MODULE *SnapShot*

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

CONSTANT *Proc*, *Val*

ASSUME $ProcFinite \triangleq IsFiniteSet(Proc)$

ASSUME $ValFinite \triangleq IsFiniteSet(Val)$

The assumption that *Val* is a finite set isn't necessary, but it simplifies the proof.

$NUnion(A) \triangleq \text{UNION } \{A[i] : i \in Nat\}$

****

--algorithm *SnapShot*

$\{$ **variables** $result = [p \in Proc \mapsto \{\}],$
$A2 = [i \in Nat \mapsto \{\}],$
$A3 = [i \in Nat \mapsto \{\}],$

process $(\ Pr \in Proc\ )$

variables $myVals = \{\},$
$known = \{\},$
$notKnown = \{\},$
$lnbpart = 0,$
$nbpart = 0,$
$nextout = \{\},$ This is a history variable, used only for the proof
$out = \{\};$

$\{\ a$: **with** $(\ P \in \{Q \in \text{SUBSET } Proc :$
$\quad \land\ self \in Q$
$\quad \land\ \forall p \in Proc \setminus \{self\} :$
$\qquad \lor\ Cardinality(result[p]) \neq Cardinality(Q)$
$\qquad \lor\ Q = result[p]$
$\}\ )$
$\{\ result[self] := P\ \}\ ;$
$A2[Cardinality(result[self]) - 1] := result[self]\,;$

b: **while** $(\ \text{TRUE}\ )$
$\{$ **with** $(\ v \in Val\ )\ \{\ myVals := myVals \cup \{v\}\ \}\ ;$
$known := myVals \cup known\,;$
$nbpart := Cardinality(NUnion(A2))\,;$

c: $lnbpart := nbpart\,;$
$known := known \cup NUnion(A3)\,;$
$notKnown := \{i \in 0 \,..\, (nbpart - 1) : known \neq A3[i]\}\,;$
if $(\ notKnown \neq \{\}\ )\ \{\ d$: **with** $(\ i \in notKnown\ )$
$\{\ A3[i] := known\ \}\ ;$
goto c
$\}$
else if $(\ nbpart = Cardinality(NUnion(A2))\ )$

```
                  { nextout := known } ;

              e: nbpart := Cardinality(NUnion(A2)) ;
                 if ( lnbpart = nbpart ) { out := known }
                 else { goto c }
              }
        }
}
```

****

BEGIN TRANSLATION

VARIABLES $result, A2, A3, pc, myVals, known, notKnown, lnbpart, nbpart, nextout, out$

$$vars \triangleq \langle result, A2, A3, pc, myVals, known, notKnown, lnbpart, nbpart, nextout, out \rangle$$

$$ProcSet \triangleq (Proc)$$

$Init \triangleq$ Global variables

$$\begin{aligned}
&\land result = [p \in Proc \mapsto \{\}]\\
&\land A2 = [i \in Nat \mapsto \{\}]\\
&\land A3 = [i \in Nat \mapsto \{\}]
\end{aligned}$$

Process Pr

$$\begin{aligned}
&\land myVals = [self \in Proc \mapsto \{\}]\\
&\land known = [self \in Proc \mapsto \{\}]\\
&\land notKnown = [self \in Proc \mapsto \{\}]\\
&\land lnbpart = [self \in Proc \mapsto 0]\\
&\land nbpart = [self \in Proc \mapsto 0]\\
&\land nextout = [self \in Proc \mapsto \{\}]\\
&\land out = [self \in Proc \mapsto \{\}]\\
&\land pc = [self \in ProcSet \mapsto \text{“a”}]
\end{aligned}$$

$$\begin{aligned}
a(self) \triangleq\ &\land pc[self] = \text{“a”}\\
&\land \exists P \in \{Q \in \text{SUBSET } Proc :\\
&\qquad\qquad \land self \in Q\\
&\qquad\qquad \land \forall p \in Proc \setminus \{self\} :\\
&\qquad\qquad\qquad \lor Cardinality(result[p]) \neq Cardinality(Q)\\
&\qquad\qquad\qquad \lor Q = result[p]\\
&\qquad\quad \} :\\
&\quad result' = [result \text{ EXCEPT } ![self] = P]\\
&\land A2' = [A2 \text{ EXCEPT } ![Cardinality(result'[self]) - 1] = result'[self]]\\
&\land pc' = [pc \text{ EXCEPT } ![self] = \text{“b”}]\\
&\land \text{UNCHANGED } \langle A3, myVals, known, notKnown, lnbpart, nbpart,\\
&\qquad\qquad nextout, out \rangle
\end{aligned}$$

$$b(self) \triangleq\ \land pc[self] = \text{“b”}$$

$$
\begin{array}{l}
\wedge\ \exists\, v \in \mathit{Val} : \\
\qquad \mathit{myVals}' = [\mathit{myVals}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{myVals}[\mathit{self}] \cup \{v\}] \\
\wedge\ \mathit{known}' = [\mathit{known}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{myVals}'[\mathit{self}] \cup \mathit{known}[\mathit{self}]] \\
\wedge\ \mathit{nbpart}' = [\mathit{nbpart}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{Cardinality}(\mathit{NUnion}(A2))] \\
\wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“c”}] \\
\wedge\ \text{UNCHANGED}\ \langle \mathit{result}, A2, A3, \mathit{notKnown}, \mathit{lnbpart}, \mathit{nextout}, \mathit{out} \rangle
\end{array}
$$

$$
\begin{array}{lcl}
c(\mathit{self}) & \triangleq & \wedge\ \mathit{pc}[\mathit{self}] = \text{“c”} \\
& & \wedge\ \mathit{lnbpart}' = [\mathit{lnbpart}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{nbpart}[\mathit{self}]] \\
& & \wedge\ \mathit{known}' = [\mathit{known}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{known}[\mathit{self}] \cup \mathit{NUnion}(A3)] \\
& & \wedge\ \mathit{notKnown}' = [\mathit{notKnown}\ \text{EXCEPT}\ ![\mathit{self}] = \{i \in 0 \mathrel{..} (\mathit{nbpart}[\mathit{self}] - 1) : \mathit{known}'[\mathit{self}] \neq A3[i]\}] \\
& & \wedge\ \text{IF}\ \mathit{notKnown}'[\mathit{self}] \neq \{\} \\
& & \qquad \text{THEN}\ \wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“d”}] \\
& & \qquad\qquad\quad \wedge\ \text{UNCHANGED}\ \mathit{nextout} \\
& & \qquad \text{ELSE}\ \wedge\ \text{IF}\ \mathit{nbpart}[\mathit{self}] = \mathit{Cardinality}(\mathit{NUnion}(A2)) \\
& & \qquad\qquad\qquad\quad \text{THEN}\ \wedge\ \mathit{nextout}' = [\mathit{nextout}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{known}'[\mathit{self}]] \\
& & \qquad\qquad\qquad\quad \text{ELSE}\ \wedge\ \text{TRUE} \\
& & \qquad\qquad\qquad\qquad\qquad \wedge\ \text{UNCHANGED}\ \mathit{nextout} \\
& & \qquad\qquad\quad \wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“e”}] \\
& & \wedge\ \text{UNCHANGED}\ \langle \mathit{result}, A2, A3, \mathit{myVals}, \mathit{nbpart}, \mathit{out} \rangle
\end{array}
$$

$$
\begin{array}{lcl}
d(\mathit{self}) & \triangleq & \wedge\ \mathit{pc}[\mathit{self}] = \text{“d”} \\
& & \wedge\ \exists\, i \in \mathit{notKnown}[\mathit{self}] : \\
& & \qquad A3' = [A3\ \text{EXCEPT}\ ![i] = \mathit{known}[\mathit{self}]] \\
& & \wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“c”}] \\
& & \wedge\ \text{UNCHANGED}\ \langle \mathit{result}, A2, \mathit{myVals}, \mathit{known}, \mathit{notKnown}, \mathit{lnbpart}, \\
& & \qquad\qquad\qquad\quad \mathit{nbpart}, \mathit{nextout}, \mathit{out} \rangle
\end{array}
$$

$$
\begin{array}{lcl}
e(\mathit{self}) & \triangleq & \wedge\ \mathit{pc}[\mathit{self}] = \text{“e”} \\
& & \wedge\ \mathit{nbpart}' = [\mathit{nbpart}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{Cardinality}(\mathit{NUnion}(A2))] \\
& & \wedge\ \text{IF}\ \mathit{lnbpart}[\mathit{self}] = \mathit{nbpart}'[\mathit{self}] \\
& & \qquad \text{THEN}\ \wedge\ \mathit{out}' = [\mathit{out}\ \text{EXCEPT}\ ![\mathit{self}] = \mathit{known}[\mathit{self}]] \\
& & \qquad\qquad\quad \wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“b”}] \\
& & \qquad \text{ELSE}\ \wedge\ \mathit{pc}' = [\mathit{pc}\ \text{EXCEPT}\ ![\mathit{self}] = \text{“c”}] \\
& & \qquad\qquad\quad \wedge\ \mathit{out}' = \mathit{out} \\
& & \wedge\ \text{UNCHANGED}\ \langle \mathit{result}, A2, A3, \mathit{myVals}, \mathit{known}, \mathit{notKnown}, \mathit{lnbpart}, \\
& & \qquad\qquad\qquad\quad \mathit{nextout} \rangle
\end{array}
$$

$$
\mathit{Pr}(\mathit{self}) \triangleq a(\mathit{self}) \vee b(\mathit{self}) \vee c(\mathit{self}) \vee d(\mathit{self}) \vee e(\mathit{self})
$$

$$
\begin{array}{l}
\mathit{Next} \triangleq (\exists\, \mathit{self} \in \mathit{Proc} : \mathit{Pr}(\mathit{self})) \\
\qquad\quad \vee\ \text{Disjunct to prevent deadlock on termination} \\
\qquad\qquad ((\forall\, \mathit{self} \in \mathit{ProcSet} : \mathit{pc}[\mathit{self}] = \text{“Done”}) \wedge \text{UNCHANGED}\ \mathit{vars})
\end{array}
$$

$$
\mathit{Spec} \triangleq \mathit{Init} \wedge \Box[\mathit{Next}]_{\mathit{vars}}
$$

$$
\mathit{Termination} \triangleq \Diamond(\forall\, \mathit{self} \in \mathit{ProcSet} : \mathit{pc}[\mathit{self}] = \text{“Done”})
$$

END TRANSLATION

The definition of the invariant.

$$PUnion(Q) \triangleq \text{UNION } \{Q[p] : p \in Proc\}$$

The type-correctness invariant.

$$\begin{aligned}
TypeOK \triangleq\ & \land\ result \in [Proc \rightarrow \text{SUBSET } Proc] \\
& \land\ myVals \in [Proc \rightarrow \text{SUBSET } Val] \\
& \land\ pc \in [Proc \rightarrow \{\text{“a”}, \text{“b”}, \text{“c”}, \text{“d”}, \text{“e”}\}] \\
& \land\ A2 \in [Nat \rightarrow \text{SUBSET } Proc] \\
& \land\ A3 \in [Nat \rightarrow \text{SUBSET } Val] \\
& \land\ known \in [Proc \rightarrow \text{SUBSET } Val] \\
& \land\ nbpart \in [Proc \rightarrow Nat] \\
& \land\ lnbpart \in [Proc \rightarrow Nat] \\
& \land\ notKnown \in [Proc \rightarrow \text{SUBSET } Nat] \\
& \land\ out \in [Proc \rightarrow \text{SUBSET } Val] \\
& \land\ nextout \in [Proc \rightarrow \text{SUBSET } Val]
\end{aligned}$$

*Inv*1 is a straightforward invariant. Its invariance is fairly easy to see by examining the algorithm's code.

$$\begin{aligned}
Inv1 \triangleq\ & \land\ \forall p \in Proc : \\
& \qquad \land\ known[p] \subseteq PUnion(myVals) \\
& \qquad \land\ out[p] \subseteq nextout[p] \\
& \qquad \land\ nextout[p] \subseteq known[p] \\
& \qquad \land\ (pc[p] = \text{“e”}) \Rightarrow (lnbpart[p] = nbpart[p]) \\
& \qquad \land\ nbpart[p] \leq Cardinality(NUnion(A2)) \\
& \qquad \land\ lnbpart[p] \leq nbpart[p] \\
& \qquad \land\ \land\ pc[p] = \text{“e”} \\
& \qquad \quad\ \land\ nbpart[p] = Cardinality(NUnion(A2)) \\
& \qquad \quad\ \Rightarrow (nextout[p] = known[p]) \\
& \qquad \land\ myVals[p] \subseteq known[p] \\
& \qquad \land\ (myVals[p] \neq \{\}) \Rightarrow (pc[p] \neq \text{“a”}) \\
& \qquad \land\ (pc[p] \neq \text{“a”}) \Rightarrow\ \land\ p \in result[p] \\
& \qquad \qquad \qquad \qquad \qquad\ \ \land\ A2[Cardinality(result[p]) - 1] = result[p] \\
& \land\ NUnion(A3) \subseteq PUnion(myVals) \\
& \land\ \forall i \in Nat :\ \lor\ A2[i] = \{\} \\
& \qquad \qquad \qquad\ \lor\ \exists p \in Proc :\ \land\ pc[p] \neq \text{“a”} \\
& \qquad \qquad \qquad \qquad \qquad \qquad\ \land\ i = Cardinality(result[p]) - 1 \\
& \qquad \qquad \qquad \qquad \qquad \qquad\ \land\ A2[i] = result[p]
\end{aligned}$$

We now define invariant *Inv*2, which is the key to the algorithm's correctness.

$$NotAProc \triangleq \text{CHOOSE } n : n \notin Proc$$

An arbitrary value that is not a process.

$$ReadyToWrite(i, p) \triangleq\ \land\ pc[p] = \text{“d”}$$

$\land i \in notKnown[p]$

True iff process p is ready to write $known[p]$ to $A3[i]$.

$$WriterAssignment \triangleq \{f \in [Nat \rightarrow Proc \cup \{NotAProc\}] : \forall i \in Nat : (f[i] \in Proc) \Rightarrow \land ReadyToWrite(i, f[i]) \land \forall j \in Nat \setminus \{i\} : f[j] \neq f[i]\}$$

The set of functions f that assign to each Nat i either a unique process that is ready to write i or the value $NotAProc$.

$$PV(wa) \triangleq [i \in Nat \mapsto \text{IF } wa[i] = NotAProc \text{ THEN } A3[i] \text{ ELSE } known[wa[i]]]$$

$$PA3 \triangleq \{PV(wa) : wa \in WriterAssignment\}$$

$PA3$ is the set of all values that $A3$ could assume if some subset of processes that are ready to write wrote.

$$Inv2 \triangleq \forall p \in Proc : \forall P \in PA3 : nextout[p] \subseteq NUnion(P)$$

Inv is the complete inductive invariant.

$$Inv \triangleq TypeOK \land Inv1 \land Inv2$$

The following are the same theorems assumed in module GFX.

