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 5\rangle 1$

$\langle 5\rangle 3$. QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF $Inv2D$

$\langle 4\rangle 2$.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \land\ X = $ TRUE
$\land\ pc[\text{“S”}] \neq 6$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 7$
$\lor\ B \neq Bot)$
$\land\ B \neq v$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 8$
$\lor\ B \neq Bot$
$\lor\ a\ \neq v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$

$\langle 5\rangle 1$. PICK $t \in T$: TRUE
BY $\langle 3\rangle 1$ DEF $Inv1A$

$\langle 5\rangle$ DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS]$

$\langle 5\rangle 2$. $u \in T'$
BY $\langle 3\rangle 1$, $\langle 4\rangle 2$, $\langle 5\rangle 1$

$\langle 5\rangle 3$. QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF $Inv2D$

$\langle 4\rangle 3$. QED
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2$.CASE $L2$

PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 4$.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 8$.CASE $L8$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 2$
PROVE $(\exists\, t \in T : t.RetW = Bot \Rightarrow (\ \vee\ (\ \wedge\ pc[\text{“S”}] \in \{7, 8\}$
$\wedge\ B \neq Bot$
$\wedge\ B \neq v)$
$\vee\ (\ \wedge\ pc[\text{“S”}] = 8$
$\wedge\ A \neq a$
$\wedge\ B = Bot)))'$

BY $\langle 3\rangle 8$ DEF $Inv2D$, $L8$

$\langle 4\rangle 1$. PICK $t \in T : \wedge\ t.State = v$
$\wedge\ t.RetW = Ack$

BY DEF $Inv2B$

$\langle 4\rangle 2$. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$

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

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$

$\langle 4\rangle 4$. QED

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$, $\langle 4\rangle 3$ DEF $Inv2D$

$\langle 3\rangle 9$.CASE $L9$

PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv2D$

$\langle 3\rangle 10$.CASE $L10$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 2$
PROVE $(\exists\, t \in T : t.RetW = Bot \Rightarrow (\ \vee\ (\ \wedge\ pc[\text{“S”}] \in \{7, 8\}$
$\wedge\ B \neq Bot$
$\wedge\ B \neq v)$
$\vee\ (\ \wedge\ pc[\text{“S”}] = 8$
$\wedge\ A \neq a$
$\wedge\ B = Bot)))'$

BY $\langle 3\rangle 10$ DEF $Inv2D$, $L10$

$\langle 4\rangle 1$. PICK $t \in T : \wedge\ t.RetW = Ack$
$\wedge\ t.RetS \neq Bot$

BY $\langle 3\rangle 10$ DEF $Inv2B$, $Inv10B$, $Inv10E$, $L10$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$

$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$

⟨4⟩2. $u \in T'$
BY ⟨3⟩10, ⟨4⟩1 DEF $L10$

⟨4⟩3. QED
BY ⟨4⟩1, ⟨4⟩2

⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv2D$

⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩10. $Inv3A'$

⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv3A$

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv3A$, $Inv2A$

⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv3A$

⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv3A$

⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv3A$

⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv3A$

⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv3A$

⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv3A$

⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv3A$

⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv3A$

⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv3A$

⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩11. $Inv3B'$

⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv3B$

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv3B$, $Inv2B$

⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv3B$

⟨3⟩4.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 8$.CASE $L8$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 3$
PROVE $\exists\, t \in T' : \wedge\, t.State = v'$
$\wedge\, t.RetW = Ack$

BY $\langle 3\rangle 8$ DEF $L8$, $Inv3B$

$\langle 4\rangle 1$. PICK $t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack$

BY DEF $Inv3B$

$\langle 4\rangle 2$. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$

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

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$

$\langle 4\rangle 4$. QED

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

$\langle 3\rangle 9$.CASE $L9$

PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 10$.CASE $L10$

$\langle 4\rangle$ SUFFICES ASSUME $(pc[\text{“W”}] = 3)'$
PROVE $(\exists\, t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack)'$

BY DEF $Inv3B$

$\langle 4\rangle 1$. PICK $t \in T : \wedge\, t.State = v$
$\wedge\, t.RetW = Ack$

BY $\langle 3\rangle 10$ DEF $L10$, $Inv3B$

$\langle 4\rangle 2$. $t.RetS \neq Bot$

BY $\langle 3\rangle 10$ DEF $L10$, $Inv10B$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$

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

BY $\langle 3\rangle 10$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L10$

$\langle 4\rangle 4$. QED

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

$\langle 3\rangle 11$.CASE UNCHANGED $vars$

PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv3B$

$\langle 3\rangle 12$. QED

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

$\langle 2\rangle 12$. $Inv3C'$
$\langle 3\rangle 1$.CASE $L1$
PROOF BY $\langle 3\rangle 1$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 2$.CASE $L2$
PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv3C$, $Inv9A$, $Inv10A$
$\langle 3\rangle 3$.CASE $L3$
PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 4$.CASE $L4$
PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 5$.CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 6$.CASE $L6$
PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 7$.CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 8$.CASE $L8$
$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 3$,
$pc'[\text{“S”}] \in \{9, 10\}$
PROVE $\exists\, t \in T' : \land\, t.State = v'$
$\land\, t.RetW = Ack$
$\land\, t.RetS \;= v'$
BY $\langle 3\rangle 8$ DEF $Inv3C$
$\langle 4\rangle 1$. PICK $t \in T : \land\, t.State = v$
$\land\, t.RetW = Ack$
BY DEF $Inv3B$
$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$
$\langle 4\rangle 2$. $u \in T'$
BY $\langle 3\rangle 8$, $\langle 4\rangle 1$
$\langle 4\rangle 3$. QED
BY $\langle 3\rangle 8$, $\langle 4\rangle 1$, $\langle 4\rangle 2$
$\langle 3\rangle 9$.CASE $L9$
PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 10$.CASE $L10$
PROOF BY $\langle 3\rangle 10$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 11$.CASE UNCHANGED *vars*
PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv3C$
$\langle 3\rangle 12$. QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 10$, $\langle 3\rangle 11$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$, $\langle 3\rangle 8$, $\langle 3\rangle 9$ DEF *Next*

$\langle 2\rangle 13$. $Inv3D'$
$\langle 3\rangle 1$.CASE $L1$

PROOF BY $\langle 3\rangle 1$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 2$.CASE $L2$

$\langle 4\rangle 1$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{TRUE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 3]$
$\land$ UNCHANGED $\langle X,\ A,\ B,\ v,\ a,\ b,\ T\rangle$

PROOF BY $\langle 4\rangle 1$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv3D$, $Inv2D$

$\langle 4\rangle 2$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{FALSE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 4]$
$\land$ UNCHANGED $\langle X,\ A,\ B,\ v,\ a,\ b,\ T\rangle$

PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv3D$

$\langle 4\rangle 3$. QED

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

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 4$.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 8$.CASE $L8$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 3$
PROVE $(\exists\, t \in T : t.RetW = Bot \Rightarrow (\ \lor (\ \land pc[\text{“S”}] \in \{7, 8\}$
$\land\, B \neq Bot$
$\land\, B \neq v)$
$\lor (\ \land pc[\text{“S”}] = 8$
$\land\, A \neq a$
$\land\, B = Bot)))'$

BY $\langle 3\rangle 8$ DEF $Inv3D$, $L8$

$\langle 4\rangle 1$. PICK $t \in T : \land\, t.State = v$
$\land\, t.RetW = Ack$

BY DEF $Inv3B$

$\langle 4\rangle 2$. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$

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

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$

$\langle 4\rangle 4$. QED

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$, $\langle 4\rangle 3$

$\langle 3\rangle 9$.CASE $L9$

PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 10$.CASE $L10$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 3$
PROVE $(\exists\, t \in T : t.RetW = Bot \Rightarrow (\ \vee (\ \wedge pc[\text{“S”}] \in \{7, 8\}$
$\wedge\ B \neq Bot$
$\wedge\ B \neq v)$
$\vee (\ \wedge pc[\text{“S”}] = 8$
$\wedge\ A \neq a$
$\wedge\ B = Bot)))'$

BY $\langle 3\rangle 10$ DEF $Inv3D$, $L10$

$\langle 4\rangle 1$. PICK $t \in T : \wedge\, t.RetW = Ack$
$\wedge\, t.RetS \neq Bot$

BY $\langle 3\rangle 10$ DEF $Inv3B$, $Inv10B$, $Inv10E$, $L10$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$

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

BY $\langle 3\rangle 10$, $\langle 4\rangle 1$ DEF $L10$

$\langle 4\rangle 3$. QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle 11$.CASE UNCHANGED $vars$

PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv3D$

$\langle 3\rangle 12$. QED

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

$\langle 2\rangle 14$. $Inv4A'$

$\langle 3\rangle 1$.CASE $L1$

PROOF BY $\langle 3\rangle 1$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 2$.CASE $L2$

PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv4A$, $Inv2A$

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv4A$, $Inv3A$

$\langle 3\rangle 4$.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 8$.CASE $L8$

PROOF BY $\langle 3\rangle 8$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 9$.CASE $L9$

PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 10$.CASE $L10$

PROOF BY $\langle 3\rangle 10$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 11$.CASE UNCHANGED $vars$

PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv4A$

$\langle 3\rangle 12$. QED

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

$\langle 2\rangle 15$. $Inv4B'$

$\langle 3\rangle 1$.CASE $L1$

PROOF BY $\langle 3\rangle 1$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 2$.CASE $L2$

$\langle 4\rangle 1$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{TRUE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 3]$
$\land$ UNCHANGED $\langle X,\, A,\, B,\, v,\, a,\, b,\, T\rangle$

PROOF BY $\langle 4\rangle 1$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv4B$

$\langle 4\rangle 2$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{FALSE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 4]$
$\land$ UNCHANGED $\langle X,\, A,\, B,\, v,\, a,\, b,\, T\rangle$

PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv4B$, $Inv2B$, $Inv2A$

$\langle 4\rangle 3$. QED

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

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv4B$, $Inv3B$, $Inv3A$

$\langle 3\rangle 4$.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 8$.CASE $L8$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“W”}] = 4$
PROVE $\exists\, t \in T' : \land\, t.State = A'$
$\land\, t.RetW = Ack$

BY $\langle 3\rangle 8$ DEF $Inv4B$

$\langle 4\rangle 1$. PICK $t \in T : \land\, t.State = A$
$\land\, t.RetW = Ack$

BY $\langle 3\rangle 8$ DEF $Inv4B$

$\langle 4\rangle 2$. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$

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

BY $\langle 3\rangle 8$, $\langle 4\rangle 1$

$\langle 4\rangle 4$. QED

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

$\langle 3\rangle 9$.CASE $L9$

PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 10$.CASE $L10$

$\langle 4\rangle$ SUFFICES ASSUME $(pc[\text{“W”}] = 4)'$
PROVE $(\exists\, t \in T : \land\, t.State = A$
$\land\, t.RetW = Ack)'$

BY DEF $Inv4B$

$\langle 4\rangle 1$. PICK $t \in T : \land\, t.State = A$
$\land\, t.RetW = Ack$

BY $\langle 3\rangle 10$ DEF $L10$, $Inv4B$

$\langle 4\rangle 2$. $t.RetS \neq Bot$

BY $\langle 3\rangle 10$ DEF $L10$, $Inv10B$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto t.RetW,$
$RetS \mapsto Bot]$

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

BY $\langle 3\rangle 10$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L10$

$\langle 4\rangle 4$. QED

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

$\langle 3\rangle 11$.CASE UNCHANGED $vars$

PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv4B$

$\langle 3\rangle 12$. QED

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

$\langle 2\rangle 16$. $Inv4C'$

$\langle 3\rangle 1$.CASE $L1$

PROOF BY $\langle 3\rangle 1$ DEF $TypeOK$, $Inv4C$

$\langle 3\rangle 2$.CASE $L2$

$\langle 4\rangle 1$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{TRUE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 3]$
$\land$ UNCHANGED $\langle X,\, A,\, B,\, v,\, a,\, b,\, T\rangle$

PROOF BY $\langle 4\rangle 1$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv4C$

$\langle 4\rangle 2$.CASE $\land\, pc[\text{“W”}] = 2$
$\land\, X = \text{FALSE}$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 4]$
$\land$ UNCHANGED $\langle X,\, A,\, B,\, v,\, a,\, b,\, T\rangle$

PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 2$ DEF $TypeOK$, $Inv4C$, $Inv2C$, $Inv2A$