THEOREM $EmptySetCardinality \triangleq Cardinality(\{\}) = 0$
PROOF OMITTED

THEOREM $NonEmptySetCardinality \triangleq$
$\forall S : IsFiniteSet(S) \land S \neq \{\} \Rightarrow (Cardinality(S) > 0)$
PROOF OMITTED

THEOREM $SingletonCardinalty \triangleq \forall x : Cardinality(\{x\}) = 1$
PROOF OMITTED

THEOREM $SubsetFinite \triangleq$
$\forall S : IsFiniteSet(S) \Rightarrow \forall T \in \text{SUBSET } S : IsFiniteSet(T)$
PROOF OMITTED

THEOREM $CardType \triangleq \forall S : IsFiniteSet(S) \Rightarrow Cardinality(S) \in Nat$
PROOF OMITTED

THEOREM $SubsetCardinality \triangleq$
$\forall T : IsFiniteSet(T) \Rightarrow \forall S \in \text{SUBSET } T : (S \neq T) \Rightarrow (Cardinality(S) < Cardinality(T))$
PROOF OMITTED

THEOREM $SubsetCardinality2 \triangleq$

$$\forall T : IsFiniteSet(T) \Rightarrow \forall S \in \text{SUBSET } T : (Cardinality(S) \leq Cardinality(T))$$

PROOF OMITTED

THEOREM $IntervalCardinality \triangleq$

$$\forall i, j \in Int : i \leq j \Rightarrow \land IsFiniteSet(i \mathrel{..} (j-1)) \land Cardinality(i \mathrel{..} (j-1)) = (j-i)$$

PROOF OMITTED

THEOREM $PigeonHolePrinciple \triangleq$

$$\forall S, T : \land IsFiniteSet(S) \land IsFiniteSet(T) \land Cardinality(T) < Cardinality(S) \Rightarrow \forall f \in [S \to T] : \exists x, y \in S : (x \neq y) \land (f[x] = f[y])$$

PROOF OMITTED

COROLLARY $InjectionCardinality \triangleq$

$$\forall S, T, f : \land IsFiniteSet(S) \land IsFiniteSet(T) \land f \in [S \to T] \land \forall x, y \in S : x \neq y \Rightarrow f[x] \neq f[y] \Rightarrow Cardinality(S) \leq Cardinality(T)$$

BY $PigeonHolePrinciple$, $CardType$, SMT

LEMMA $NotAProcProp \triangleq NotAProc \notin Proc$

BY $NoSetContainsEverything$ DEF $NotAProc$

LEMMA $A2monotonic \triangleq$ ASSUME $TypeOK$, $TypeOK'$, $Inv1$, NEW $p \in Proc$, $a(p)$

PROVE $\land IsFiniteSet(NUnion(A2'))$
$\land NUnion(A2) \subseteq NUnion(A2')$
$\land Cardinality(NUnion(A2)) \in Nat$
$\land Cardinality(NUnion(A2')) \in Nat$
$\land Cardinality(NUnion(A2)) \leq Cardinality(NUnion(A2'))$

$\langle 1 \rangle 1.$ ASSUME NEW $i \in Nat$
PROVE $A2[i] \subseteq A2'[i]$

$\langle 2 \rangle$ DEFINE $k \triangleq Cardinality(result'[p])$

$\langle 2 \rangle 1.$ $p \in result'[p]$
BY SMT DEF a, $TypeOK$

$\langle 2 \rangle 2.$ $k \in Nat \land k > 0$

$\langle 3 \rangle 1.$ $IsFiniteSet(result'[p])$
BY $SubsetFinite$, $ProcFinite$, SMT DEF $TypeOK$

$\langle 3 \rangle 2.$ QED
BY $\langle 2 \rangle 1$, $\langle 3 \rangle 1$, $NonEmptySetCardinality$, $CardType$, SMT

$\langle 2 \rangle 3.$CASE $i = k - 1$

$\langle 3\rangle 1.\text{CASE } A2[i] = \{\}$
  BY $\langle 3\rangle 1$
$\langle 3\rangle 2.\text{CASE } \exists\, q \in Proc : \land\, pc[q] \neq \text{“a”}$
$\qquad\qquad\qquad\qquad\qquad \land\, i = Cardinality(result[q]) - 1$
$\qquad\qquad\qquad\qquad\qquad \land\, A2[i] = result[q]$
  $\langle 4\rangle 1.$ PICK $q \in Proc : \land\, pc[q] \neq \text{“a”}$
$\qquad\qquad\qquad\qquad\qquad \land\, i = Cardinality(result[q]) - 1$
$\qquad\qquad\qquad\qquad\qquad \land\, A2[i] = result[q]$
    BY $\langle 3\rangle 2$
  $\langle 4\rangle 2.\ A2'[i] = result'[p]$
    BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, SMT DEF a, $TypeOK$
  $\langle 4\rangle 3.\ result'[p] = result[q]$
    $\langle 5\rangle 1.\ result'[p] \in \{Q \in \text{SUBSET } Proc :$
$\qquad\qquad\qquad\qquad \land\, p \in Q$
$\qquad\qquad\qquad\qquad \land\, \forall\, pp \in Proc \setminus \{p\} :$
$\qquad\qquad\qquad\qquad\quad \lor\, Cardinality(result[pp]) \neq Cardinality(Q)$
$\qquad\qquad\qquad\qquad\quad \lor\, Q = result[pp]\}$
        BY SMT DEF a, $TypeOK$
    $\langle 5\rangle 2.\ \forall\, pp \in Proc \setminus \{p\} :$
$\qquad\qquad \lor\, Cardinality(result[pp]) \neq Cardinality(result'[p])$
$\qquad\qquad \lor\, result'[p] = result[pp]$
      BY $\langle 5\rangle 1$
    $\langle 5\rangle 3.\ q \neq p$
      BY $\langle 4\rangle 1$ DEF a
    $\langle 5\rangle 4.\ Cardinality(result[q]) \in Nat$
      BY $ProcFinite$, $SubsetFinite$, $CardType$, SMT DEF $TypeOK$
    $\langle 5\rangle 5.\ Cardinality(result[q]) = Cardinality(result'[p])$
      BY $\langle 5\rangle 4$, $\langle 4\rangle 1$, $\langle 2\rangle 3$, $\langle 2\rangle 2$, SMT
    $\langle 5\rangle 6.\ result'[p] = result[q]$
      BY $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 5$
    $\langle 5\rangle 7.$ QED
      BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 5\rangle 6$
  $\langle 4\rangle 4.$ QED
    BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, SMT
$\langle 3\rangle 3.$ QED
  BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 3\rangle 1$, $\langle 3\rangle 2$, SMT DEF $Inv1$
$\langle 2\rangle 4.\text{CASE } i \neq k - 1$
  BY $\langle 2\rangle 4$, SMT DEF a, $TypeOK$
$\langle 2\rangle 5.$ QED
  BY $\langle 2\rangle 3$, $\langle 2\rangle 4$
$\langle 1\rangle 2.\ NUnion(A2) \subseteq NUnion(A2')$
  BY $\langle 1\rangle 1$, SMT DEF $NUnion$
$\langle 1\rangle 3.\ IsFiniteSet(NUnion(A2'))$
  BY $ProcFinite$, $SubsetFinite$, SMT DEF $NUnion$, $TypeOK$
$\langle 1\rangle 4.\ IsFiniteSet(NUnion(A2))$

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\mathit{SubsetFinite}$

$\langle 1\rangle 5.$ QED

BY $\langle 1\rangle 2$, $\langle 1\rangle 3$, $\langle 1\rangle 4$, $\mathit{CardType}$, $\mathit{SubsetCardinality}2$

THEOREM $\mathit{Invariance} \triangleq \mathit{Spec} \Rightarrow \Box \mathit{Inv}$

$\langle 1\rangle$ USE DEF $\mathit{ProcSet}$, Pr

$\langle 1\rangle 1.$ $\mathit{Init} \Rightarrow \mathit{Inv}$

$\langle 2\rangle$ SUFFICES ASSUME InitPROVE Inv

OBVIOUS

$\langle 2\rangle$ USE DEF Init, Inv

$\langle 2\rangle 1.$ TypeOK

BY SMT DEF TypeOK

$\langle 2\rangle 2.$ $\mathit{Inv}1$

$\langle 3\rangle 0.$ $\forall i \in \mathit{Nat} : \mathit{Cardinality}(A2[i]) \in \{0,\ i+1\}$

BY $\mathit{EmptySetCardinality}$, SMT DEF $\mathit{Inv}1$, NUnion, PUnion

$\langle 3\rangle 1.$ $\forall p \in \mathit{Proc}$:

$$
\begin{array}{l}
\land\ \mathit{known}[p] \subseteq\ \mathit{PUnion}(\mathit{myVals}) \\
\land\ \mathit{out}[p] \subseteq \mathit{nextout}[p] \\
\land\ \mathit{nextout}[p] \subseteq \mathit{known}[p] \\
\land\ (\mathit{pc}[p] = \text{"e"}) \Rightarrow (\mathit{lnbpart}[p] = \mathit{nbpart}[p]) \\
\land\ \mathit{nbpart}[p] \leq \mathit{Cardinality}(\mathit{NUnion}(A2)) \\
\land\ \mathit{lnbpart}[p] \leq \mathit{nbpart}[p] \\
\land\ \land\ \mathit{pc}[p] = \text{"e"} \\
\quad\ \land\ \mathit{nbpart}[p] = \mathit{Cardinality}(\mathit{NUnion}(A2)) \\
\quad\ \Rightarrow (\mathit{nextout}[p] = \mathit{known}[p]) \\
\land\ \mathit{myVals}[p] \subseteq \mathit{known}[p] \\
\land\ (\mathit{myVals}[p] \neq \{\}) \Rightarrow (\mathit{pc}[p] \neq \text{"a"}) \\
\land\ (\mathit{pc}[p] \neq \text{"a"}) \Rightarrow\ \land\ p \in \mathit{result}[p] \\
\qquad\qquad\qquad\qquad\quad\ \land\ A2[\mathit{Cardinality}(\mathit{result}[p]) - 1] = \mathit{result}[p]
\end{array}
$$

$\langle 4\rangle$ SUFFICES ASSUME NEW $p \in \mathit{Proc}$

PROVE

$$
\begin{array}{l}
\land\ \mathit{known}[p] \subseteq\ \mathit{PUnion}(\mathit{myVals}) \\
\land\ \mathit{out}[p] \subseteq \mathit{nextout}[p] \\
\land\ \mathit{nextout}[p] \subseteq \mathit{known}[p] \\
\land\ (\mathit{pc}[p] = \text{"e"}) \Rightarrow (\mathit{lnbpart}[p] = \mathit{nbpart}[p]) \\
\land\ \mathit{nbpart}[p] \leq \mathit{Cardinality}(\mathit{NUnion}(A2)) \\
\land\ \mathit{lnbpart}[p] \leq \mathit{nbpart}[p] \\
\land\ \land\ \mathit{pc}[p] = \text{"e"} \\
\quad\ \land\ \mathit{nbpart}[p] = \mathit{Cardinality}(\mathit{NUnion}(A2)) \\
\quad\ \Rightarrow (\mathit{nextout}[p] = \mathit{known}[p]) \\
\land\ \mathit{myVals}[p] \subseteq \mathit{known}[p] \\
\land\ (\mathit{myVals}[p] \neq \{\}) \Rightarrow (\mathit{pc}[p] \neq \text{"a"}) \\
\land\ (\mathit{pc}[p] \neq \text{"a"}) \Rightarrow\ \land\ p \in \mathit{result}[p] \\
\qquad\qquad\qquad\qquad\quad\ \land\ A2[\mathit{Cardinality}(\mathit{result}[p]) - 1] = \mathit{result}[p]
\end{array}
$$

OBVIOUS

$\langle 4\rangle 1.$ $\mathit{known}[p] \subseteq\ \mathit{PUnion}(\mathit{myVals})$

BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩2. $out[p] \subseteq nextout[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩3. $nextout[p] \subseteq known[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩4. $(pc[p] = \text{"e"}) \Rightarrow (lnbpart[p] = nbpart[p])$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩5. $nbpart[p] \leq Cardinality(NUnion(A2))$
⟨5⟩ $Cardinality(NUnion(A2)) = 0$
BY ⟨3⟩0, *EmptySetCardinality* DEF *Inv*1, *NUnion*, *PUnion*
⟨5⟩ QED
BY ⟨3⟩0 DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩6. $lnbpart[p] \leq nbpart[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩7. $\land\ pc[p] = \text{"e"}$
$\land\ nbpart[p] = Cardinality(NUnion(A2))$
$\Rightarrow (nextout[p] = known[p])$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩8. $myVals[p] \subseteq known[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩9. $(myVals[p] \neq \{\}) \Rightarrow (pc[p] \neq \text{"a"})$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩10. $(pc[p] \neq \text{"a"}) \Rightarrow\ \land\ p \in result[p]$
$\land\ A2[Cardinality(result[p]) - 1] = result[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨4⟩11. QED
BY ⟨4⟩1, ⟨4⟩2, ⟨4⟩3, ⟨4⟩4, ⟨4⟩5, ⟨4⟩6, ⟨4⟩7, ⟨4⟩8, ⟨4⟩9, ⟨4⟩10
⟨3⟩2. $NUnion(A3) \subseteq PUnion(myVals)$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨3⟩3. $\forall\, i \in Nat : \ \lor\ A2[i] = \{\}$
$\lor\ \exists\, p \in Proc : \ \land\ pc[p] \neq \text{"a"}$
$\land\ i = Cardinality(result[p]) - 1$
$\land\ A2[i] = result[p]$
BY ⟨3⟩0, *EmptySetCardinality*, *SMT* DEF *Inv*1, *NUnion*, *PUnion*
⟨3⟩4. QED
BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3 DEF *Inv*1
⟨2⟩3. *Inv*2
BY *SMT* DEF *Inv*2
⟨2⟩4. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3

⟨1⟩2. $Inv \land [Next]_{vars} \Rightarrow Inv'$
⟨2⟩ SUFFICES ASSUME Inv, $[Next]_{vars}$
PROVE Inv'
OBVIOUS

$\langle 2 \rangle$ USE DEF *Inv*
$\langle 2 \rangle 1.$ ASSUME NEW $p \in Proc$, $pc[p] \neq$ "a"
    PROVE $p \in NUnion(A2)$
  $\langle 3 \rangle 1.$ $p \in result[p]$
    BY $\langle 2 \rangle 1$ DEF *Inv*1
  $\langle 3 \rangle 2.$ $\land\ IsFiniteSet(result[p])$
    $\land\ Cardinality(result[p]) \in Nat$
    BY *ProcFinite*, *SubsetFinite*, *CardType*, *SMT* DEF *TypeOK*
  $\langle 3 \rangle 3.$ $Cardinality(result[p]) - 1 \in Nat$
    BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, *NonEmptySetCardinality*, *SMT*
  $\langle 3 \rangle 4.$ $result[p] = A2[Cardinality(result[p]) - 1]$
    BY $\langle 2 \rangle 1$ DEF *Inv*1
  $\langle 3 \rangle 5.$ QED
    BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$, $\langle 3 \rangle 4$ DEF *NUnion*
$\langle 2 \rangle 2.$ $\land\ IsFiniteSet(NUnion(A2))$
  $\land\ Cardinality(NUnion(A2)) \in Nat$
  BY *ProcFinite*, *SubsetFinite*, *CardType*, *SMT* DEF *TypeOK*, *NUnion*
$\langle 2 \rangle 3.$ $PA3 \subseteq [Nat \rightarrow \text{SUBSET } Val]$
  $\langle 3 \rangle$ SUFFICES ASSUME NEW $wa \in WriterAssignment$
      PROVE $PV(wa) \in [Nat \rightarrow \text{SUBSET } Val]$
    BY DEF *PA*3
  $\langle 3 \rangle 1.$ $wa \in [Nat \rightarrow Proc \cup \{NotAProc\}]$
    BY DEF *WriterAssignment*
  $\langle 3 \rangle 2.$ $\land\ \forall\, i \in Nat\ : A3[i] \in \text{SUBSET } Val$
    $\land\ \forall\, p \in Proc : known[p] \in \text{SUBSET } Val$
    BY DEF *TypeOK*
  $\langle 3 \rangle 3.$ QED
    BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, *SMT* DEF *PV*
$\langle 2 \rangle 4.$ ASSUME $vars' = vars$
    PROVE Inv'
  $\langle 3 \rangle$ USE $\langle 2 \rangle 4$
  $\langle 3 \rangle 1.$ $TypeOK'$
    BY *SMT* DEF *TypeOK*, *vars*
  $\langle 3 \rangle 2.$ $Inv1'$
    BY *SMT* DEF *Inv*1, *vars*
  $\langle 3 \rangle 3.$ $Inv2'$
    $\langle 4 \rangle$ SUFFICES $PA3' = PA3$
      BY DEF *Inv*2, *vars*
    $\langle 4 \rangle 1.$ ASSUME NEW *wa*
        PROVE $PV(wa) = PV(wa)'$
      $\langle 5 \rangle$ $A3' = A3 \land known' = known$
        BY DEF *vars*
      $\langle 5 \rangle$ QED
        BY DEF *PV*
    $\langle 4 \rangle 2.$ $WriterAssignment' = WriterAssignment$

BY SMT DEF $WriterAssignment$, $ReadyToWrite$, $vars$

⟨4⟩3. QED

BY ⟨4⟩1, ⟨4⟩2 DEF $PA3$

⟨3⟩4. QED

BY ⟨3⟩1, ⟨3⟩2, ⟨3⟩3

⟨2⟩5. ASSUME NEW $p \in Proc$, $a(p)$

PROVE Inv'

⟨3⟩ USE ⟨2⟩5

⟨3⟩1. $TypeOK'$

BY DEF $TypeOK$, a — SMT worked on 14 Feb 2013, SMT & $Z3$ timed out on 31 May 2013

⟨3⟩2. $Inv1'$

⟨4⟩1. $p \in result'[p]$

BY SMT DEF $TypeOK$, a

⟨4⟩2. $\land\ A2'[Cardinality(result'[p]) - 1] = result'[p]$

$\land\ Cardinality(result'[p]) \in Nat$

$\land\ Cardinality(result'[p]) > 0$

$\land\ IsFiniteSet(result'[p])$

⟨5⟩1. $\land\ Cardinality(result'[p]) \in Nat$

$\land\ IsFiniteSet(result'[p])$

BY $ProcFinite$, $SubsetFinite$, $CardType$, $TypeOK'$, SMT DEF $TypeOK$

⟨5⟩2. $result'[p] \neq \{\}$

BY ⟨4⟩1

⟨5⟩3. $Cardinality(result'[p]) > 0$

BY ⟨5⟩1, ⟨5⟩2, $NonEmptySetCardinality$, SMT

⟨5⟩4. QED

BY ⟨5⟩1, ⟨5⟩3, SMT DEF a, $TypeOK$

⟨4⟩3. ASSUME NEW $q \in Proc$

PROVE $Inv1!1!(q)'$

⟨5⟩1. $Inv1!1!(q)!1'$

BY SMT DEF $Inv1$, $TypeOK$, a

⟨5⟩2. $Inv1!1!(q)!2'$

BY SMT DEF $Inv1$, $TypeOK$, a

⟨5⟩3. $Inv1!1!(q)!3'$

BY SMT DEF $Inv1$, $TypeOK$, a

⟨5⟩4. $Inv1!1!(q)!4'$

BY SMT DEF $Inv1$, $TypeOK$, a

⟨5⟩5. $Inv1!1!(q)!5'$

⟨6⟩1. $\land\ \forall i \in Nat : Cardinality(A2[i]) \in Nat$

$\land\ Cardinality(NUnion(A2)) \in Nat$

$\land\ Cardinality(NUnion(A2')) \in Nat$

$\land\ nbpart'[q] \in Nat$

⟨7⟩1. $nbpart'[q] \in Nat$

BY $TypeOK'$ DEF $TypeOK$

⟨7⟩2. $\forall i \in Nat : Cardinality(A2[i]) \in Nat$

BY $ProcFinite$, $SubsetFinite$, $CardType$, SMT DEF $TypeOK$

$\langle 7 \rangle 3.$ QED
BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $TypeOK'$, $A2monotonic$, SMT
$\langle 6 \rangle 2.$ $nbpart[q] \leq Cardinality(NUnion(A2))$
BY SMT DEF $Inv1$
$\langle 6 \rangle 3.$ $nbpart' = nbpart$
BY DEF a
$\langle 6 \rangle 4.$ QED
BY $\langle 6 \rangle 1$, $A2monotonic$, $TypeOK'$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, SMT
$\langle 5 \rangle 6.$ $Inv1!1!(q)!6'$
BY SMT DEF $Inv1$, $TypeOK$, a
$\langle 5 \rangle 7.$ $Inv1!1!(q)!7'$
$\langle 6 \rangle 1.$CASE $q \neq p$
$\langle 7 \rangle 1.$ $\land\ pc'[q] = pc[q]$
$\land\ nextout'[q] = nextout[q]$
$\land\ known'[q] = known[q]$
BY $\langle 6 \rangle 1$ DEF a, $TypeOK$
$\langle 7 \rangle 2.$ $\land\ nbpart'[q] = nbpart[q]$
$\land\ nbpart[q] \in Nat$
$\land\ nbpart'[q] \in Nat$
BY DEF a, $TypeOK$
$\langle 7 \rangle 3.$ $nbpart[q] \leq Cardinality(NUnion(A2))$
BY DEF $Inv1$
$\langle 7 \rangle 4.$ $nbpart'[q] = Cardinality(NUnion(A2'))$
$\Rightarrow nbpart[q] = Cardinality(NUnion(A2))$
BY $A2monotonic$, $TypeOK'$, $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $\langle 7 \rangle 3$, SMT
$\langle 7 \rangle 5$ QED
BY $\langle 7 \rangle 1$, $\langle 7 \rangle 4$ DEF $Inv1$, a
$\langle 6 \rangle 2.$CASE $q = p$
BY $\langle 6 \rangle 2$, SMT DEF $Inv1$, $TypeOK$, a
$\langle 6 \rangle 3.$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle 8.$ $Inv1!1!(q)!8'$
BY SMT DEF $Inv1$, $TypeOK$, a
$\langle 5 \rangle 9.$ $Inv1!1!(q)!9'$
BY SMT DEF $Inv1$, $TypeOK$, a
$\langle 5 \rangle 10.$ $Inv1!1!(q)!10'$
$\langle 6 \rangle 3.$CASE $q \neq p$
$\langle 7 \rangle 1.$ $\land\ pc'[q] = pc[q]$
$\land\ result'[q] = result[q]$
BY $\langle 6 \rangle 3$ DEF a, $TypeOK$
$\langle 7 \rangle 2.$ SUFFICES ASSUME $pc[q] \neq$ "a"
PROVE $A2'[Cardinality(result[q]) - 1] = result[q]$
BY $\langle 7 \rangle 1$, SMT DEF $Inv1$
$\langle 7 \rangle 3.$ $\forall\, qq \in Proc \setminus \{p\}$:
$\lor\ Cardinality(result[qq]) \neq Cardinality(result'[p])$

$\lor\ result'[p] = result[qq]$

BY SMT DEF a, $TypeOK$

$\langle 7\rangle 4.$ CASE $Cardinality(result[q]) \neq Cardinality(result'[p])$

$\langle 8\rangle 1.$ $\land\ IsFiniteSet(result[q])$
$\land\ Cardinality(result[q]) \in Nat$

BY $ProcFinite$, $SubsetFinite$, $CardType$, SMT DEF $TypeOK$

$\langle 8\rangle 2.$ $q \in result[q]$

BY $\langle 7\rangle 2$, SMT DEF $Inv1$

$\langle 8\rangle 3.$ $Cardinality(result[q]) - 1 \in Nat$

BY $\langle 8\rangle 1$, $\langle 8\rangle 2$, $NonEmptySetCardinality$, SMT

$\langle 8\rangle 4.$ $A2[Cardinality(result[q]) - 1] = result[q]$

BY $\langle 7\rangle 2$, SMT DEF $Inv1$

$\langle 8\rangle 5.$ $Cardinality(result[q]) - 1 \neq Cardinality(result'[p]) - 1$

BY $\langle 7\rangle 4$, $\langle 8\rangle 1$, $\langle 4\rangle 2$, SMT

$\langle 8\rangle 6.$ $Cardinality(result'[p]) - 1 \in Nat$

BY $\langle 4\rangle 2$, SMT

$\langle 8\rangle 7.$ $A2'[Cardinality(result[q]) - 1] = A2[Cardinality(result[q]) - 1]$

BY $\langle 8\rangle 3$, $\langle 8\rangle 6$, $\langle 8\rangle 5$, SMT DEF a, $TypeOK$

$\langle 8\rangle 8.$ QED

BY $\langle 8\rangle 4$, $\langle 8\rangle 7$

$\langle 7\rangle 5.$ CASE $result'[p] = result[q]$

$\langle 8\rangle 1.$ $A2[Cardinality(result[q]) - 1] = result[q]$

BY $\langle 7\rangle 2$, SMT DEF $Inv1$

$\langle 8\rangle 2.$ QED

BY $\langle 4\rangle 2$, $\langle 8\rangle 1$, $\langle 7\rangle 5$, SMT

$\langle 7\rangle 6.$ QED

BY $\langle 7\rangle 3$, $\langle 7\rangle 4$, $\langle 7\rangle 5$, $\langle 6\rangle 3$, SMT

$\langle 6\rangle 4.$ CASE $q = p$

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 6\rangle 4$

$\langle 6\rangle 5.$ QED

BY $\langle 6\rangle 3$, $\langle 6\rangle 4$

$\langle 5\rangle 11.$ QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, $\langle 5\rangle 7$, $\langle 5\rangle 8$, $\langle 5\rangle 9$, $\langle 5\rangle 10$,
SMT DEF $Inv1$

$\langle 4\rangle 4.$ $NUnion(A3') \subseteq PUnion(myVals')$

BY SMT DEF $Inv1$, $TypeOK$, a

$\langle 4\rangle 5.$ ASSUME NEW $i \in Nat$
PROVE $\lor\ A2'[i] = \{\}$
$\lor\ \exists\, q \in Proc : \land\ pc'[q] \neq \text{"a"}$
$\land\ i = Cardinality(result'[q]) - 1$
$\land\ A2'[i] = result'[q]$

$\langle 5\rangle 1.$ CASE $i = Cardinality(result'[p]) - 1$

$\langle 6\rangle 1.$ $pc'[p] \neq \text{"a"}$

BY DEF a, $TypeOK$

$\langle 6\rangle 2.$ $A2'[i] = result'[p]$

BY $\langle 4 \rangle 2$, $\langle 5 \rangle 1$
$\langle 6 \rangle 3$. QED
BY $\langle 5 \rangle 1$, $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle 2$.CASE $i \neq Cardinality(result'[p]) - 1$
$\langle 6 \rangle 1$. $A2'[i] = A2[i]$
BY $\langle 5 \rangle 2$, $\langle 4 \rangle 2$, SMT DEF a, $TypeOK$
$\langle 6 \rangle 2$.CASE $A2[i] = \{\}$
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 6 \rangle 3$.CASE $\exists\, q \in Proc : \begin{array}{l} \land\, pc[q] \neq \text{“a”} \\ \land\, i = Cardinality(result[q]) - 1 \\ \land\, A2[i] = result[q] \end{array}$
$\langle 7 \rangle 1$. PICK $q \in Proc : \begin{array}{l} \land\, pc[q] \neq \text{“a”} \\ \land\, i = Cardinality(result[q]) - 1 \\ \land\, A2[i] = result[q] \end{array}$
BY $\langle 6 \rangle 3$
$\langle 7 \rangle 2$. $\begin{array}{l} \land\, pc'[q] = pc[q] \\ \land\, result'[q] = result[q] \end{array}$
BY $\langle 7 \rangle 1$ DEF a, $TypeOK$
$\langle 7 \rangle 3$. $A2'[i] = A2[i]$
BY $\langle 4 \rangle 2$, $\langle 5 \rangle 2$, SMT DEF $TypeOK$, a
$\langle 7 \rangle 4$. QED
BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $\langle 7 \rangle 3$, SMT
$\langle 6 \rangle 4$. QED
BY $\langle 6 \rangle 2$, $\langle 6 \rangle 3$, SMT DEF $Inv1$
$\langle 5 \rangle 3$. QED
BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$
$\langle 4 \rangle 6$. QED
BY $\langle 4 \rangle 3$, $\langle 4 \rangle 4$, $\langle 4 \rangle 5$ DEF $Inv1$
$\langle 3 \rangle 3$. $Inv2'$
$\langle 4 \rangle$ SUFFICES $PA3' = PA3$
BY DEF $Inv2$, a
$\langle 4 \rangle 1$. ASSUME NEW wa
PROVE $PV(wa) = PV(wa)'$
$\langle 5 \rangle$ $A3' = A3 \land known' = known$
BY DEF a
$\langle 5 \rangle$ QED
BY DEF PV
$\langle 4 \rangle 2$. $WriterAssignment' = WriterAssignment$
$\langle 5 \rangle 1$. ASSUME NEW $q \in Proc$
PROVE $(pc[q] = \text{“d”}) = (pc'[q] = \text{“d”})$
$\langle 6 \rangle 1$. $pc[q] = \text{“d”} \Rightarrow p \neq q$
BY DEF a
$\langle 6 \rangle 2$. $pc'[q] = \text{“d”} \Rightarrow p \neq q$
BY DEF a, $TypeOK$
$\langle 6 \rangle 3$. $p \neq q \Rightarrow pc'[q] = pc[q]$

BY DEF a, TypeOK

$\langle 6\rangle 4.$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$

$\langle 5\rangle 2.$ $\forall\, i \in \mathit{Nat},\ q \in \mathit{Proc} : \mathit{ReadyToWrite}(i,\ q) = \mathit{ReadyToWrite}(i,\ q)'$

BY $\langle 5\rangle 1$, SMT DEF $\mathit{ReadyToWrite}$, a

$\langle 5\rangle 3.$ QED

BY $\langle 5\rangle 2$, SMT DEF $\mathit{WriterAssignment}$

$\langle 4\rangle 3.$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $\mathit{PA}3$

$\langle 3\rangle 4.$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle 6.$ ASSUME NEW $p \in \mathit{Proc}$, $b(p)$

PROVE Inv'

$\langle 3\rangle$ USE $\langle 2\rangle 6$

$\langle 3\rangle 1.$ TypeOK'

$\langle 4\rangle 1.$ $\mathit{TypeOK}!1'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 2.$ $\mathit{TypeOK}!2'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 3.$ $\mathit{TypeOK}!3'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 4.$ $\mathit{TypeOK}!4'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 5.$ $\mathit{TypeOK}!5'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 6.$ $\mathit{TypeOK}!6'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 7.$ $\mathit{TypeOK}!7'$

BY $\langle 2\rangle 2$, SMT DEF TypeOK, b

$\langle 4\rangle 8.$ $\mathit{TypeOK}!8'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 9.$ $\mathit{TypeOK}!9'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 10.$ $\mathit{TypeOK}!10'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 11.$ $\mathit{TypeOK}!11'$

BY SMT DEF TypeOK, b

$\langle 4\rangle 12.$ QED

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

$\langle 3\rangle 2.$ $\mathit{Inv}1'$

$\langle 4\rangle 1.$ ASSUME NEW $q \in \mathit{Proc}$

PROVE $\mathit{Inv}1!1!(q)'$

$\langle 5\rangle 1.$ $\mathit{Inv}1!1!(q)!1'$

BY SMT DEF $\mathit{Inv}1$, TypeOK, b, PUnion

$\langle 5\rangle 2.$ $Inv1!1!(q)!2'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 3.$ $Inv1!1!(q)!3'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 4.$ $Inv1!1!(q)!4'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 5.$ $nbpart'[q] \leq Cardinality(NUnion(A2'))$
$\langle 6\rangle 1.$CASE $q \neq p$
BY $\langle 6\rangle 1$, SMT DEF b, $TypeOK$, $Inv1$
$\langle 6\rangle 2.$CASE $q = p$
$\langle 7\rangle$ $nbpart'[q] = Cardinality(NUnion(A2))$
BY $\langle 6\rangle 2$, SMT DEF b, $TypeOK$
$\langle 7\rangle$ QED
BY $TypeOK'$, $\langle 6\rangle 2$, SMT DEF b, $TypeOK$
$\langle 6\rangle 3.$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle 6.$ $lnbpart'[q] \leq nbpart'[q]$
$\langle 6\rangle 1.$CASE $q \neq p$
BY $\langle 6\rangle 1$, SMT DEF b, $TypeOK$, $Inv1$
$\langle 6\rangle 2.$CASE $q = p$
$\langle 7\rangle$ $\land\ nbpart'[q] = Cardinality(NUnion(A2))$
$\land\ lnbpart'[q] = lnbpart[q]$
BY $\langle 6\rangle 2$, SMT DEF b, $TypeOK$
$\langle 7\rangle$ $\land\ lnbpart[q] \leq nbpart[q]$
$\land\ nbpart[q] \leq Cardinality(NUnion(A2))$
BY DEF $Inv1$
$\langle 7\rangle$ $\land\ nbpart'[q] \in Nat$
$\land\ nbpart[q] \in Nat$
$\land\ lnbpart[q] \in Nat$
BY $TypeOK'$ DEF $TypeOK$
$\langle 7\rangle$ QED
BY SMT
$\langle 6\rangle 3.$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle 7.$ $Inv1!1!(q)!7'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 8.$ $Inv1!1!(q)!8'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 9.$ $Inv1!1!(q)!9'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 10.$ $Inv1!1!(q)!10'$
BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 5\rangle 11.$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, $\langle 5\rangle 7$, $\langle 5\rangle 8$, $\langle 5\rangle 9$, $\langle 5\rangle 10$,
SMT DEF $Inv1$