$\langle 4\rangle 3$. QED

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

⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv4C$, $Inv0B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv4C$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv4C$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv4C$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv4C$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv4C$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv4C$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv4C$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv4C$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩17. $Inv5A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv5A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv5A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv5A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv5A$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv5A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv5A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv5A$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv5A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv5A$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv5A$, $Inv10A$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv5A$
⟨3⟩12. QED

BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩18. $Inv5B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv5B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv5B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv5B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv5B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv5B$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv5B$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv5B$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv5B$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv5B$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv5B$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv5B$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩19. $Inv5C'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv5A$, $Inv5C$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv5C$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv5C$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv5C$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv5C$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv5C$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv5C$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv5C$

⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv5C$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv5C$, $Inv10E$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv5C$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩20. $Inv6A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv6A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv6A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv6A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv6A$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv6A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv6A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv6A$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv6A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv6A$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv6A$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv6A$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩21. $Inv6B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv6B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv6B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv6B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv6B$
⟨3⟩5.CASE $L5$

PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*6*B*, *Inv*5*B*
⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*6*B*
⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*6*B*
⟨3⟩8.CASE *L*8
PROOF BY ⟨3⟩8 DEF *TypeOK*, *Inv*6*B*
⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*6*B*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*6*B*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*6*B*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩22. *Inv*7*A*′
⟨3⟩1.CASE *L*1
PROOF BY ⟨3⟩1 DEF *TypeOK*, *Inv*7*A*
⟨3⟩2.CASE *L*2
PROOF BY ⟨3⟩2 DEF *TypeOK*, *Inv*7*A*
⟨3⟩3.CASE *L*3
PROOF BY ⟨3⟩3 DEF *TypeOK*, *Inv*7*A*
⟨3⟩4.CASE *L*4
PROOF BY ⟨3⟩4 DEF *TypeOK*, *Inv*7*A*
⟨3⟩5.CASE *L*5
PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*7*A*
⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*7*A*, *Inv*6*A*
⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*7*A*
⟨3⟩8.CASE *L*8
PROOF BY ⟨3⟩8 DEF *TypeOK*, *Inv*7*A*
⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*7*A*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*7*A*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*7*A*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩23. *Inv*7*B*′
⟨3⟩1.CASE *L*1
PROOF BY ⟨3⟩1 DEF *TypeOK*, *Inv*7*B*

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv7B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv7B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv7B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv7B$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv7B$, $Inv6B$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv7B$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv7B$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv7B$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv7B$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv7B$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩24. $Inv7C'$
⟨3⟩1.CASE $L1$
⟨4⟩1.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
⟨5⟩ SUFFICES ASSUME $pc[\text{“S”}] = 7,$
$B \neq Bot$
PROVE $\exists\, t \in T' : t.State = B$
BY ⟨4⟩1 DEF $Inv7C$
⟨5⟩1. $B = v$

BY $\langle 4\rangle 1$ DEF $Inv7A$

$\langle 5\rangle 2$. PICK $t \in T$: TRUE

BY $\langle 4\rangle 1$ DEF $Inv1A$

$\langle 5\rangle$ DEFINE $u \triangleq [State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS]$

$\langle 5\rangle 3$. $u \in T'$

BY $\langle 4\rangle 1, \langle 5\rangle 2$

$\langle 5\rangle 4$. QED

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

$\langle 4\rangle 2$.CASE $\land pc[\text{“W”}] = 1$
$\land pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\land A' = v$
$\land (\land X = \text{TRUE}$
$\land pc[\text{“S”}] \neq 6$
$\land (\lor pc[\text{“S”}] \neq 7$
$\lor B \neq Bot)$
$\land B \neq v$
$\land (\lor pc[\text{“S”}] \neq 8$
$\lor B \neq Bot$
$\lor a \neq v))$
$\land T' = \{[State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X, B, v, a, b\rangle$

PROOF BY $\langle 4\rangle 2, \langle 3\rangle 1$ DEF $TypeOK, Inv7C$

$\langle 4\rangle 3$. QED

BY $\langle 3\rangle 1, \langle 4\rangle 1, \langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2$.CASE $L2$

PROOF BY $\langle 3\rangle 2$ DEF $TypeOK, Inv7C$

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK, Inv7C, Inv3B$

$\langle 3\rangle 4$.CASE $L4$

$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 7,$
$B \neq Bot$
PROVE $\exists\, t \in T' : t.State = B$

BY $\langle 3\rangle 4$ DEF $Inv7C$

$\langle 4\rangle 1$. PICK $t \in T : t.State = B$

BY $\langle 3\rangle 4$ DEF $Inv7C$

$\langle 4\rangle$ DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Bot,$
$RetS \mapsto t.RetS]$

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

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

$\langle 3\rangle 5$.CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 6$.CASE $L6$
PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 7$.CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 8$.CASE $L8$
PROOF BY $\langle 3\rangle 8$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 9$.CASE $L9$
PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 10$.CASE $L10$
PROOF BY $\langle 3\rangle 10$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 11$.CASE UNCHANGED $vars$
PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv7C$
$\langle 3\rangle 12$. QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 10$, $\langle 3\rangle 11$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$, $\langle 3\rangle 8$, $\langle 3\rangle 9$ DEF $Next$

$\langle 2\rangle 2$. $Inv7D'$
$\langle 3\rangle 1$.CASE $L1$
$\langle 4\rangle 1$.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
$\langle 5\rangle$ SUFFICES ASSUME $pc'[\text{“S”}] = 7$,
$B' = Bot$
PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 4\rangle 1$ DEF $Inv7D$
$\langle 5\rangle 1$. PICK $t \in T$: TRUE
BY $\langle 4\rangle 1$ DEF $Inv1A$
$\langle 5\rangle$ DEFINE $u \triangleq [State\ \mapsto v,$

$RetW \ \mapsto Ack,$
$RetS \ \mapsto t.RetS]$

$\langle 5\rangle 2. \wedge u \in T'$
$\wedge u.State = A'$
BY $\langle 4\rangle 1$, $\langle 5\rangle 1$

PROOF BY $\langle 4\rangle 1$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv7D$, $Inv1A$, $Inv0B$