$\langle 4\rangle 2.$ $NUnion(A3') \subseteq PUnion(myVals')$
  BY SMT DEF $TypeOK$, $Inv1$, b, $PUnion$
$\langle 4\rangle 3.$ $Inv1!3'$
  BY SMT DEF $Inv1$, $TypeOK$, b
$\langle 4\rangle 4.$ QED
  BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $Inv1$
$\langle 3\rangle 3.$ $Inv2'$
  $\langle 4\rangle$ SUFFICES $PA3' = PA3$
    BY DEF $Inv2$, b
  $\langle 4\rangle 1.$ $WriterAssignment' = WriterAssignment$
    $\langle 5\rangle 1.$ ASSUME NEW $q \in Proc$
        PROVE $(pc[q] = \text{"d"}) = (pc'[q] = \text{"d"})$
      $\langle 6\rangle 1.$ $pc[q] = \text{"d"} \Rightarrow p \neq q$
        BY DEF b
      $\langle 6\rangle 2.$ $pc'[q] = \text{"d"} \Rightarrow p \neq q$
        BY DEF b, $TypeOK$
      $\langle 6\rangle 3.$ $p \neq q \Rightarrow pc'[q] = pc[q]$
        BY DEF b, $TypeOK$
      $\langle 6\rangle 4.$ QED
        BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$
    $\langle 5\rangle 2.$ $\forall\, i \in Nat,\ q \in Proc : ReadyToWrite(i,\ q) = ReadyToWrite(i,\ q)'$
      BY $\langle 5\rangle 1$, SMT DEF $ReadyToWrite$, b
    $\langle 5\rangle 3.$ QED
      BY $\langle 5\rangle 2$, SMT DEF $WriterAssignment$
  $\langle 4\rangle 2.$ ASSUME NEW $wa \in WriterAssignment$
      PROVE $PV(wa) = PV(wa)'$
    $\langle 5\rangle 1.$ $A3' = A3$
      BY DEF b
    $\langle 5\rangle 2.$ ASSUME $wa \in WriterAssignment$, NEW $i \in Nat$, $wa[i] \neq NotAProc$
        PROVE $known'[wa[i]] = known[wa[i]]$
      $\langle 6\rangle 1.$ $wa[i] \in Proc$
        BY $\langle 5\rangle 2$, SMT DEF $WriterAssignment$
      $\langle 6\rangle 2.$ $ReadyToWrite(i,\ wa[i])$
        BY $\langle 5\rangle 2$, $\langle 6\rangle 1$, SMT DEF $WriterAssignment$
      $\langle 6\rangle 3.$ $pc[wa[i]] = \text{"d"}$
        BY $\langle 6\rangle 2$ DEF $ReadyToWrite$
      $\langle 6\rangle 4.$ $wa[i] \neq p$
        BY $\langle 6\rangle 3$ DEF b
      $\langle 6\rangle 5.$ QED
        BY $\langle 6\rangle 4$, SMT DEF $TypeOK$, b
    $\langle 5\rangle 3.$ ASSUME NEW $i \in Nat$, $wa \in WriterAssignment$
        PROVE (IF $wa[i] = NotAProc$ THEN $A3[i]$ ELSE $known[wa[i]]) =$
            (IF $wa[i] = NotAProc$ THEN $A3'[i]$ ELSE $known'[wa[i]])$
      $\langle 6\rangle 1.$CASE $wa[i] = NotAProc$
        BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 1$

$\langle 6 \rangle 2.$CASE $wa[i] \neq NotAProc$
BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 6 \rangle 2$
$\langle 6 \rangle 3.$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle 4.$ QED
BY $\langle 5 \rangle 3$ DEF PV
$\langle 4 \rangle 3.$ QED
BY $\langle 4 \rangle 2$, $\langle 4 \rangle 1$ DEF $PA3$
$\langle 3 \rangle 4.$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$, $\langle 3 \rangle 3$
$\langle 2 \rangle 7.$ ASSUME NEW $p \in Proc$, $c(p)$
PROVE Inv'
$\langle 3 \rangle$ USE $\langle 2 \rangle 7$
$\langle 3 \rangle 1.$ $TypeOK'$
BY SMT DEF $TypeOK$, c, $NUnion$
$\langle 3 \rangle 2.$ $Inv1'$
$\langle 4 \rangle 1.$ ASSUME NEW $q \in Proc$
PROVE $Inv1!1!(q)'$
$\langle 5 \rangle 1.$ $known'[q] \subseteq PUnion(myVals')$
$\langle 6 \rangle 1.$CASE $p \neq q$
BY $\langle 6 \rangle 1$, SMT DEF c, $TypeOK$, $Inv1$, $PUnion$
$\langle 6 \rangle 2.$CASE $p = q$
$\langle 7 \rangle 1.$ $known[p] \subseteq PUnion(myVals)$
BY DEF $Inv1$
$\langle 7 \rangle 2.$ $NUnion(A3) \subseteq PUnion(myVals)$
BY SMT DEF c, $Inv1$
$\langle 7 \rangle 3.$ QED
BY $\langle 6 \rangle 2$, $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, SMT DEF c, $TypeOK$
$\langle 6 \rangle 3.$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle 2.$ $Inv1!1!(q)!2'$
BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 3.$ $Inv1!1!(q)!3'$
BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 4.$ $Inv1!1!(q)!4'$
BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 5.$ $Inv1!1!(q)!5'$
BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 6.$ $Inv1!1!(q)!6'$
$\langle 6 \rangle 1.$CASE $q \neq p$
BY $\langle 6 \rangle 1$, SMT DEF $Inv1$, $TypeOK$, c
$\langle 6 \rangle 2.$CASE $q = p$
BY $\langle 6 \rangle 2$, SMT DEF $Inv1$, $TypeOK$, c
$\langle 6 \rangle 3.$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$

$\langle 5 \rangle 7.\ Inv1!1!(q)!7'$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 8.\ Inv1!1!(q)!8'$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 9.\ Inv1!1!(q)!9'$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 10.\ Inv1!1!(q)!10'$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 5 \rangle 11.$ QED
  BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$, $\langle 5 \rangle 4$, $\langle 5 \rangle 5$, $\langle 5 \rangle 6$, $\langle 5 \rangle 7$, $\langle 5 \rangle 8$, $\langle 5 \rangle 9$, $\langle 5 \rangle 10$,
    SMT DEF $Inv1$
$\langle 4 \rangle 2.\ NUnion(A3') \subseteq PUnion(myVals')$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 4 \rangle 3.\ Inv1!3'$
  BY SMT DEF $Inv1$, $TypeOK$, c
$\langle 4 \rangle 4.$ QED
  BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF $Inv1$
$\langle 3 \rangle 3.\ Inv2'$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $q \in Proc$, NEW $P \in PA3'$
    PROVE $nextout'[q] \subseteq NUnion(P)$
  BY DEF $Inv2$
$\langle 4 \rangle 1.$CASE $notKnown'[p] \neq \{\}$
$\langle 5 \rangle 1.\ \wedge pc[p] = \text{“c”}$
  $\wedge\ lnbpart' = [lnbpart$ EXCEPT $![p] = nbpart[p]]$
  $\wedge\ known' = [known$ EXCEPT $![p] =$
    $known[p] \cup$ UNION $\{A3[i] : i \in Nat\}]$
  $\wedge\ notKnown' = [notKnown$ EXCEPT $![p] =$
    $\{i \in 0 \,..\, (nbpart[p] - 1) :$
      $known'[p] \neq A3[i]\}]$
  $\wedge\ notKnown'[p] \neq \{\}$
  $\wedge\ pc' = [pc$ EXCEPT $![p] = \text{“d”}]$
  $\wedge$ UNCHANGED $nextout$
  $\wedge$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out \rangle$
  BY $\langle 4 \rangle 1$ DEF c, $NUnion$
$\langle 5 \rangle 2.$CASE $P \in PA3$
  BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, SMT DEF $Inv2$
$\langle 5 \rangle 3.$CASE $P \in PA3' \setminus PA3$
$\langle 6 \rangle 1.$ PICK $i \in Nat :$
  $\wedge\ ReadyToWrite(i, p)'$
  $\wedge\ P[i] = known'[p]$
  $\wedge\ \exists\, wa \in WriterAssignment' : \wedge\ wa[i] = p$
    $\wedge\ P = PV(wa)'$
$\langle 7 \rangle 1.$ PICK $wa \in WriterAssignment' : \wedge\ P = PV(wa)'$
  $\wedge\ PV(wa)' \in PA3'$
  $\wedge\ PV(wa)' \notin PA3$

BY $\langle 5\rangle 3$ DEF $PA3$

$\langle 7\rangle 2.$CASE $wa \notin WriterAssignment$

$\langle 8\rangle 1.$ PICK $i \in Nat : \land\, wa[i] \in Proc$
$\qquad\qquad\qquad\qquad\quad \land\, \neg ReadyToWrite(i,\ wa[i])$
$\qquad\qquad\qquad\qquad\quad \land\, ReadyToWrite(i,\ wa[i])'$

BY $\langle 7\rangle 2$, SMT DEF $WriterAssignment$

$\langle 8\rangle 2.$ $wa[i] = p$

BY $\langle 8\rangle 1$, SMT DEF c, $TypeOK$, $ReadyToWrite$

$\langle 8\rangle 3.$ QED

BY $\langle 8\rangle 1$, $\langle 8\rangle 2$, $\langle 7\rangle 1$, $NotAProcProp$ DEF PV

$\langle 7\rangle 3.$CASE $wa \in WriterAssignment \land PV(wa) \neq PV(wa)'$

$\langle 8\rangle 1.$ PICK $i \in Nat : PV(wa)[i] \neq PV(wa)'[i]$

$\langle 9\rangle \land PV(wa) = [i \in Nat \mapsto PV(wa)[i]]$
$\quad\ \land PV(wa)' = [i \in Nat \mapsto PV(wa)'[i]]$

BY DEF PV

$\langle 9\rangle$ QED

BY $\langle 7\rangle 3$

$\langle 8\rangle 2.$ $wa[i] = p$

BY $\langle 8\rangle 1$, SMT DEF c, $TypeOK$, PV

$\langle 8\rangle 3.$ $ReadyToWrite(i,\ p)'$

BY $\langle 8\rangle 2$, SMT DEF $WriterAssignment$

$\langle 8\rangle 4.$ $PV(wa)'[i] = known'[wa[i]]$

BY $\langle 8\rangle 2$, $NotAProcProp$ DEF PV

$\langle 8\rangle 5.$ QED

BY $\langle 8\rangle 2$, $\langle 8\rangle 3$, $\langle 8\rangle 4$, $\langle 7\rangle 1$

$\langle 7\rangle 4.$ QED

BY $\langle 7\rangle 1$, $\langle 7\rangle 2$, $\langle 7\rangle 3$ DEF $PA3$

$\langle 6\rangle$ DEFINE $Q \triangleq [P$ EXCEPT $![i] = A3[i]]$

$\langle 6\rangle 2.$ $Q \in PA3$

$\langle 7\rangle 1.$ PICK $wa \in WriterAssignment' : \land\, wa[i] = p$
$\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\, P = PV(wa)'$

BY $\langle 6\rangle 1$

$\langle 7\rangle$ DEFINE $za \triangleq [wa$ EXCEPT $![i] = NotAProc]$

$\langle 7\rangle 2.$ ASSUME NEW $j \in Nat$, $j \neq i$
PROVE $wa[j] \neq p \ \land\ PV(wa)'[j] = PV(wa)[j]$

$\langle 8\rangle 1.$ $wa[j] \neq p$

BY $\langle 7\rangle 1$, $\langle 7\rangle 2$, SMT DEF $WriterAssignment$

$\langle 8\rangle 2.$ QED

BY $\langle 8\rangle 1$, SMT DEF PV, c, $TypeOK$

$\langle 7\rangle 3.$ $za \in WriterAssignment$

$\langle 8\rangle 1.$ $wa \in [Nat \rightarrow Proc \cup \{NotAProc\}]$

BY DEF $WriterAssignment$

$\langle 8\rangle 2.$ $za \in [Nat \rightarrow Proc \cup \{NotAProc\}]$

BY $\langle 8\rangle 1$

$\langle 8\rangle$ SUFFICES ASSUME NEW $j \in Nat$, $za[j] \in Proc$

PROVE $\wedge\ ReadyToWrite(j,\ za[j])$
$\wedge\ \forall\, k \in Nat \setminus \{j\} : za[k] \neq za[j]$
BY $\langle 8\rangle 2$ DEF $WriterAssignment$
$\langle 8\rangle 4.$CASE $j = i$
BY $\langle 8\rangle 1$, $\langle 8\rangle 4$, $NotAProcProp$
$\langle 8\rangle 5.$CASE $j \neq i$
$\langle 9\rangle 1.$ $za[j] = wa[j]$
BY $\langle 8\rangle 1$, $\langle 8\rangle 5$
$\langle 9\rangle 2.$ $za[j] \neq p$
BY $\langle 8\rangle 5$, $\langle 9\rangle 1$, $\langle 7\rangle 1$, SMT DEF $WriterAssignment$
$\langle 9\rangle 3.$ $ReadyToWrite(j,\ za[j])$
$\langle 10\rangle$ $ReadyToWrite(j,\ za[j])'$
BY $\langle 9\rangle 1$, SMT DEF $WriterAssignment$
$\langle 10\rangle$ QED
BY $\langle 9\rangle 2$, SMT DEF c, $TypeOK$, $ReadyToWrite$
$\langle 9\rangle 4.$ ASSUME NEW $k \in Nat \setminus \{j\}$
PROVE $za[k] \neq za[j]$
$\langle 10\rangle$CASE $k = i$
BY $\langle 8\rangle 1$, $NotAProcProp$, SMT
$\langle 10\rangle$CASE $k \neq i$
BY $\langle 9\rangle 1$, $\langle 9\rangle 4$, $\langle 8\rangle 1$, SMT DEF $WriterAssignment$
$\langle 10\rangle$ QED
OBVIOUS
$\langle 9\rangle 5.$ QED
BY $\langle 9\rangle 3$, $\langle 9\rangle 4$
$\langle 8\rangle 6.$ QED
BY $\langle 8\rangle 4$, $\langle 8\rangle 5$
$\langle 7\rangle 4.$ $Q = PV(za)$
$\langle 8\rangle$ $\wedge\ PV(za) = [j \in Nat \mapsto PV(za)[j]]$
$\wedge\ PV(wa)' = [j \in Nat \mapsto PV(wa)'[j]]$
BY DEF PV
$\langle 8\rangle$ $wa = [j \in Nat \mapsto wa[j]]$
BY DEF $WriterAssignment$
$\langle 8\rangle$ $za = [j \in Nat \mapsto za[j]]$
OBVIOUS
$\langle 8\rangle$ $PV(za)[i] = A3[i]$
BY $NotAProcProp$ DEF PV
$\langle 8\rangle$ ASSUME NEW $j \in Nat$, $j \neq i$
PROVE $PV(za)[j] = PV(wa)[j]$
BY DEF PV
$\langle 8\rangle$ HIDE DEF za
$\langle 8\rangle$ QED
BY $\langle 7\rangle 1$, $\langle 7\rangle 2$, $NotAProcProp$
$\langle 7\rangle 5.$ QED
BY $\langle 7\rangle 3$, $\langle 7\rangle 4$ DEF $PA3$

$\langle 6 \rangle 3.\ nextout[q] \subseteq NUnion(Q)$
BY $\langle 6 \rangle 2$ DEF $Inv2$
$\langle 6 \rangle 4.\ A3[i] \subseteq known'[p]$
BY $\langle 5 \rangle 1$, SMT DEF $TypeOK$
$\langle 6 \rangle 5.\ Q[i] \subseteq P[i]$
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, $\langle 6 \rangle 4$, $\langle 2 \rangle 3$, SMT
$\langle 6 \rangle 6.\ NUnion(Q) \subseteq NUnion(P)$
$\langle 7 \rangle$ SUFFICES ASSUME NEW $j \in Nat$
PROVE $Q[j] \subseteq P[j]$
BY DEF $NUnion$
$\langle 7 \rangle$CASE $j \neq i$
$\langle 8 \rangle\ P = [k \in Nat \mapsto P[k]]$
BY $\langle 5 \rangle 3$ DEF $PA3$, PV
$\langle 8 \rangle$ QED
OBVIOUS
$\langle 7 \rangle$ QED
BY $\langle 6 \rangle 5$
$\langle 6 \rangle 7.\ nextout'[q] = nextout[q]$
BY $\langle 5 \rangle 1$
$\langle 6 \rangle 8.$ QED
BY $\langle 6 \rangle 3$, $\langle 6 \rangle 6$, $\langle 6 \rangle 7$, SMT
$\langle 5 \rangle 4$ QED
BY $\langle 5 \rangle 2$, $\langle 5 \rangle 3$
$\langle 4 \rangle 2.$CASE $\land\ notKnown'[p] = \{\}$
$\land\ nbpart[p] = Cardinality(NUnion(A2))$
$\langle 5 \rangle 1.\ \land\ pc[p] =$ "c"
$\land\ lnbpart' = [lnbpart$ EXCEPT $![p] = nbpart[p]]$
$\land\ known' = [known$ EXCEPT $![p] =$
$known[p] \cup$ UNION $\{A3[i] : i \in Nat\}]$
$\land\ notKnown' = [notKnown$ EXCEPT $![p] =$
$\{i \in 0 \,..\, (nbpart[p] - 1) :$
$known'[p] \neq A3[i]\}]$
$\land\ notKnown'[p] = \{\}$
$\land\ nbpart[p] = Cardinality(NUnion(A2))$
$\land\ nextout' = [nextout$ EXCEPT $![p] = known'[p]]$
$\land\ pc' = [pc$ EXCEPT $![p] =$ "e"$]$
$\land$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out \rangle$
BY $\langle 4 \rangle 2$ DEF c, $NUnion$
$\langle 5 \rangle 2.\ PA3' = PA3$
$\langle 6 \rangle 1.$ ASSUME NEW $i \in Nat$, NEW $r \in Proc$
PROVE $ReadyToWrite(i, r)' = ReadyToWrite(i, r)$
BY $\langle 5 \rangle 1$, SMT DEF $ReadyToWrite$, $TypeOK$
$\langle 6 \rangle 2.\ WriterAssignment' = WriterAssignment$
BY $\langle 6 \rangle 1$, SMT DEF $WriterAssignment$
$\langle 6 \rangle 3.$ ASSUME NEW $wa \in WriterAssignment$, NEW $i \in Nat$,

$wa[i] \neq NotAProc$

PROVE $known'[wa[i]] = known[wa[i]]$

$\langle 7 \rangle$ USE $\langle 6 \rangle 3$

$\langle 7 \rangle 1.$ $ReadyToWrite(i,\ wa[i])$

BY $NotAProcProp$, SMT DEF $WriterAssignment$

$\langle 7 \rangle 2.$ $wa[i] \neq p$

BY $\langle 5 \rangle 1$, $\langle 7 \rangle 1$, SMT DEF $ReadyToWrite$

$\langle 7 \rangle 3.$ $wa[i] \in Proc$

BY SMT DEF $WriterAssignment$

$\langle 7 \rangle 4.$ QED

BY $\langle 7 \rangle 2$, $\langle 7 \rangle 3$, $\langle 5 \rangle 1$, SMT DEF $TypeOK$

$\langle 6 \rangle 4.$ $A3' = A3$

BY $\langle 5 \rangle 1$

$\langle 6 \rangle 5.$ QED

$\langle 7 \rangle$ SUFFICES ASSUME NEW $wa \in WriterAssignment$,

NEW $i \in Nat$

PROVE $PV(wa)[i] = PV(wa)[i]'$

$\langle 8 \rangle$ ASSUME NEW $wa \in WriterAssignment$

PROVE $\wedge\ PV(wa) = [i \in Nat \mapsto PV(wa)[i]]$

$\wedge\ PV(wa)' = [i \in Nat \mapsto PV(wa)[i]]$

BY DEF PV

$\langle 8 \rangle$ QED

BY $\langle 6 \rangle 2$ DEF $PA3$

$\langle 7 \rangle 1.$CASE $wa[i] = NotAProc$

BY $\langle 7 \rangle 1$, $\langle 6 \rangle 4$ DEF $PA3$, PV

$\langle 7 \rangle 2.$CASE $wa[i] \neq NotAProc$

BY $\langle 7 \rangle 2$, $\langle 6 \rangle 3$ DEF $PA3$, PV

$\langle 7 \rangle 3.$ QED

BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$

$\langle 5 \rangle 3.$ SUFFICES ASSUME $p = q$

PROVE $nextout'[q] \subseteq NUnion(P)$

$\langle 6 \rangle$ SUFFICES ASSUME $p \neq q$

PROVE $nextout'[q] \subseteq NUnion(P)$

OBVIOUS

$\langle 6 \rangle$ $nextout'[q] = nextout[q]$

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

$\langle 6 \rangle$ QED

BY $\langle 5 \rangle 2$ DEF $Inv2$

$\langle 5 \rangle 4.$ $\wedge\ \forall\, i \in 0 \,..\, (nbpart[p] - 1) : known'[p] = A3[i]$

$\wedge\ known'[p] = NUnion(A3)$

$\wedge\ nbpart[p] - 1 \geq 0$

$\langle 6 \rangle 1.$ $\forall\, i \in 0 \,..\, (nbpart[p] - 1) : known'[p] = A3[i]$

$\langle 7 \rangle$ $\wedge\ notKnown'[p] = \{i \in 0 \,..\, (nbpart[p] - 1) :$

$known'[p] \neq A3[i]\}$

$\wedge\ notKnown'[p] = \{\}$

BY ⟨5⟩1, *SMT* DEF *TypeOK*

⟨7⟩ QED

OBVIOUS

⟨6⟩2. $nbpart[p] - 1 \geq 0$

⟨7⟩1. $NUnion(A2) \neq \{\}$

BY ⟨5⟩1, ⟨2⟩1

⟨7⟩2. $Cardinality(NUnion(A2)) > 0$

BY ⟨2⟩2, ⟨7⟩1, *NonEmptySetCardinality*, *SMT*

⟨7⟩3. QED

BY ⟨2⟩2, ⟨5⟩1, ⟨7⟩2, *SMT*

⟨6⟩3. $known'[p] = A3[0]$

BY ⟨6⟩1, ⟨6⟩2, *SMT* DEF *TypeOK*

⟨6⟩4. $NUnion(A3) \subseteq known'[p]$

BY ⟨5⟩1 DEF *NUnion*, *TypeOK*

⟨6⟩5. $NUnion(A3) = known'[p]$

BY ⟨6⟩3, ⟨6⟩4 DEF *NUnion*

⟨6⟩6. QED

BY ⟨6⟩1, ⟨6⟩2, ⟨6⟩5

⟨5⟩5.CASE $\exists\, i \in 0 \,..\, (nbpart[p] - 1) : P[i] = A3[i]$

⟨6⟩1. PICK $i \in 0 \,..\, (nbpart[p] - 1) : P[i] = A3[i]$

BY ⟨5⟩5

⟨6⟩2. $A3[i] \subseteq NUnion(P)$

BY ⟨6⟩1, *SMT* DEF *NUnion*, *TypeOK*

⟨6⟩3. $known'[p] \subseteq NUnion(P)$

BY ⟨6⟩2, ⟨5⟩4

⟨6⟩4. $nextout'[p] = known'[p]$

BY ⟨5⟩1, *SMT* DEF *TypeOK*

⟨6⟩5. QED

BY ⟨6⟩3, ⟨6⟩4, ⟨5⟩3

⟨5⟩6.CASE $\forall\, i \in 0 \,..\, (nbpart[p] - 1) : P[i] \neq A3[i]$

⟨6⟩ PICK $wa \in WriterAssignment : P = PV(wa)$

BY ⟨5⟩2 DEF *PA3*

⟨6⟩1. $\forall\, i \in 0 \,..\, (nbpart[p] - 1) : \begin{array}{l} \land\, wa[i] \neq NotAProc \\ \land\, P[i] = known[wa[i]] \end{array}$

BY ⟨5⟩6, *SMT* DEF *PV*

⟨6⟩2. $\forall\, i \in 0 \,..\, (nbpart[p] - 1) : \begin{array}{l} \land\, wa[i] \in Proc \\ \land\, ReadyToWrite(i,\, wa[i]) \end{array}$

⟨7⟩1. $nbpart[p] \in Nat$

BY DEF *TypeOK*

⟨7⟩ SUFFICES ASSUME NEW $i \in 0 \,..\, (nbpart[p] - 1)$

PROVE $\begin{array}{l} \land\, wa[i] \in Proc \\ \land\, ReadyToWrite(i,\, wa[i]) \end{array}$

OBVIOUS

⟨7⟩ $i \in Nat$

BY ⟨7⟩1, *SMT*

$\langle 7 \rangle 2.\ wa[i] \in Proc$
  BY $\langle 6 \rangle 1$, SMT DEF $WriterAssignment$
$\langle 7 \rangle 3.$ QED
  BY $\langle 6 \rangle 1$, SMT DEF $WriterAssignment$
$\langle 6 \rangle 3.\ \forall\, i, j \in 0 \mathrel{..} (nbpart[p] - 1) : (i \neq j) \Rightarrow (wa[i] \neq wa[j])$
$\langle 7 \rangle\ nbpart[p] \in Nat$
  BY DEF $TypeOK$
$\langle 7 \rangle$ QED
  BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$, SMT DEF $WriterAssignment$
$\langle 6 \rangle$ DEFINE $S \triangleq \{wa[i] : i \in 0 \mathrel{..} (nbpart[p] - 1)\}$
$\langle 6 \rangle 4.\ Cardinality(S) = nbpart[p]$
$\langle 7 \rangle$ DEFINE $T \triangleq 0 \mathrel{..} (nbpart[p] - 1)$
$\langle 7 \rangle 1.\ \land IsFiniteSet(T)$
$\land Cardinality(T) = nbpart[p]$
$\land nbpart[p] \in Int$
  BY $IntervalCardinality$, $Z3$ DEF $TypeOK$
$\langle 7 \rangle 2.\ IsFiniteSet(S)$
$\langle 8 \rangle 1.$ ASSUME NEW $s \in S$
PROVE $s \in Proc$
$\langle 9 \rangle 1.\ nbpart[p] \in Nat$
  BY DEF $TypeOK$
$\langle 9 \rangle 2.$ QED
  BY $\langle 9 \rangle 1$, $\langle 6 \rangle 1$, $Z3$ DEF $WriterAssignment$ SMT worked on 14 Feb 2013, timed out on 31 May 201
$\langle 8 \rangle 2.$ QED
  BY $\langle 8 \rangle 1$, $ProcFinite$, $SubsetFinite$, SMT
$\langle 7 \rangle 3.\ Cardinality(S) \leq nbpart[p]$
$\langle 8 \rangle$ DEFINE $f \triangleq [s \in S \mapsto$ CHOOSE $i \in T : s = wa[i]]$
$\langle 8 \rangle 1.\ \forall\, s \in S : \land s = wa[f[s]]$
$\land f[s] \in T$
  OBVIOUS
$\langle 8 \rangle 2.\ f \in [S \to T]$
  BY $\langle 8 \rangle 1$
$\langle 8 \rangle$ HIDE DEF f, S, T
$\langle 8 \rangle 3.\ \forall\, x, y \in S : x \neq y \Rightarrow f[x] \neq f[y]$
  BY $\langle 8 \rangle 1$, SMT
$\langle 8 \rangle 4.$ QED
  BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, $\langle 8 \rangle 2$, $\langle 8 \rangle 3$, $InjectionCardinality$, $Z3$
$\langle 7 \rangle 4.\ nbpart[p] \leq Cardinality(S)$
$\langle 8 \rangle$ DEFINE $f \triangleq [i \in T \mapsto wa[i]]$
$\langle 8 \rangle 1.\ f \in [T \to S]$
  BY SMT
$\langle 8 \rangle 2.\ \forall\, x, y \in T : x \neq y \Rightarrow f[x] \neq f[y]$
  BY $\langle 6 \rangle 3$
$\langle 8 \rangle 3.\ nbpart[p] \in Int$
  BY DEF $TypeOK$

$\langle 8 \rangle$ HIDE DEF T, S, f

$\langle 8 \rangle 4.$ QED

BY $\langle 7 \rangle 2$, $\langle 8 \rangle 1$, $\langle 8 \rangle 2$, $\langle 7 \rangle 1$, *InjectionCardinality*, *Z3*

$\langle 7 \rangle 5.$ QED

BY $\langle 7 \rangle 2$, $\langle 7 \rangle 3$, $\langle 7 \rangle 4$, *CardType*, *SMT* DEF *TypeOK*

$\langle 6 \rangle 5.$ $\forall s \in S : \wedge\, pc[s] = \text{"d"}$
$\qquad\qquad\quad \wedge\, s \in NUnion(A2)$

$\langle 7 \rangle$ SUFFICES ASSUME NEW $s \in S$PROVE $s \in NUnion(A2) \wedge pc[s] = \text{"d"}$

OBVIOUS

$\langle 7 \rangle 1.$ PICK $i \in 0 \,..\, (nbpart[p] - 1) : s = wa[i]$

OBVIOUS

$\langle 7 \rangle 2.$ $i \in Nat$

BY *SMT* DEF *TypeOK*

$\langle 7 \rangle 3.$ $wa[i] \in Proc$

BY $\langle 6 \rangle 1$, $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, *SMT* DEF *WriterAssignment*

$\langle 7 \rangle 4.$ $pc[s] = \text{"d"}$

BY $\langle 7 \rangle 1$, $\langle 7 \rangle 3$, *SMT* DEF *WriterAssignment*, *ReadyToWrite*

$\langle 7 \rangle 5.$ QED

BY $\langle 7 \rangle 4$, $\langle 7 \rangle 1$, $\langle 7 \rangle 3$, $\langle 2 \rangle 1$

$\langle 6 \rangle 6.$ $Cardinality(S) = Cardinality(NUnion(A2))$

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

$\langle 6 \rangle 7.$ $S = NUnion(A2)$

$\langle 7 \rangle 1.$ $S \subseteq NUnion(A2)$

BY $\langle 6 \rangle 5$, *SMT*

$\langle 7 \rangle 2.$ $S \neq NUnion(A2) \Rightarrow Cardinality(S) < Cardinality(NUnion(A2))$

BY $\langle 7 \rangle 1$, $\langle 2 \rangle 2$, *SubsetCardinality*, *SMT*

$\langle 7 \rangle 3.$ QED

BY $\langle 2 \rangle 2$, $\langle 7 \rangle 2$, $\langle 6 \rangle 6$, *SMT*

$\langle 6 \rangle 8.$ $p \in NUnion(A2)$

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

$\langle 6 \rangle 9.$ QED

BY $\langle 5 \rangle 1$, $\langle 6 \rangle 8$, $\langle 6 \rangle 7$, $\langle 6 \rangle 5$

$\langle 5 \rangle 7.$ QED

BY $\langle 5 \rangle 5$, $\langle 5 \rangle 6$

$\langle 4 \rangle 3.$CASE $\wedge\, notKnown'[p] = \{\}$
$\qquad\quad \wedge\, nbpart[p] \neq Cardinality(NUnion(A2))$

$\langle 5 \rangle 1.$ $\wedge\, pc[p] = \text{"c"}$
$\quad \wedge\, lnbpart' = [lnbpart \text{ EXCEPT } ![p] = nbpart[p]]$
$\quad \wedge\, known' = [known \text{ EXCEPT } ![p] =$
$\qquad\qquad known[p] \cup \text{UNION } \{A3[i] : i \in Nat\}]$
$\quad \wedge\, notKnown' = [notKnown \text{ EXCEPT } ![p] =$
$\qquad\qquad \{i \in 0 \,..\, (nbpart[p] - 1) :$
$\qquad\qquad\quad known'[p] \neq A3[i]\}]$
$\quad \wedge\, notKnown'[p] = \{\}$
$\quad \wedge\, nbpart[p] \neq Cardinality(NUnion(A2))$

$\land$ UNCHANGED $nextout$
$\land$ $pc' = [pc$ EXCEPT $![p] = \text{"e"}]$
$\land$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out\rangle$
BY $\langle 4\rangle 3$ DEF c, $NUnion$
$\langle 5\rangle 2.$ $PA3' = PA3$

This proof copied from the proof of CASE $\langle 4\rangle 2$.