$\langle 5\rangle 3.$ QED
BY $\langle 5\rangle 2$

$\langle 4\rangle 2.$CASE $\wedge pc[\text{“W”}] = 1$
$\wedge pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\wedge A' = v$
$\wedge (\wedge X = \text{TRUE}$
$\wedge pc[\text{“S”}] \neq 6$
$\wedge (\vee pc[\text{“S”}] \neq 7$
$\vee B \neq Bot)$
$\wedge B \neq v$
$\wedge (\vee pc[\text{“S”}] \neq 8$
$\vee B \neq Bot$
$\vee a \neq v))$
$\wedge T' = \{[State \ \mapsto v,$
$RetW \ \mapsto Ack,$
$RetS \ \mapsto t.RetS] : t \in T\} \cup T$
$\wedge$ UNCHANGED $\langle X, B, v, a, b\rangle$
PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv7D$

$\langle 4\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2.$CASE $L2$
PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv7D$

$\langle 3\rangle 3.$CASE $L3$
PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv7D$

$\langle 3\rangle 4.$CASE $L4$
$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 7,$
$B = Bot$
PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 3\rangle 4$ DEF $Inv7D$

$\langle 4\rangle 1.$ PICK $t \in T : t.State = A$
BY $\langle 3\rangle 4$ DEF $Inv7D$

$\langle 4\rangle$ DEFINE $u \triangleq [State \ \mapsto t.State,$
$RetW \ \mapsto Bot,$
$RetS \ \mapsto t.RetS]$

$\langle 4\rangle 2. \wedge u \in T'$
$\wedge u.State = A'$
BY $\langle 3\rangle 4$, $\langle 4\rangle 1$

$\langle 4\rangle$ QED

PROOF BY $\langle 3\rangle 4$, $\langle 4\rangle 2$ DEF $TypeOK$, $Inv7D$

$\langle 3\rangle 5$.CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv7D$
$\langle 3\rangle 6$.CASE $L6$
$\langle 4\rangle 1$.CASE $pc[\text{“W”}] = 1$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 6$, $B' = Bot$ PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 3\rangle 6$, $\langle 4\rangle 1$ DEF $Inv7D$
$\langle 5\rangle 1$. PICK $t \in T : t.State = A$
BY $\langle 4\rangle 1$ DEF $Inv1A$
$\langle 5\rangle$ QED
BY $\langle 3\rangle 6$, $\langle 4\rangle 1$, $\langle 5\rangle 1$
$\langle 4\rangle 2$.CASE $pc[\text{“W”}] = 2$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 6$, $B' = Bot$ PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 3\rangle 6$, $\langle 4\rangle 2$ DEF $Inv7D$
$\langle 5\rangle 1$. PICK $t \in T : t.State = A$
BY $\langle 4\rangle 2$ DEF $Inv2A$, $Inv2B$
$\langle 5\rangle$ QED
BY $\langle 3\rangle 6$, $\langle 4\rangle 2$, $\langle 5\rangle 1$
$\langle 4\rangle 3$.CASE $pc[\text{“W”}] = 3$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 6$, $B' = Bot$ PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 3\rangle 6$, $\langle 4\rangle 3$ DEF $Inv7D$
$\langle 5\rangle 1$. PICK $t \in T : t.State = A$
BY $\langle 4\rangle 3$ DEF $Inv3A$, $Inv3B$
$\langle 5\rangle$ QED
BY $\langle 3\rangle 6$, $\langle 4\rangle 3$, $\langle 5\rangle 1$
$\langle 4\rangle 4$.CASE $pc[\text{“W”}] = 4$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 6$, $B' = Bot$ PROVE $\exists\, t\_pr \in T' : t\_pr.State = A'$
BY $\langle 3\rangle 6$, $\langle 4\rangle 4$ DEF $Inv7D$
$\langle 5\rangle 1$. PICK $t \in T : t.State = A$
BY $\langle 4\rangle 4$ DEF $Inv4A$, $Inv4B$
$\langle 5\rangle$ QED
BY $\langle 3\rangle 6$, $\langle 4\rangle 3$, $\langle 5\rangle 1$
$\langle 4\rangle 5$. QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$ DEF $TypeOK$
$\langle 3\rangle 7$.CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv7D$

⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv7D$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv7D$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv7D$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv7D$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩25. $Inv8A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv8A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv8A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv8A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv8A$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv8A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv8A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv8A$, $Inv7A$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv8A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv8A$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv8A$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv8A$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩26. $Inv8B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv8B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv8B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv8B$
⟨3⟩4.CASE $L4$

PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 5$.CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 6$.CASE $L6$
PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 7$.CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv8B$, $Inv7B$
$\langle 3\rangle 8$.CASE $L8$
PROOF BY $\langle 3\rangle 8$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 9$.CASE $L9$
PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 10$.CASE $L10$
PROOF BY $\langle 3\rangle 10$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 11$.CASE UNCHANGED $vars$
PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv8B$
$\langle 3\rangle 12$. QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 10$, $\langle 3\rangle 11$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$, $\langle 3\rangle 8$, $\langle 3\rangle 9$ DEF $Next$

$\langle 2\rangle 27$. $Inv8C'$
$\langle 3\rangle 1$.CASE $L1$
$\langle 4\rangle 1$.CASE $\land\, pc[\text{“W”}] = 1$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\, A' = v$
$\land\, (\lor\, X = \text{FALSE}$
$\lor\, pc[\text{“S”}] = 6$
$\lor\, (\land\, pc[\text{“S”}] = 7$
$\land\, B = Bot)$
$\lor\, B = v$
$\lor\, (\land\, pc[\text{“S”}] = 8$
$\land\, B = Bot$
$\land\, a\ = v))$
$\land\, T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\, B,\, v,\, a,\, b\rangle$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 8$,
$B \neq Bot$
PROVE $\exists\, t \in T' : t.State = B$
BY $\langle 4\rangle 1$ DEF $Inv8C$
$\langle 5\rangle 1$. $B = v$
BY $\langle 4\rangle 1$ DEF $Inv8A$
$\langle 5\rangle 2$. PICK $t \in T$: TRUE
BY $\langle 4\rangle 1$ DEF $Inv1A$
$\langle 5\rangle$ DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$

$RetS \ \mapsto t.RetS]$

$\langle 5\rangle 3.\ u \in T'$
BY $\langle 4\rangle 1$, $\langle 5\rangle 2$
$\langle 5\rangle 4.$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 3$