$\langle 6\rangle 1.$ ASSUME NEW $i \in Nat$, NEW $r \in Proc$
PROVE $ReadyToWrite(i, r)' = ReadyToWrite(i, r)$
BY $\langle 5\rangle 1$, SMT DEF $ReadyToWrite$, $TypeOK$
$\langle 6\rangle 2.$ $WriterAssignment' = WriterAssignment$
BY $\langle 6\rangle 1$, SMT DEF $WriterAssignment$
$\langle 6\rangle 3.$ ASSUME NEW $wa \in WriterAssignment$, NEW $i \in Nat$,
$wa[i] \neq NotAProc$
PROVE $known'[wa[i]] = known[wa[i]]$
$\langle 7\rangle$ USE $\langle 6\rangle 3$
$\langle 7\rangle 1.$ $ReadyToWrite(i, wa[i])$
BY $NotAProcProp$, SMT DEF $WriterAssignment$
$\langle 7\rangle 2.$ $wa[i] \neq p$
BY $\langle 5\rangle 1$, $\langle 7\rangle 1$, SMT DEF $ReadyToWrite$
$\langle 7\rangle 3.$ $wa[i] \in Proc$
BY SMT DEF $WriterAssignment$
$\langle 7\rangle 4.$ QED
BY $\langle 7\rangle 2$, $\langle 7\rangle 3$, $\langle 5\rangle 1$, SMT DEF $TypeOK$
$\langle 6\rangle 4.$ $A3' = A3$
BY $\langle 5\rangle 1$
$\langle 6\rangle 5.$ QED
$\langle 7\rangle$ SUFFICES ASSUME NEW $wa \in WriterAssignment$,
NEW $i \in Nat$
PROVE $PV(wa)[i] = PV(wa)[i]'$
$\langle 8\rangle$ ASSUME NEW $wa \in WriterAssignment$
PROVE $\land PV(wa) = [i \in Nat \mapsto PV(wa)[i]]$
$\land PV(wa)' = [i \in Nat \mapsto PV(wa)[i]]$
BY DEF PV
$\langle 8\rangle$ QED
BY $\langle 6\rangle 2$ DEF $PA3$
$\langle 7\rangle 1.$ CASE $wa[i] = NotAProc$
BY $\langle 7\rangle 1$, $\langle 6\rangle 4$ DEF $PA3$, PV
$\langle 7\rangle 2.$ CASE $wa[i] \neq NotAProc$
BY $\langle 7\rangle 2$, $\langle 6\rangle 3$ DEF $PA3$, PV
$\langle 7\rangle 3.$ QED
BY $\langle 7\rangle 1$, $\langle 7\rangle 2$
$\langle 5\rangle 3.$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$ DEF $Inv2$
$\langle 4\rangle 4.$ QED

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

$\langle 3\rangle 4$. QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle 8$. ASSUME NEW $p \in Proc$, $d(p)$
PROVE Inv'

$\langle 3\rangle$ USE $\langle 2\rangle 8$

$\langle 3\rangle 1$. $TypeOK'$

BY SMT DEF $TypeOK$, d

$\langle 3\rangle 2$. $Inv1'$

$\langle 4\rangle 1$. ASSUME NEW $q \in Proc$
PROVE $Inv1!1!(q)'$

$\langle 5\rangle 1$. $Inv1!1!(q)!1'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 2$. $Inv1!1!(q)!2'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 3$. $Inv1!1!(q)!3'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 4$. $Inv1!1!(q)!4'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 5$. $Inv1!1!(q)!5'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 6$. $Inv1!1!(q)!6'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 7$. $Inv1!1!(q)!7'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 8$. $Inv1!1!(q)!8'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 9$. $Inv1!1!(q)!9'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 10$. $Inv1!1!(q)!10'$

BY SMT DEF $Inv1$, $TypeOK$, d

$\langle 5\rangle 11$. QED

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, $\langle 5\rangle 7$, $\langle 5\rangle 8$, $\langle 5\rangle 9$, $\langle 5\rangle 10$,
SMT DEF $Inv1$

$\langle 4\rangle 2$. $NUnion(A3') \subseteq PUnion(myVals')$

$\langle 5\rangle 1$. PICK $j \in notKnown[p] : A3' = [A3 \text{ EXCEPT } ![j] = known[p]]$

BY DEF d

$\langle 5\rangle$ $j \in Nat$

BY DEF $TypeOK$

$\langle 5\rangle 2$. $A3'[j] = known[p]$

BY $\langle 5\rangle 1$, SMT DEF $TypeOK$, $Inv1$

$\langle 5\rangle 3$. $known[p] \subseteq PUnion(myVals)$

BY SMT DEF $Inv1$

$\langle 5\rangle 4$. $\forall\, i \in Nat : A3[i] \subseteq PUnion(myVals)$

BY SMT DEF $TypeOK$, $Inv1$, $NUnion$

$\langle 5 \rangle 5.$ ASSUME NEW $i \in Nat$
PROVE $A3'[i] \subseteq PUnion(myVals)$
$\langle 6 \rangle 1.$CASE $i \neq j$
BY $\langle 6 \rangle 1$, $\langle 5 \rangle 4$, $\langle 5 \rangle 1$, SMT DEF $TypeOK$
$\langle 6 \rangle 2.$CASE $i = j$
BY $\langle 6 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$, SMT
$\langle 6 \rangle 3.$ QED
BY $\langle 6 \rangle 1$, $\langle 6 \rangle 2$
$\langle 5 \rangle 6.$ $myVals = myVals'$
BY DEF d
$\langle 5 \rangle 7.$ QED
BY $\langle 5 \rangle 5$, $\langle 5 \rangle 6$, SMT DEF $NUnion$
$\langle 4 \rangle 3.$ $Inv1!3'$
BY SMT DEF $Inv1$, $TypeOK$, d
$\langle 4 \rangle 4.$ QED
BY $\langle 4 \rangle 1$, $\langle 4 \rangle 2$, $\langle 4 \rangle 3$ DEF $Inv1$
$\langle 3 \rangle 3.$ $Inv2'$
$\langle 4 \rangle$ SUFFICES $PA3' \subseteq PA3$
BY DEF d, $Inv2$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $P \in PA3'$
PROVE $P \in PA3$
OBVIOUS
$\langle 4 \rangle$ PICK $wa \in WriterAssignment' : P = PV(wa)'$
BY DEF $PA3$
$\langle 4 \rangle 1.$ ASSUME NEW $i \in Nat$, NEW $q \in Proc$,
$ReadyToWrite(i, q)'$
PROVE $ReadyToWrite(i, q)$
$\langle 5 \rangle$ $\wedge\ pc'[q] = \text{“d”} \Rightarrow pc[q] = \text{“d”}$
$\wedge\ notKnown' = notKnown$
BY SMT DEF d, $TypeOK$
$\langle 5 \rangle$ QED
BY $\langle 4 \rangle 1$, SMT DEF $ReadyToWrite$
$\langle 4 \rangle 2.$ $wa \in WriterAssignment$
BY $\langle 4 \rangle 1$, SMT DEF $WriterAssignment$
$\langle 4 \rangle 3.$ PICK $j \in notKnown[p] : A3' = [A3$ EXCEPT $![j] = known[p]]$
BY DEF d
$\langle 4 \rangle$ $j \in Nat$
BY DEF $TypeOK$
$\langle 4 \rangle 4.$CASE $wa[j] \neq NotAProc$
$\langle 5 \rangle 1.$ $PV(wa)' = PV(wa)$
$\langle 6 \rangle 1.$ SUFFICES ASSUME NEW $i \in Nat$
PROVE $PV(wa)'[i] = PV(wa)[i]$
BY DEF PV
$\langle 6 \rangle 2.$CASE $wa[i] \neq NotAProc$
$\langle 7 \rangle$ $known'[wa[i]] = known[wa[i]]$

BY DEF d
⟨7⟩ QED
BY ⟨6⟩2 DEF PV
⟨6⟩3.CASE $wa[i] = NotAProc$
⟨7⟩ $i \neq j$
BY ⟨4⟩4, ⟨6⟩3
⟨7⟩ $A3'[i] = A3[i]$
BY ⟨4⟩3, SMT DEF $TypeOK$
⟨7⟩ QED
BY ⟨6⟩3 DEF PV
⟨6⟩4. QED
BY ⟨6⟩2, ⟨6⟩3
⟨5⟩2. QED
BY ⟨4⟩2, ⟨5⟩1 DEF $PA3$
⟨4⟩5.CASE $wa[j] = NotAProc$
⟨5⟩1. ASSUME NEW $i \in Nat$
PROVE $wa[i] \neq p$
⟨6⟩1. $\neg ReadyToWrite(i, p)'$
BY SMT DEF d, $ReadyToWrite$, $TypeOK$
⟨6⟩2. QED
BY ⟨6⟩1, SMT DEF $WriterAssignment$
⟨5⟩ DEFINE $za \triangleq [wa \text{ EXCEPT } ![j] = p]$
⟨5⟩2. $za \in WriterAssignment$
⟨6⟩1. $wa \in [Nat \rightarrow Proc \cup \{NotAProc\}]$
BY ⟨4⟩2 DEF $WriterAssignment$
⟨6⟩2. $za \in [Nat \rightarrow Proc \cup \{NotAProc\}]$
BY ⟨6⟩1
⟨6⟩3. ASSUME NEW $i \in Nat$,
$za[i] \in Proc$
PROVE $\forall k \in Nat \setminus \{i\} : za[k] \neq za[i]$
⟨7⟩ SUFFICES ASSUME NEW $k \in Nat \setminus \{i\}$
PROVE $za[k] \neq za[i]$
OBVIOUS
⟨7⟩1.CASE $k \neq j \wedge i \neq j$
⟨8⟩ $za[k] = wa[k] \wedge za[i] = wa[i]$
BY ⟨7⟩1, ⟨6⟩1
⟨8⟩ $wa[i] \in Proc$
BY ⟨6⟩3
⟨8⟩ $wa[k] \neq wa[i]$
BY ⟨4⟩2, SMT DEF $WriterAssignment$
⟨8⟩ QED
BY SMT
⟨7⟩2.CASE $j \in \{i, k\}$
⟨8⟩1. PICK $m \in \{i, k\} : m \neq j$
BY SMT

$\langle 8 \rangle$ SUFFICES $za[j] \neq za[m]$
  BY $\langle 8 \rangle 1$, $\langle 7 \rangle 2$, SMT
$\langle 8 \rangle 2$. $za[j] = p \wedge za[m] = wa[m]$
  BY $\langle 6 \rangle 1$, $\langle 8 \rangle 1$
$\langle 8 \rangle$ HIDE DEF za
$\langle 8 \rangle 3$. QED
  BY $\langle 8 \rangle 2$, $\langle 5 \rangle 1$, SMT
$\langle 7 \rangle 3$. QED
  BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$, SMT
$\langle 6 \rangle 4$. ASSUME NEW $i \in Nat$
  PROVE $WriterAssignment!(za)!(i)$
$\langle 7 \rangle 1$.CASE $i \neq j$
$\langle 8 \rangle 1$. $za[i] = wa[i]$
  BY $\langle 7 \rangle 1$, $\langle 6 \rangle 1$
$\langle 8 \rangle 2$. $WriterAssignment!(wa)!(i)$
  BY $\langle 4 \rangle 2$, SMT DEF $WriterAssignment$
$\langle 8 \rangle$ HIDE DEF za
$\langle 8 \rangle 3$. QED
  BY $\langle 8 \rangle 1$, $\langle 8 \rangle 2$, $\langle 6 \rangle 3$
$\langle 7 \rangle 2$.CASE $i = j$
$\langle 8 \rangle 1$. $ReadyToWrite(j, p)$
  BY SMT DEF $ReadyToWrite$, d
$\langle 8 \rangle 2$. $za[j] = p$
  BY $\langle 6 \rangle 1$
$\langle 8 \rangle$ HIDE DEF za
$\langle 8 \rangle 3$. QED
  BY $\langle 7 \rangle 2$, $\langle 8 \rangle 1$, $\langle 8 \rangle 2$, $\langle 6 \rangle 2$, $\langle 6 \rangle 3$ DEF $WriterAssignment$
$\langle 7 \rangle 3$. QED
  BY $\langle 7 \rangle 1$, $\langle 7 \rangle 2$
$\langle 6 \rangle 5$. QED
  BY $\langle 6 \rangle 2$, $\langle 6 \rangle 4$, SMT DEF $WriterAssignment$
$\langle 5 \rangle 3$. $PV(wa)' = PV(za)$
$\langle 6 \rangle 1$. $wa = [k \in Nat \mapsto wa[k]]$
  BY DEF $WriterAssignment$
$\langle 6 \rangle 2$. SUFFICES ASSUME NEW $i \in Nat$
  PROVE $PV(wa)'[i] = PV(za)[i]$
  BY DEF PV
$\langle 6 \rangle 3$.CASE $wa[i] \neq NotAProc$
$\langle 7 \rangle 1$. $i \neq j$
  BY $\langle 4 \rangle 5$, $\langle 6 \rangle 3$
$\langle 7 \rangle 2$. $known'[wa[i]] = known[wa[i]]$
  BY $\langle 7 \rangle 1$ DEF d
$\langle 7 \rangle 3$. $PV(wa)'[i] = known'[wa[i]]$
  BY $\langle 6 \rangle 3$, SMT DEF PV
$\langle 7 \rangle 4$. $za[i] = wa[i]$

BY $\langle 6\rangle 1$, $\langle 7\rangle 1$

$\langle 7\rangle 5$. $PV(za)[i] = known[wa[i]]$

BY $\langle 7\rangle 4$, $\langle 6\rangle 3$ DEF PV

$\langle 7\rangle 6$. QED

BY $\langle 7\rangle 2$, $\langle 7\rangle 3$, $\langle 7\rangle 5$

$\langle 6\rangle 4$.CASE $wa[i] = NotAProc$

$\langle 7\rangle 1$.CASE $i \neq j$

$\langle 8\rangle$ $A3'[i] = A3[i]$

BY $\langle 7\rangle 1$, $\langle 4\rangle 3$, SMT DEF $TypeOK$

$\langle 8\rangle$ $wa[i] = za[i]$

BY $\langle 6\rangle 1$, $\langle 7\rangle 1$

$\langle 8\rangle$ QED

BY $\langle 6\rangle 4$ DEF PV

$\langle 7\rangle 2$.CASE $i = j$

$\langle 8\rangle 1$. $PV(wa)'[j] = A3[j]'$

BY $\langle 7\rangle 2$, $\langle 6\rangle 4$ DEF PV

$\langle 8\rangle 2$. $za[j] = p$

BY $\langle 6\rangle 1$, $\langle 7\rangle 2$

$\langle 8\rangle 3$. $PV(za)[j] = known[p]$

BY $\langle 8\rangle 2$, $NotAProcProp$, SMT DEF PV

$\langle 8\rangle 4$. $A3'[j] = known[p]$

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

$\langle 8\rangle$ HIDE DEF za

$\langle 8\rangle 5$. QED

BY $\langle 7\rangle 2$, $\langle 8\rangle 1$, $\langle 8\rangle 3$, $\langle 8\rangle 4$

$\langle 7\rangle 3$. QED

BY $\langle 7\rangle 1$, $\langle 7\rangle 2$

$\langle 6\rangle 5$. QED

BY $\langle 6\rangle 3$, $\langle 6\rangle 4$

$\langle 5\rangle 4$. QED

BY $\langle 5\rangle 2$, $\langle 5\rangle 3$ DEF $PA3$

$\langle 4\rangle 6$. QED

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

$\langle 3\rangle 4$. QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle 9$. ASSUME NEW $p \in Proc$, $e(p)$

PROVE Inv'

$\langle 3\rangle$ USE $\langle 2\rangle 9$

$\langle 3\rangle 1$. $TypeOK'$

$\langle 4\rangle 1$. $TypeOK!1'$

BY SMT DEF $TypeOK$, e

$\langle 4\rangle 2$. $TypeOK!2'$

BY SMT DEF $TypeOK$, e

$\langle 4\rangle 3$. $TypeOK!3'$

BY SMT DEF $TypeOK$, e

$\langle 4\rangle 4.$ $TypeOK!4'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 5.$ $TypeOK!5'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 6.$ $TypeOK!6'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 7.$ $TypeOK!7'$
BY $\langle 2\rangle 2$, SMT DEF $TypeOK$, e
$\langle 4\rangle 8.$ $TypeOK!8'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 9.$ $TypeOK!9'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 10.$ $TypeOK!10'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 11.$ $TypeOK!11'$
BY SMT DEF $TypeOK$, e
$\langle 4\rangle 12.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$, $\langle 4\rangle 6$,
$\langle 4\rangle 7$, $\langle 4\rangle 8$, $\langle 4\rangle 9$, $\langle 4\rangle 10$, $\langle 4\rangle 11$, SMT DEF $TypeOK$
$\langle 3\rangle 2.$ $Inv1'$
$\langle 4\rangle 1.$ ASSUME NEW $q \in Proc$
PROVE $Inv1!1!(q)'$
$\langle 5\rangle 1.$ $Inv1!1!(q)!1'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 2.$ $Inv1!1!(q)!2'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 3.$ $Inv1!1!(q)!3'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 4.$ $Inv1!1!(q)!4'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 5.$ $nbpart'[q] \leq Cardinality(NUnion(A2'))$
$\langle 6\rangle$ $Cardinality(NUnion(A2')) = Cardinality(NUnion(A2))$
BY DEF e
$\langle 6\rangle 1.$CASE $p = q$
BY $\langle 2\rangle 2$, $\langle 6\rangle 1$, SMT DEF $Inv1$, $TypeOK$, e
$\langle 6\rangle 2.$CASE $p \neq q$
BY $\langle 2\rangle 2$, $\langle 6\rangle 2$, SMT DEF $Inv1$, $TypeOK$, e
$\langle 6\rangle 3.$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle 6.$ $Inv1!1!(q)!6'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 7.$ $Inv1!1!(q)!7'$
BY SMT DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 8.$ $Inv1!1!(q)!8'$
BY SMT DEF $Inv1$, $TypeOK$, e

$\langle 5\rangle 9.$ $Inv1!1!(q)!9'$
BY *SMT* DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 10.$ $Inv1!1!(q)!10'$
BY *SMT* DEF $Inv1$, $TypeOK$, e
$\langle 5\rangle 11.$ QED
BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, $\langle 5\rangle 4$, $\langle 5\rangle 5$, $\langle 5\rangle 6$, $\langle 5\rangle 7$, $\langle 5\rangle 8$, $\langle 5\rangle 9$, $\langle 5\rangle 10$, *SMT* DEF $Inv1$
$\langle 4\rangle 2.$ $NUnion(A3') \subseteq PUnion(myVals')$
BY *SMT* DEF $Inv1$, $TypeOK$, e
$\langle 4\rangle 3.$ $Inv1!3'$
BY *SMT* DEF $Inv1$, $TypeOK$, e
$\langle 4\rangle 4.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $Inv1$
$\langle 3\rangle 3.$ $Inv2'$

This proof copied from the proof of for $b(p)$.