$\langle 4\rangle 2.$CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\land\ A' = v$
$\land$ ($\land\ X =$ TRUE
$\land\ pc[\text{“S”}] \neq 6$
$\land$ ($\lor\ pc[\text{“S”}] \neq 7$
$\lor\ B \neq Bot$)
$\land\ B \neq v$
$\land$ ($\lor\ pc[\text{“S”}] \neq 8$
$\lor\ B \neq Bot$
$\lor\ a \neq v$))
$\land\ T' = \{[State \ \mapsto v,$
$RetW \ \mapsto Ack,$
$RetS \ \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv8C$
$\langle 4\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2.$CASE $L2$
PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv8C$
$\langle 3\rangle 3.$CASE $L3$
PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv8C$, $Inv3B$
$\langle 3\rangle 4.$CASE $L4$
$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 8$,
$B \neq Bot$
PROVE $\exists\, t \in T' : t.State = B$
BY $\langle 3\rangle 4$ DEF $Inv8C$
$\langle 4\rangle 1.$ PICK $t \in T : t.State = B$
BY $\langle 3\rangle 4$ DEF $Inv8C$
$\langle 4\rangle$ DEFINE $u \triangleq [State \ \mapsto t.State,$
$RetW \ \mapsto Bot,$
$RetS \ \mapsto t.RetS]$
$\langle 4\rangle 2.\ u \in T'$
BY $\langle 3\rangle 4$
$\langle 4\rangle 3.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$

$\langle 3\rangle 5.$CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv8C$

⟨3⟩6. CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv8C$
⟨3⟩7. CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv8C$, $Inv7C$
⟨3⟩8. CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv8C$
⟨3⟩9. CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv8C$
⟨3⟩10. CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv8C$
⟨3⟩11. CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv8C$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩28. $Inv8D'$
⟨3⟩1. CASE $L1$
⟨4⟩1. CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
⟨5⟩ SUFFICES ASSUME $pc'[\text{“S”}] = 8,$
$B' = Bot$
PROVE $\exists\, t \in T' : t.State = a'$
BY ⟨4⟩1 DEF $Inv8D$
⟨5⟩1. $a = v$
BY ⟨4⟩1 DEF $Inv8A$
⟨5⟩2. PICK $t \in T$: TRUE
BY ⟨4⟩1 DEF $Inv1A$
⟨5⟩ DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS]$
⟨5⟩3. $u \in T'$
BY ⟨4⟩1, ⟨5⟩2

⟨5⟩4. QED
BY ⟨4⟩1, ⟨5⟩1, ⟨5⟩3

⟨4⟩2.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \land\ X = \text{TRUE}$
$\land\ pc[\text{“S”}] \neq 6$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 7$
$\lor\ B \neq Bot)$
$\land\ B \neq v$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 8$
$\lor\ B \neq Bot$
$\lor\ a\ \neq v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
PROOF BY ⟨4⟩2, ⟨3⟩1 DEF $TypeOK$, $Inv8D$
⟨4⟩3. QED
BY ⟨3⟩1, ⟨4⟩1, ⟨4⟩2 DEF $L1$

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv8D$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv8D$
⟨3⟩4.CASE $L4$
⟨4⟩ SUFFICES ASSUME $pc[\text{“S”}] = 8$,
$B = Bot$
PROVE $\exists\, t\_pr \in T' : t\_pr.State = a'$
BY ⟨3⟩4 DEF $Inv8D$
⟨4⟩1. PICK $t \in T : t.State = a$
BY ⟨3⟩4 DEF $Inv8D$
⟨4⟩ DEFINE $u \triangleq [State\ \mapsto t.State,$
$RetW\ \mapsto Bot,$
$RetS\ \mapsto t.RetS]$
⟨4⟩2. $\land\ u \in T'$
$\land\ u.State = a'$
BY ⟨3⟩4, ⟨4⟩1
⟨4⟩ QED
PROOF BY ⟨3⟩4, ⟨4⟩2
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv8D$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv8D$

⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv8D$, $Inv7D$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv8D$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv8D$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv8D$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv8D$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩29. $Inv9A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv9A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv9A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv9A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv9A$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv9A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv9A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv9A$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv9A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv9A$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv9A$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv9A$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩30. $Inv9B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv9B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv9B$
⟨3⟩3.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 4$.CASE $L4$
PROOF BY $\langle 3\rangle 4$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 5$.CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 6$.CASE $L6$
PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 7$.CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 8$.CASE $L8$
PROOF BY $\langle 3\rangle 8$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 9$.CASE $L9$
PROOF BY $\langle 3\rangle 9$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 10$.CASE $L10$
PROOF BY $\langle 3\rangle 10$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 11$.CASE UNCHANGED $vars$
PROOF BY $\langle 3\rangle 11$ DEF $TypeOK$, $Inv9B$
$\langle 3\rangle 12$. QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 10$, $\langle 3\rangle 11$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$, $\langle 3\rangle 5$, $\langle 3\rangle 6$, $\langle 3\rangle 7$, $\langle 3\rangle 8$, $\langle 3\rangle 9$ DEF $Next$

$\langle 2\rangle 31$. $Inv9C'$
$\langle 3\rangle 1$.CASE $L1$
$\langle 4\rangle 1$.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X =$ FALSE
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 9,$
$B \neq Bot$
PROVE $\exists\, t \in T' : t.RetS = B$
BY $\langle 4\rangle 1$ DEF $Inv9C$
$\langle 5\rangle 1$. PICK $t \in T : t.RetS = B$
BY $\langle 4\rangle 1$ DEF $Inv9C$
$\langle 5\rangle$ DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$

$RetS \ \mapsto t.RetS]$

$\langle 5\rangle 2. \land u \in T'$
$\quad \land u.RetS = B$
BY $\langle 4\rangle 1$, $\langle 5\rangle 1$

$\langle 5\rangle 3.$ QED
BY $\langle 5\rangle 2$

$\langle 4\rangle 2.$CASE $\land pc[\text{“W”}] = 1$
$\land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land A' = v$
$\land (\land X = \text{TRUE}$
$\land pc[\text{“S”}] \neq 6$
$\land (\lor pc[\text{“S”}] \neq 7$
$\lor B \neq Bot)$
$\land B \neq v$
$\land (\lor pc[\text{“S”}] \neq 8$
$\lor B \neq Bot$
$\lor a \neq v))$
$\land T' = \{[State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X, B, v, a, b\rangle$
PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 1$, *Zenon* DEF $TypeOK$, $Inv9C$

$\langle 4\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2.$CASE $L2$
PROOF BY $\langle 3\rangle 2$ DEF $TypeOK$, $Inv9C$
$\langle 3\rangle 3.$CASE $L3$
PROOF BY $\langle 3\rangle 3$ DEF $TypeOK$, $Inv9C$, $Inv3C$
$\langle 3\rangle 4.$CASE $L4$
PROOF BY $\langle 3\rangle 4$, *Isa* DEF $TypeOK$, $Inv9C$
$\langle 3\rangle 5.$CASE $L5$
PROOF BY $\langle 3\rangle 5$ DEF $TypeOK$, $Inv9C$
$\langle 3\rangle 6.$CASE $L6$
PROOF BY $\langle 3\rangle 6$ DEF $TypeOK$, $Inv9C$
$\langle 3\rangle 7.$CASE $L7$
PROOF BY $\langle 3\rangle 7$ DEF $TypeOK$, $Inv9C$
$\langle 3\rangle 8.$CASE $L8$
$\langle 4\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 8$,
$B \neq Bot$
PROVE $\exists\, t\_pr \in T' : t\_pr.RetS = B$
BY $\langle 3\rangle 8$ DEF $Inv9C$
$\langle 4\rangle 1.$ PICK $t \in T : t.State = B$
BY $\langle 3\rangle 8$ DEF $Inv8C$
$\langle 4\rangle 2.$CASE $t.RetW = Ack$

⟨5⟩1. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$
⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩2
⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2
⟨4⟩3.CASE $t.RetW = Bot \land pc[\text{“W”}] = 1$
⟨5⟩1. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Bot,$
$RetS \mapsto t.State]$
⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩3
⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2
⟨4⟩4.CASE $t.RetW = Bot \land pc[\text{“W”}] \neq 1$
⟨5⟩1. DEFINE $u \triangleq [State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$
⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩4
⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2
⟨4⟩5. QED
BY ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 DEF *TypeOK*

⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*9*C*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*9*C*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*9*C*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩32. *Inv*9*D*′
⟨3⟩1.CASE *L*1
⟨4⟩1.CASE $\land pc[\text{“W”}] = 1$
$\land pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land A' = v$
$\land (\lor X = \text{FALSE}$
$\lor pc[\text{“S”}] = 6$
$\lor (\land pc[\text{“S”}] = 7$
$\land B = Bot)$
$\lor B = v$

$\lor$ ($\land$ $pc[\text{“S”}] = 8$
$\land B = Bot$
$\land a = v$))
$\land T' = \{[State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X, B, v, a, b\rangle$

$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 9,$
$B = Bot$
PROVE $\exists\, t \in T' : t.RetS = a$
BY $\langle 4\rangle 1$ DEF $Inv9D$

$\langle 5\rangle 1$. PICK $t \in T : t.RetS = a$
BY $\langle 4\rangle 1$ DEF $Inv9D$

$\langle 5\rangle$ DEFINE $u \triangleq [State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS]$

$\langle 5\rangle 2$. $\land u \in T'$
$\land u.RetS = a$
BY $\langle 4\rangle 1, \langle 5\rangle 1$

$\langle 5\rangle 3$. QED
BY $\langle 5\rangle 2$

$\langle 4\rangle 2$.CASE $\land pc[\text{“W”}] = 1$
$\land pc' = [pc$ EXCEPT $![\text{“W”}] = 2]$
$\land A' = v$
$\land$ ($\land X =$ TRUE
$\land pc[\text{“S”}] \neq 6$
$\land$ ($\lor pc[\text{“S”}] \neq 7$
$\lor B \neq Bot$)
$\land B \neq v$
$\land$ ($\lor pc[\text{“S”}] \neq 8$
$\lor B \neq Bot$
$\lor a \neq v$))
$\land T' = \{[State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X, B, v, a, b\rangle$

PROOF BY $\langle 4\rangle 2, \langle 3\rangle 1$ DEF $TypeOK, Inv9D$

$\langle 4\rangle 3$. QED
BY $\langle 3\rangle 1, \langle 4\rangle 1, \langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2$.CASE $L2$
PROOF BY $\langle 3\rangle 2$ DEF $TypeOK, Inv9D$

$\langle 3\rangle 3$.CASE $L3$
PROOF BY $\langle 3\rangle 3$ DEF $TypeOK, Inv9D$

$\langle 3\rangle 4$.CASE $L4$

⟨4⟩ SUFFICES ASSUME $pc[\text{“S”}] = 9$,
$B = Bot$
PROVE $\exists\, t \in T' : t.RetS = a$
BY ⟨3⟩4 DEF $Inv9D$
⟨4⟩1. PICK $t \in T : t.RetS = a$
BY ⟨3⟩4 DEF $Inv9D$
⟨4⟩2. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Bot,$
$RetS \mapsto t.RetS]$
⟨4⟩3. $u \in T'$
BY ⟨3⟩4, ⟨4⟩1
⟨4⟩4. QED
BY ⟨4⟩1, ⟨4⟩3

⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv9D$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv9D$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv9D$
⟨3⟩8.CASE $L8$
⟨4⟩ SUFFICES ASSUME $pc[\text{“S”}] = 8$,
$B = Bot$
PROVE $\exists\, t \in T' : t.RetS = a$
BY ⟨3⟩8 DEF $Inv9D$
⟨4⟩1. PICK $t \in T : t.State = a$
BY ⟨3⟩8 DEF $Inv8D$
⟨4⟩2.CASE $t.RetW = Ack$
⟨5⟩1. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Ack,$
$RetS \mapsto t.State]$
⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩2
⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2
⟨4⟩3.CASE $t.RetW = Bot \wedge pc[\text{“W”}] = 1$
⟨5⟩1. DEFINE $u \triangleq [State \mapsto t.State,$
$RetW \mapsto Bot,$
$RetS \mapsto t.State]$
⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩3
⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2
⟨4⟩4.CASE $t.RetW = Bot \wedge pc[\text{“W”}] \neq 1$
⟨5⟩1. DEFINE $u \triangleq [State \mapsto v,$