$\langle 4\rangle$ SUFFICES $PA3' = PA3$
BY DEF $Inv2$, e
$\langle 4\rangle 1.$ $WriterAssignment' = WriterAssignment$
$\langle 5\rangle 1.$ ASSUME NEW $q \in Proc$
PROVE $(pc[q] = \text{"d"}) = (pc'[q] = \text{"d"})$
$\langle 6\rangle 1.$ $pc[q] = \text{"d"} \Rightarrow p \neq q$
BY DEF e
$\langle 6\rangle 2.$ $pc'[q] = \text{"d"} \Rightarrow p \neq q$
BY DEF e, $TypeOK$
$\langle 6\rangle 3.$ $p \neq q \Rightarrow pc'[q] = pc[q]$
BY DEF e, $TypeOK$
$\langle 6\rangle 4.$ QED
BY $\langle 6\rangle 1$, $\langle 6\rangle 2$, $\langle 6\rangle 3$
$\langle 5\rangle 2.$ $\forall\, i \in Nat,\ q \in Proc : ReadyToWrite(i,\ q) = ReadyToWrite(i,\ q)'$
BY $\langle 5\rangle 1$, *SMT* DEF $ReadyToWrite$, e
$\langle 5\rangle 3.$ QED
BY $\langle 5\rangle 2$, *SMT* DEF $WriterAssignment$
$\langle 4\rangle 2.$ ASSUME NEW $wa \in WriterAssignment$
PROVE $PV(wa) = PV(wa)'$
$\langle 5\rangle 1.$ $A3' = A3$
BY DEF e
$\langle 5\rangle 2.$ ASSUME $wa \in WriterAssignment$, NEW $i \in Nat$, $wa[i] \neq NotAProc$
PROVE $known'[wa[i]] = known[wa[i]]$
$\langle 6\rangle 1.$ $wa[i] \in Proc$
BY $\langle 5\rangle 2$, *SMT* DEF $WriterAssignment$
$\langle 6\rangle 2.$ $ReadyToWrite(i,\ wa[i])$
BY $\langle 5\rangle 2$, $\langle 6\rangle 1$, *SMT* DEF $WriterAssignment$
$\langle 6\rangle 3.$ $pc[wa[i]] = \text{"d"}$
BY $\langle 6\rangle 2$ DEF $ReadyToWrite$

$\langle 6\rangle 4.\ wa[i] \neq p$

BY $\langle 6\rangle 3$ DEF e

$\langle 6\rangle 5.$ QED

BY $\langle 6\rangle 4$, SMT DEF $TypeOK$, e

$\langle 5\rangle 3.$ ASSUME NEW $i \in Nat$, $wa \in WriterAssignment$

PROVE $(\text{IF } wa[i] = NotAProc \text{ THEN } A3[i] \text{ ELSE } known[wa[i]]) =$
$(\text{IF } wa[i] = NotAProc \text{ THEN } A3'[i] \text{ ELSE } known'[wa[i]])$

$\langle 6\rangle 1.$CASE $wa[i] = NotAProc$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 1$

$\langle 6\rangle 2.$CASE $wa[i] \neq NotAProc$

BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 6\rangle 2$

$\langle 6\rangle 3.$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 2$

$\langle 5\rangle 4.$ QED

BY $\langle 5\rangle 3$ DEF PV

$\langle 4\rangle 3.$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 1$ DEF $PA3$

$\langle 3\rangle 4.$ QED

BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$

$\langle 2\rangle 10.$ QED

BY $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, $\langle 2\rangle 8$, $\langle 2\rangle 9$ DEF $Next$

$\langle 1\rangle 3.$ QED

** PROOF

By $\langle 1\rangle 1$, $\langle 1\rangle 2$ and TLA reasoning.

** OMITTED

We now prove that algorithm *SnapShot* implements/refines the specification *BigSpec* of module *SnapSpec*.

$$pcBar \triangleq [p \in Proc \mapsto \text{CASE } pc[p] \in \{\text{“a”}, \text{“b”}\} \rightarrow \text{“A”} \;\Box\; pc[p] \in \{\text{“c”}, \text{“d”}\} \rightarrow \text{“B”} \;\Box\; pc[p] = \text{“e”} \rightarrow \text{IF } lnbpart[p] = Cardinality(NUnion(A2)) \text{ THEN “C” ELSE “B”}]$$

LEMMA $pcBarFcn \triangleq \land\ pcBar = [i \in Proc \mapsto pcBar[i]]$
$\land\ pcBar' = [i \in Proc \mapsto pcBar'[i]]$

BY DEF $pcBar$

$S \triangleq$ INSTANCE $SnapSpec$ WITH $pc \leftarrow pcBar$

THEOREM $Spec \Rightarrow S!BigSpec$

$\langle 1\rangle$ USE DEF $ProcSet$, $S!ProcSet$, Pr, $S!Pr$

$\langle 1\rangle 1.\ Init \Rightarrow S!Init$

$\langle 2 \rangle$ SUFFICES ASSUME $Init$
PROVE $S!Init$
OBVIOUS
$\langle 2 \rangle 1.$ $S!Init!1$
BY SMT DEF $Init$
$\langle 2 \rangle 2.$ $S!Init!2$
BY SMT DEF $Init$
$\langle 2 \rangle 3.$ $S!Init!3$
BY SMT DEF $Init$
$\langle 2 \rangle 4.$ $S!Init!4$
$\langle 3 \rangle 1.$ $NUnion(A2) = \{\}$
BY SMT DEF $NUnion$, $Init$
$\langle 3 \rangle 2.$ $Cardinality(\{\}) = 0$
BY $EmptySetCardinality$, SMT
$\langle 3 \rangle 3.$ QED
BY $\langle 3 \rangle 1$, $\langle 3 \rangle 2$ DEF $Init$, $pcBar$
$\langle 2 \rangle 5.$ QED
BY $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, $\langle 2 \rangle 3$, $\langle 2 \rangle 4$, SMT DEF $S!Init$

$\langle 1 \rangle 2.$ $Inv \wedge Inv' \wedge [Next]_{vars} \Rightarrow [S!BigNext]_{S!vars}$
$\langle 2 \rangle 1.$ SUFFICES ASSUME Inv, Inv', $[Next]_{vars}$
PROVE $[S!BigNext]_{S!vars}$
OBVIOUS

We want to use Inv' only when necessary.

$\langle 2 \rangle$ SUFFICES ASSUME Inv, $[Next]_{vars}$
PROVE $[S!BigNext]_{S!vars}$
BY $\langle 2 \rangle 1$
$\langle 2 \rangle$ USE Inv DEF Inv
$\langle 2 \rangle 2.$ ASSUME UNCHANGED $vars$
PROVE UNCHANGED $S!vars$
$\langle 3 \rangle$ $pcBar' = pcBar$
$\langle 4 \rangle$ $A2' = A2 \wedge pc' = pc \wedge lnbpart = lnbpart'$
BY $\langle 2 \rangle 2$ DEF $vars$
$\langle 4 \rangle$ QED
BY DEF $pcBar$
$\langle 3 \rangle$ QED
BY $\langle 2 \rangle 2$, SMT DEF $vars$, $S!vars$
$\langle 2 \rangle 3.$ ASSUME NEW $p \in Proc$, $a(p)$
PROVE $[S!BigNext]_{S!vars}$
$\langle 3 \rangle$ USE $\langle 2 \rangle 3$
$\langle 3 \rangle 1.$CASE $Cardinality(NUnion(A2')) = Cardinality(NUnion(A2))$
$\langle 4 \rangle$ SUFFICES ASSUME NEW $q \in Proc$
PROVE $pcBar'[q] = pcBar[q]$
BY DEF $pcBar$, $S!vars$, a
$\langle 4 \rangle$ QED

BY $\langle 3\rangle 1$ DEF a, $TypeOK$, $pcBar$

$\langle 3\rangle 2.$CASE $Cardinality(NUnion(A2')) \neq Cardinality(NUnion(A2))$

$\langle 4\rangle 1.$ $\land\ Cardinality(NUnion(A2')) \in Nat$
$\land\ Cardinality(NUnion(A2)) \in Nat$

$\langle 5\rangle 1.$ $\land\ NUnion(A2) \in$ SUBSET $Proc$
$\land\ NUnion(A2') \in$ SUBSET $Proc$

BY $\langle 2\rangle 1$, $\langle 2\rangle 1$ DEF $TypeOK$, $NUnion$

$\langle 5\rangle 2.$ QED

BY $\langle 5\rangle 1$, $ProcFinite$, $SubsetFinite$, $CardType$, SMT

$\langle 4\rangle$ SUFFICES $S!BigNext!2!(p)$

BY DEF $S!BigNext$

$\langle 4\rangle 2.$ $Cardinality(NUnion(A2')) > Cardinality(NUnion(A2))$

$\langle 5\rangle 1.$ $Cardinality(NUnion(A2)) \leq Cardinality(NUnion(A2'))$

BY $\langle 2\rangle 1$, $A2monotonic$, $TypeOK'$, SMT

$\langle 5\rangle 2.$ QED

BY $\langle 5\rangle 1$, $\langle 4\rangle 1$, $\langle 3\rangle 2$, SMT

$\langle 4\rangle 3.$ $\land\ pcBar[p] =$ "A"
$\land\ pcBar'[p] =$ "A"

BY DEF a, $pcBar$, $TypeOK$

$\langle 4\rangle$ DEFINE $P \triangleq \{q \in Proc \setminus \{p\} : pcBar[q] =$ "C"$\}$

$\langle 4\rangle 4.$ $pcBar' = [q \in Proc \mapsto$ IF $q \in P$ THEN "B"
ELSE $pcBar[q]]$

$\langle 5\rangle 1.$ ASSUME NEW $q \in P$
PROVE $pcBar'[q] =$ "B"

$\langle 6\rangle 1.$ $\land\ pc[q] =$ "e"
$\land\ lnbpart[q] = Cardinality(NUnion(A2))$

$\langle 7\rangle 1.$ $\land\ q \in Proc$
$\land\ pcBar[q] =$ "C"

OBVIOUS

$\langle 7\rangle$ HIDE DEF P

$\langle 7\rangle 2.$ $pc[q] \in \{$"a", "b", "c", "d", "e"$\}$

BY $\langle 7\rangle 1$ DEF $TypeOK$

$\langle 7\rangle 3.$ QED

BY $\langle 7\rangle 1$, $\langle 7\rangle 2$ DEF $pcBar$

$\langle 6\rangle 2.$ $q \neq p$

BY $\langle 6\rangle 1$ DEF a

$\langle 6\rangle 3.$ $\land\ pc'[q] = pc[q]$
$\land\ lnbpart'[q] = lnbpart[q]$

BY DEF a, $TypeOK$

$\langle 6\rangle 4.$ $lnbpart'[q] \neq Cardinality(NUnion(A2'))$

BY $\langle 3\rangle 2$, $\langle 6\rangle 1$, $\langle 6\rangle 3$

$\langle 6\rangle 5.$ QED

BY $\langle 6\rangle 1$, $\langle 6\rangle 3$, $\langle 6\rangle 4$ DEF $pcBar$

$\langle 5\rangle 2.$ ASSUME NEW $q \in Proc$, $q \notin P$
PROVE $pcBar'[q] = pcBar[q]$

$\langle 6\rangle 1.$ CASE $q = p$
  BY $\langle 6\rangle 1$, $\langle 4\rangle 3$
$\langle 6\rangle 2.$ CASE $q \neq p$
  $\langle 7\rangle 1.$ $\land\ pc'[q] = pc[q]$
      $\land\ lnbpart'[q] = lnbpart[q]$
    BY $\langle 6\rangle 2$ DEF a, $TypeOK$
  $\langle 7\rangle 2.$ CASE $pc[q] \in \{\text{“a”}, \text{“b”}, \text{“c”}, \text{“d”}\}$
    BY $\langle 7\rangle 1$, $\langle 7\rangle 2$ DEF $pcBar$
  $\langle 7\rangle 3.$ CASE $pc[q] = \text{“e”}$
    $\langle 8\rangle 1.$ $pcBar[q] \neq \text{“C”}$
      BY $\langle 5\rangle 2$, $\langle 6\rangle 2$
    $\langle 8\rangle$ HIDE DEF P
    $\langle 8\rangle 2.$ $lnbpart[q] \neq Cardinality(NUnion(A2))$
      BY $\langle 7\rangle 3$, $\langle 8\rangle 1$ DEF $pcBar$
    $\langle 8\rangle 3.$ $lnbpart[q] < Cardinality(NUnion(A2))$
      BY $\langle 8\rangle 2$, $\langle 4\rangle 1$, SMT DEF $Inv1$, $TypeOK$
    $\langle 8\rangle 4.$ $lnbpart'[q] \neq Cardinality(NUnion(A2'))$
      BY $\langle 8\rangle 3$, $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 7\rangle 1$, SMT DEF $TypeOK$
    $\langle 8\rangle 5.$ $pcBar'[q] = \text{“B”}$
      BY $\langle 7\rangle 1$, $\langle 7\rangle 3$, $\langle 8\rangle 4$ DEF $pcBar$
    $\langle 8\rangle 6.$ $pcBar[q] = \text{“B”}$
      BY $\langle 7\rangle 3$, $\langle 8\rangle 2$ DEF $pcBar$
    $\langle 8\rangle 7.$ QED
      BY $\langle 8\rangle 5$, $\langle 8\rangle 6$
  $\langle 7\rangle 4.$ QED
    BY $\langle 7\rangle 2$, $\langle 7\rangle 3$ DEF $TypeOK$
$\langle 6\rangle 3.$ QED
  BY $\langle 6\rangle 1$, $\langle 6\rangle 2$
$\langle 5\rangle 3.$ QED
 $\langle 6\rangle$ $pcBar' = [q \in Proc \mapsto pcBar'[q]]$
   BY DEF $pcBar$
 $\langle 6\rangle$ HIDE DEF P
 $\langle 6\rangle$ ASSUME NEW $q \in Proc$
   PROVE $pcBar'[q] = \text{IF } q \in P \text{ THEN “B” ELSE } pcBar[q]$
   BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, SMT
 $\langle 6\rangle$ QED
   OBVIOUS BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, SMT
$\langle 4\rangle 5.$ UNCHANGED $\langle myVals, nextout, out\rangle$
  BY DEF a
$\langle 4\rangle 6.$ $\land\ P \in \text{SUBSET } (Proc \setminus \{p\})$
   $\land\ \forall q \in P : pcBar[q] = \text{“C”}$
  OBVIOUS
$\langle 4\rangle$ HIDE DEF P
$\langle 4\rangle 7.$ $\exists PP \in \text{SUBSET } (Proc \setminus \{p\}) :$
      $\land\ \forall q \in PP : pcBar[q] = \text{“C”}$