$RetW \ \mapsto Ack,$
$RetS \ \mapsto t.State]$

⟨5⟩2. $u \in T'$
BY ⟨3⟩8, ⟨4⟩1, ⟨4⟩4

⟨5⟩3. QED
BY ⟨4⟩1, ⟨5⟩2

⟨4⟩5. QED
BY ⟨4⟩2, ⟨4⟩3, ⟨4⟩4 DEF *TypeOK*

⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*9*D*

⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*9*D*

⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*9*D*

⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩33. *Inv*9*E*′

⟨3⟩1.CASE *L*1
PROOF BY ⟨3⟩1 DEF *TypeOK*, *Inv*9*A*, *Inv*9*E*

⟨3⟩2.CASE *L*2
PROOF BY ⟨3⟩2 DEF *TypeOK*, *Inv*9*E*

⟨3⟩3.CASE *L*3
PROOF BY ⟨3⟩3 DEF *TypeOK*, *Inv*9*E*

⟨3⟩4.CASE *L*4
PROOF BY ⟨3⟩4 DEF *TypeOK*, *Inv*9*E*

⟨3⟩5.CASE *L*5
PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*9*E*

⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*9*E*

⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*9*E*

⟨3⟩8.CASE *L*8

⟨4⟩1. $(\forall\, t \in T : pc[\text{“W”}] \neq 1 \Rightarrow t.RetW = Ack)'$
PROOF BY ⟨3⟩8 DEF *Inv*9*E*

⟨4⟩2. $(\forall\, t \in T : t.State = A)'$

⟨5⟩ SUFFICES ASSUME NEW $u \in T'$
PROVE $u.State = A$
BY ⟨3⟩8

⟨5⟩1.CASE $\exists\, t \in T :$ $\land\ t.RetW = Bot$
$\land\ pc[\text{“W”}] \neq 1$
$\land\ u.State = v$
$\land\ u.RetW = Ack$
$\land\ u.RetS = t.State$

⟨6⟩1. $v = A$
BY ⟨5⟩1 DEF $TypeOK$, $Inv2A$, $Inv3A$, $Inv4A$
⟨6⟩2. QED
BY ⟨5⟩1, ⟨6⟩1
⟨5⟩2.CASE $\exists\, t \in T :\ \wedge\, t.RetW = Bot$
$\wedge\, pc[\text{“W”}] = 1$
$\wedge\, u.State\ = t.State$
$\wedge\, u.RetW = Bot$
$\wedge\, u.RetS\ = t.State$
⟨6⟩1. $\forall\, t \in T : t.State = A$
BY ⟨5⟩2 DEF $Inv1B$
⟨6⟩2. QED
BY ⟨5⟩2, ⟨6⟩1
⟨5⟩3.CASE $\exists\, t \in T :\ \wedge\, t.RetW = Ack$
$\wedge\, u.State = t.State$
$\wedge\, u.RetW = Ack$
$\wedge\, u.RetS\ = t.State$
⟨6⟩1. $\forall\, t \in T : t.RetW = Ack \Rightarrow t.State = A$
BY DEF $Inv0B$
⟨6⟩2. QED
BY ⟨5⟩3, ⟨6⟩1
⟨5⟩4. QED
BY ⟨3⟩8, ⟨5⟩1, ⟨5⟩2, ⟨5⟩3
PROOF BY ⟨3⟩8 DEF $Inv8A$, $Inv8B$, $Inv1A$, $Inv1B$, $Inv2A$, $Inv2C$, $Inv3A$, $Inv4A$
⟨4⟩3. QED
BY ⟨4⟩1, ⟨4⟩2 DEF $Inv9E$

⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv9E$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv9E$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv9E$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩34. $Inv10A'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv10A$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv10A$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv10A$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv10A$

⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv10A$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv10A$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv10A$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv10A$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv10A$, $Inv9A$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv10A$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv10A$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩35. $Inv10B'$
⟨3⟩1.CASE $L1$
PROOF BY ⟨3⟩1 DEF $TypeOK$, $Inv10B$
⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv10B$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv10B$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4 DEF $TypeOK$, $Inv10B$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv10B$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv10B$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv10B$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv10B$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv10B$, $Inv9B$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv10B$
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv10B$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩36. $Inv10C'$
⟨3⟩1.CASE $L1$

$\langle 4\rangle 1$.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
$\langle 5\rangle$ SUFFICES ASSUME $pc[\text{“S”}] = 10,$
$b \neq Bot$
PROVE $\exists\, t \in T' : t.RetS = b$
BY $\langle 4\rangle 1$ DEF $Inv10C$
$\langle 5\rangle 1$. PICK $t \in T : t.RetS = b$
BY $\langle 4\rangle 1$ DEF $Inv10C$
$\langle 5\rangle 2$. DEFINE $u \triangleq [State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS]$
$\langle 5\rangle 3$. $u \in T'$
BY $\langle 4\rangle 1$
$\langle 5\rangle 4$. QED
BY $\langle 4\rangle 1$, $\langle 5\rangle 1$, $\langle 5\rangle 3$

$\langle 4\rangle 2$.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \land\ X = \text{TRUE}$
$\land\ pc[\text{“S”}] \neq 6$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 7$
$\lor\ B \neq Bot)$
$\land\ B \neq v$
$\land\ (\ \lor\ pc[\text{“S”}] \neq 8$
$\lor\ B \neq Bot$
$\lor\ a\ \neq v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
PROOF BY $\langle 4\rangle 2$, $\langle 3\rangle 1$ DEF $TypeOK$, $Inv10C$

⟨4⟩3. QED
BY ⟨3⟩1, ⟨4⟩1, ⟨4⟩2 DEF $L1$

⟨3⟩2.CASE $L2$
PROOF BY ⟨3⟩2 DEF $TypeOK$, $Inv10C$
⟨3⟩3.CASE $L3$
PROOF BY ⟨3⟩3 DEF $TypeOK$, $Inv10C$, $Inv10E$
⟨3⟩4.CASE $L4$
PROOF BY ⟨3⟩4, Isa DEF $TypeOK$, $Inv10C$
⟨3⟩5.CASE $L5$
PROOF BY ⟨3⟩5 DEF $TypeOK$, $Inv10C$
⟨3⟩6.CASE $L6$
PROOF BY ⟨3⟩6 DEF $TypeOK$, $Inv10C$
⟨3⟩7.CASE $L7$
PROOF BY ⟨3⟩7 DEF $TypeOK$, $Inv10C$
⟨3⟩8.CASE $L8$
PROOF BY ⟨3⟩8 DEF $TypeOK$, $Inv10C$
⟨3⟩9.CASE $L9$
PROOF BY ⟨3⟩9 DEF $TypeOK$, $Inv10C$, $Inv9C$
⟨3⟩10.CASE $L10$
PROOF BY ⟨3⟩10 DEF $TypeOK$, $Inv10C$
⟨3⟩11.CASE UNCHANGED $vars$
PROOF BY ⟨3⟩11 DEF $TypeOK$, $Inv10C$
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF $Next$

⟨2⟩37. $Inv10D'$
⟨3⟩1.CASE $L1$
⟨4⟩1.CASE $\land\ pc[\text{“W”}] = 1$
$\land\ pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\ A' = v$
$\land\ (\ \lor\ X = \text{FALSE}$
$\lor\ pc[\text{“S”}] = 6$
$\lor\ (\ \land\ pc[\text{“S”}] = 7$
$\land\ B = Bot)$
$\lor\ B = v$
$\lor\ (\ \land\ pc[\text{“S”}] = 8$
$\land\ B = Bot$
$\land\ a\ = v))$
$\land\ T' = \{[State\ \mapsto v,$
$RetW\ \mapsto Ack,$
$RetS\ \mapsto t.RetS] : t \in T\}$
$\land$ UNCHANGED $\langle X,\ B,\ v,\ a,\ b\rangle$
⟨5⟩ SUFFICES ASSUME $pc[\text{“S”}] = 10,$
$b = Bot$

PROVE $\exists\, t \in T' : t.RetS = a$

BY $\langle 4\rangle 1$ DEF $Inv10D$

$\langle 5\rangle 1$. PICK $t \in T : t.RetS = a$

BY $\langle 4\rangle 1$ DEF $Inv10D$

$\langle 5\rangle 2$. DEFINE $u \triangleq [State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS]$

$\langle 5\rangle 3$. $u \in T'$

BY $\langle 4\rangle 1$

$\langle 5\rangle 4$. QED

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

$\langle 4\rangle 2$.CASE $\land\, pc[\text{“W”}] = 1$
$\land\, pc' = [pc \text{ EXCEPT } ![\text{“W”}] = 2]$
$\land\, A' = v$
$\land\, (\, \land\, X = \text{TRUE}$
$\land\, pc[\text{“S”}] \neq 6$
$\land\, (\, \lor\, pc[\text{“S”}] \neq 7$
$\lor\, B \neq Bot)$
$\land\, B \neq v$
$\land\, (\, \lor\, pc[\text{“S”}] \neq 8$
$\lor\, B \neq Bot$
$\lor\, a \neq v))$
$\land\, T' = \{[State \mapsto v,$
$RetW \mapsto Ack,$
$RetS \mapsto t.RetS] : t \in T\} \cup T$
$\land$ UNCHANGED $\langle X, B, v, a, b\rangle$

PROOF BY $\langle 4\rangle 2, \langle 3\rangle 1$ DEF $TypeOK, Inv10D$

$\langle 4\rangle 3$. QED

BY $\langle 3\rangle 1, \langle 4\rangle 1, \langle 4\rangle 2$ DEF $L1$

$\langle 3\rangle 2$.CASE $L2$

PROOF BY $\langle 3\rangle 2$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 3$.CASE $L3$

PROOF BY $\langle 3\rangle 3$ DEF $TypeOK, Inv10D, Inv10E$

$\langle 3\rangle 4$.CASE $L4$

PROOF BY $\langle 3\rangle 4, Isa$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 5$.CASE $L5$

PROOF BY $\langle 3\rangle 5$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 6$.CASE $L6$

PROOF BY $\langle 3\rangle 6$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 7$.CASE $L7$

PROOF BY $\langle 3\rangle 7$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 8$.CASE $L8$

PROOF BY $\langle 3\rangle 8$ DEF $TypeOK, Inv10D$

$\langle 3\rangle 9$.CASE $L9$

PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*10*D*, *Inv*9*D*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*10*D*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*10*D*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩38. *Inv*10E'
⟨3⟩1.CASE *L*1
PROOF BY ⟨3⟩1 DEF *TypeOK*, *Inv*10*A*, *Inv*10*E*
⟨3⟩2.CASE *L*2
PROOF BY ⟨3⟩2 DEF *TypeOK*, *Inv*10*E*
⟨3⟩3.CASE *L*3
PROOF BY ⟨3⟩3 DEF *TypeOK*, *Inv*10*E*
⟨3⟩4.CASE *L*4
PROOF BY ⟨3⟩4 DEF *TypeOK*, *Inv*10*E*
⟨3⟩5.CASE *L*5
PROOF BY ⟨3⟩5 DEF *TypeOK*, *Inv*10*E*
⟨3⟩6.CASE *L*6
PROOF BY ⟨3⟩6 DEF *TypeOK*, *Inv*10*E*
⟨3⟩7.CASE *L*7
PROOF BY ⟨3⟩7 DEF *TypeOK*, *Inv*10*E*
⟨3⟩8.CASE *L*8
PROOF BY ⟨3⟩8 DEF *TypeOK*, *Inv*10*E*
⟨3⟩9.CASE *L*9
PROOF BY ⟨3⟩9 DEF *TypeOK*, *Inv*9*E*, *Inv*10*E*
⟨3⟩10.CASE *L*10
PROOF BY ⟨3⟩10 DEF *TypeOK*, *Inv*10*E*
⟨3⟩11.CASE UNCHANGED *vars*
PROOF BY ⟨3⟩11 DEF *TypeOK*, *Inv*10*E*
⟨3⟩12. QED
BY ⟨3⟩1, ⟨3⟩10, ⟨3⟩11, ⟨3⟩2, ⟨3⟩3, ⟨3⟩4, ⟨3⟩5, ⟨3⟩6, ⟨3⟩7, ⟨3⟩8, ⟨3⟩9 DEF *Next*

⟨2⟩39. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩10, ⟨2⟩11, ⟨2⟩12, ⟨2⟩13, ⟨2⟩14, ⟨2⟩15, ⟨2⟩16, ⟨2⟩17, ⟨2⟩18, ⟨2⟩19, ⟨2⟩20, ⟨2⟩21, ⟨2⟩22, ⟨2⟩23,

⟨1⟩3. QED
BY ⟨1⟩1, ⟨1⟩2, *PTL* DEF *Spec*

* Modification History
* Last modified *Fri* May 14 16:30:14 *EDT* 2021 by *uguryavuz*
* Created *Thu* May 13 11:08:51 *EDT* 2021 by *uguryavuz*