$\wedge\ pcBar' = [q \in Proc \mapsto \text{IF } q \in PP \text{ THEN } \text{“B”}$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE } pcBar[q]]$
$\wedge\ \text{UNCHANGED } \langle myVals,\ nextout,\ out\rangle$
BY $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$, $\langle 4\rangle 6$
$\langle 4\rangle 8.$ QED
BY $\langle 4\rangle 3$, $\langle 4\rangle 7$, SMT
$\langle 3\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 2\rangle 4.$ ASSUME NEW $p \in Proc$, $b(p)$
PROVE $[S!Next]_S!vars$
$\langle 3\rangle$ USE $\langle 2\rangle 4$
$\langle 3\rangle$ SUFFICES $S!A(p)$
BY DEF $S!Next$
$\langle 3\rangle 1.$ $pcBar[p] = \text{“A”}$
BY DEF b, $pcBar$
$\langle 3\rangle 2.$ $pcBar' = [pcBar \text{ EXCEPT } ![p] = \text{“B”}]$
$\langle 4\rangle$ USE DEF $pcBar$
$\langle 4\rangle 1.$ $pcBar'[p] = \text{“B”}$
BY SMT DEF b, $TypeOK$
$\langle 4\rangle 2.$ $\forall\, q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
BY DEF b, $pcBar$, $TypeOK$
$\langle 4\rangle 3.$ $pcBar' = [q \in Proc \mapsto pcBar'[q]]$
BY DEF $pcBar$
$\langle 4\rangle 4.$ $pcBar = [q \in Proc \mapsto pcBar[q]]$
BY DEF $pcBar$
$\langle 4\rangle$ HIDE DEF $pcBar$
$\langle 4\rangle 5.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, $\langle 4\rangle 3$, $\langle 4\rangle 4$
$\langle 3\rangle 3.$ $\exists\, v \in Val :$
$\qquad myVals' = [myVals \text{ EXCEPT } ![p] = myVals[p] \cup \{v\}]$
BY DEF b
$\langle 3\rangle 4.$ UNCHANGED $\langle out,\ nextout\rangle$
BY DEF b
$\langle 3\rangle 5.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$ DEF $S!A$
$\langle 2\rangle 5.$ ASSUME NEW $p \in Proc$, $c(p)$
PROVE $[S!Next]_S!vars$
$\langle 3\rangle$ USE $\langle 2\rangle 5$
$\langle 3\rangle 1.$ $A3 \in PA3$
$\langle 4\rangle$ DEFINE $wa \triangleq [i \in Nat \mapsto NotAProc]$
$\langle 4\rangle 1.$ $wa \in WriterAssignment$
BY $NotAProcProp$, SMT DEF $WriterAssignment$
$\langle 4\rangle 2.$ $A3 = PV(wa)$
BY SMT DEF $TypeOK$, PV
$\langle 4\rangle 3.$ QED

BY $\langle 4\rangle 1$, $\langle 4\rangle 2$ DEF $PA3$

$\langle 3\rangle 2.$CASE $notKnown'[p] \neq \{\}$

$\langle 4\rangle$ SUFFICES UNCHANGED $S!vars$

OBVIOUS

$\langle 4\rangle 1. \land pc[p] = \text{"c"}$
$\land\ lnbpart' = [lnbpart \text{ EXCEPT } ![p] = nbpart[p]]$
$\land\ known' = [known \text{ EXCEPT } ![p] = known[p] \cup \text{UNION } \{A3[i] : i \in Nat\}]$
$\land\ notKnown' = [notKnown \text{ EXCEPT } ![p] = \{i \in 0 \,..\, (nbpart[p] - 1) : known'[p] \neq A3[i]\}]$
$\land\ notKnown'[p] \neq \{\}$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = \text{"d"}]$
$\land$ UNCHANGED $nextout$
$\land$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out\rangle$

BY $\langle 3\rangle 2$ DEF c, $NUnion$

$\langle 4\rangle 2.$ UNCHANGED $\langle myVals, nextout, out\rangle$

BY $\langle 4\rangle 1$

$\langle 4\rangle 3.$ UNCHANGED $pcBar$

$\langle 5\rangle$ $pc[p] = \text{"c"} \land pc'[p] = \text{"d"}$

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

$\langle 5\rangle$ $pcBar'[p] = pcBar[p]$

BY DEF $pcBar$

$\langle 5\rangle$ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$

BY $\langle 4\rangle 1$, SMT DEF $pcBar$, $TypeOK$

$\langle 5\rangle$ QED

BY DEF $pcBar$

$\langle 4\rangle 4.$ QED

BY $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $S!vars$

$\langle 3\rangle 3.$CASE $\land\ notKnown'[p] = \{\}$
$\land\ nbpart[p] = Cardinality(NUnion(A2))$

$\langle 4\rangle$ SUFFICES $S!B(p)$

BY DEF $S!Next$

$\langle 4\rangle 1. \land pc[p] = \text{"c"}$
$\land\ lnbpart' = [lnbpart \text{ EXCEPT } ![p] = nbpart[p]]$
$\land\ known' = [known \text{ EXCEPT } ![p] = known[p] \cup \text{UNION } \{A3[i] : i \in Nat\}]$
$\land\ notKnown' = [notKnown \text{ EXCEPT } ![p] = \{i \in 0 \,..\, (nbpart[p] - 1) : known'[p] \neq A3[i]\}]$
$\land\ notKnown'[p] = \{\}$
$\land\ nbpart[p]$ $lnbpart'[p]$ $= Cardinality(NUnion(A2))$
$\land\ nextout' = [nextout \text{ EXCEPT } ![p] = known'[p]]$
$\land\ pc' = [pc \text{ EXCEPT } ![p] = \text{"e"}]$
$\land$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out\rangle$

$\langle 5 \rangle 1. \langle 4 \rangle 1!1$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 2. \langle 4 \rangle 1!2$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 3. \langle 4 \rangle 1!3$

BY $\langle 3 \rangle 3$ DEF c, $NUnion$

$\langle 5 \rangle 4. \langle 4 \rangle 1!4$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 5. \langle 4 \rangle 1!5$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 6. \langle 4 \rangle 1!6$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 7. \langle 4 \rangle 1!7$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 8. \langle 4 \rangle 1!8$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 9. \langle 4 \rangle 1!9$

BY $\langle 3 \rangle 3$ DEF c

$\langle 5 \rangle 10.$ QED

BY $\langle 5 \rangle 1$, $\langle 5 \rangle 2$, $\langle 5 \rangle 3$, $\langle 5 \rangle 4$, $\langle 5 \rangle 5$, $\langle 5 \rangle 6$, $\langle 5 \rangle 7$, $\langle 5 \rangle 8$, $\langle 5 \rangle 9$

$\langle 4 \rangle 2. \land NUnion(A3) \subseteq nextout'[p]$
$\quad \land \forall\, i \in 0 \,..\, (nbpart[p] - 1) : nextout'[p] = A3[i]$

$\langle 5 \rangle$ USE DEF $NUnion$

$\langle 5 \rangle 1.\ \{i \in 0 \,..\, (nbpart[p] - 1) : known'[p] \neq A3[i]\} = \{\}$

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

$\langle 5 \rangle 2.\ \forall\, i \in 0 \,..\, (nbpart[p] - 1) : known'[p] = A3[i]$

BY $\langle 5 \rangle 1$

$\langle 5 \rangle 3.\ known'[p] = known[p] \cup \text{UNION } \{A3[i] : i \in Nat\}$

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

$\langle 5 \rangle 4.\ nextout'[p] = known'[p]$

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

$\langle 5 \rangle 5.$ QED

BY $\langle 5 \rangle 4$, $\langle 5 \rangle 3$, $\langle 5 \rangle 2$

$\langle 4 \rangle 3.\ PUnion(nextout) \subseteq nextout'[p]$

$\langle 5 \rangle 1.$ SUFFICES ASSUME NEW $q \in Proc$
PROVE $nextout[q] \subseteq nextout'[p]$

BY DEF $PUnion$

$\langle 5 \rangle 2.\ nextout[q] \subseteq NUnion(A3)$

BY $\langle 3 \rangle 1$, SMT DEF $Inv2$

$\langle 5 \rangle 3.$ QED

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

$\langle 4 \rangle 4.\ pcBar[p] = \text{“B”}$

BY $\langle 4 \rangle 1$, SMT DEF $pcBar$

$\langle 4 \rangle 5.\ \exists\, V \in \{W \in \text{SUBSET } S\,!\,PUnion(myVals) :$
$\quad \land myVals[p] \subseteq W$

$\land S!PUnion(nextout) \subseteq W\}$:
$nextout' = [nextout$ EXCEPT $![p] = V]$
⟨5⟩ DEFINE $V \triangleq nextout'[p]$
⟨5⟩1. $V \in$ SUBSET $S!PUnion(myVals)$
⟨6⟩ $\land V \subseteq known'[p]$
$\land known'[p] \subseteq PUnion(myVals')$
BY ⟨2⟩1, *SMT* DEF *Inv*1, *TypeOK* , *S*!*PUnion*, *PUnion*
⟨6⟩ $myVals' = myVals$
BY ⟨4⟩1
⟨6⟩ $PUnion(myVals') = S!PUnion(myVals')$
BY DEF *S*!*PUnion*, *PUnion*
⟨6⟩ QED
BY *SMT*
⟨5⟩2. $myVals'[p] \subseteq V$
⟨6⟩ $myVals'[p] \subseteq known'[p]$
BY ⟨2⟩1, *SMT* DEF *Inv*1
⟨6⟩ $\land myVals' = myVals$
$\land V = known'[p]$
BY ⟨4⟩1, *SMT* DEF *TypeOK*
⟨6⟩ QED
OBVIOUS
⟨5⟩3. $S!PUnion(nextout) \subseteq V$
BY ⟨4⟩3 DEF *PUnion*, *S*!*PUnion*
⟨5⟩4. $V \in$ ⟨4⟩5!1
BY ⟨4⟩1, ⟨5⟩1, ⟨5⟩2, ⟨5⟩3, *SMT*
⟨5⟩5. $nextout' = [nextout$ EXCEPT $![p] = V]$
BY ⟨4⟩1
⟨5⟩6. QED
BY ⟨5⟩4, ⟨5⟩5
⟨4⟩6. $pcBar' = [pcBar$ EXCEPT $![p] =$ "C"$]$
⟨5⟩ $pcBar'[p] =$ "C"
BY ⟨4⟩1, *SMT* DEF *pcBar*, *TypeOK*
⟨5⟩ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
BY ⟨4⟩1 DEF *pcBar*, *TypeOK*
⟨5⟩ QED
BY *pcBarFcn*
⟨4⟩7. UNCHANGED $\langle myVals, out\rangle$
BY ⟨4⟩1
⟨4⟩8. QED
BY ⟨4⟩4, ⟨4⟩5, ⟨4⟩6, ⟨4⟩7, *Z*3 DEF *S*!*B* *SMT* worked on 14 *Feb* 2013, failed on 31 May 2013
⟨3⟩4.CASE $\land notKnown'[p] = \{\}$
$\land nbpart[p] \neq Cardinality(NUnion(A2))$
⟨4⟩ SUFFICES UNCHANGED *S*!*vars*
OBVIOUS
⟨4⟩1. $\land pc[p] =$ "c"

$\land$ $lnbpart' = [lnbpart$ EXCEPT $![p] = nbpart[p]]$
$\land$ $known' = [known$ EXCEPT $![p] =$
$\quad known[p] \cup$ UNION $\{A3[i] : i \in Nat\}]$
$\land$ $notKnown' = [notKnown$ EXCEPT $![p] =$
$\quad \{i \in 0 \, .. \, (nbpart[p] - 1) :$
$\quad\quad known'[p] \neq A3[i]\}]$
$\land$ $notKnown'[p] = \{\}$
$\land$ $nbpart[p] \neq Cardinality(NUnion(A2))$
$\land$ UNCHANGED $nextout$
$\land$ $pc' = [pc$ EXCEPT $![p] =$ "e"$]$
$\land$ UNCHANGED $\langle result, A2, A3, myVals, nbpart, out\rangle$
BY $\langle 3\rangle 4$ DEF c, $NUnion$
$\langle 4\rangle 2.$ UNCHANGED $\langle myVals, nextout, out\rangle$
BY $\langle 4\rangle 1$
$\langle 4\rangle 3.$ UNCHANGED $pcBar$
$\langle 5\rangle$ $pc[p] =$ "c" $\land$ $pc'[p] =$ "e" $\land$ $lnbpart'[p] \neq Cardinality(NUnion(A2'))$
BY $\langle 4\rangle 1$ DEF $TypeOK$
$\langle 5\rangle$ $pcBar'[p] = pcBar[p]$
BY DEF $pcBar$
$\langle 5\rangle$ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
BY $\langle 4\rangle 1$ DEF $pcBar$, $TypeOK$
$\langle 5\rangle$ QED
BY DEF $pcBar$
$\langle 4\rangle 4.$ QED
BY $\langle 4\rangle 2$, $\langle 4\rangle 3$ DEF $S!vars$
$\langle 3\rangle 5.$ QED
BY $\langle 3\rangle 2$, $\langle 3\rangle 3$, $\langle 3\rangle 4$
$\langle 2\rangle 6.$ ASSUME NEW $p \in Proc$, $d(p)$
PROVE $[S!Next]_{S!vars}$
$\langle 3\rangle$ USE $\langle 2\rangle 6$
$\langle 3\rangle$ SUFFICES UNCHANGED $S!vars$
OBVIOUS
$\langle 3\rangle 1.$ $pcBar' = pcBar$
$\langle 4\rangle$ $pcBar[p] =$ "B"
BY DEF d, $pcBar$
$\langle 4\rangle$ $pcBar'[p] =$ "B"
BY DEF d, $pcBar$, $TypeOK$
$\langle 4\rangle$ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
BY DEF d, $pcBar$, $TypeOK$
$\langle 4\rangle$ QED
BY $pcBarFcn$
$\langle 3\rangle 2.$ QED
BY $\langle 3\rangle 1$ DEF d, $S!vars$
$\langle 2\rangle 7.$ ASSUME NEW $p \in Proc$, $e(p)$
PROVE $[S!Next]_{S!vars}$

$\langle 3\rangle$ USE $\langle 2\rangle 7$
$\langle 3\rangle 1.$CASE $lnbpart[p] = nbpart'[p]$
  $\langle 4\rangle 1.$ $\wedge\ lnbpart[p] \quad = nbpart'[p]$
      $\wedge\ pc[p] = \text{“e”}$
      $\wedge\ nbpart' = [nbpart \text{ EXCEPT } ![p] = Cardinality(NUnion(A2))]$
      $\wedge\ out' = [out \text{ EXCEPT } ![p] = known[p]]$
      $\wedge\ pc' = [pc \text{ EXCEPT } ![p] = \text{“b”}]$
      $\wedge$ UNCHANGED $\langle result, A2, A3, myVals, known, notKnown, lnbpart,$
        $nextout\rangle$
    BY $\langle 3\rangle 1$ DEF e
  $\langle 4\rangle 2.$ $nbpart[p] = Cardinality(NUnion(A2))$
    $\langle 5\rangle 1.$ $lnbpart[p] = Cardinality(NUnion(A2))$
      BY $\langle 4\rangle 1$, SMT DEF $TypeOK$
    $\langle 5\rangle 2.$ $\wedge\ lnbpart[p] \leq nbpart[p]$
        $\wedge\ nbpart[p] \leq Cardinality(NUnion(A2))$
      BY $\langle 4\rangle 1$ DEF $Inv1$
    $\langle 5\rangle 3.$ $lnbpart[p] \in Nat \wedge nbpart[p] \in Nat$
      BY SMT DEF $TypeOK$
    $\langle 5\rangle 4.$ QED
      BY $\langle 5\rangle 1$, $\langle 5\rangle 2$, $\langle 5\rangle 3$, SMT
  $\langle 4\rangle 3.$ $nextout[p] = known[p]$
    BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, SMT DEF $Inv1$
  $\langle 4\rangle 4.$ $pcBar[p] = \text{“C”} \wedge pcBar'[p] = \text{“A”}$
    BY $\langle 4\rangle 1$ DEF $pcBar$, $TypeOK$
  $\langle 4\rangle 5.$ $pcBar' = [pcBar \text{ EXCEPT } ![p] = \text{“A”}]$
    $\langle 5\rangle$ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
      BY $\langle 4\rangle 1$ DEF $pcBar$, $TypeOK$
    $\langle 5\rangle$ $\wedge\ pcBar = [q \in Proc \mapsto pcBar[q]]$
      $\wedge\ pcBar' = [q \in Proc \mapsto pcBar'[q]]$
      BY DEF $pcBar$
    $\langle 5\rangle$ QED
      BY $\langle 4\rangle 4$
  $\langle 4\rangle 6.$ $S!C(p)$
    BY $\langle 4\rangle 3$, $\langle 4\rangle 4$, $\langle 4\rangle 5$, $\langle 4\rangle 1$, SMT DEF $S!C$
  $\langle 4\rangle 7.$ QED
    BY $\langle 4\rangle 6$ DEF $S!Next$
$\langle 3\rangle 2.$CASE $lnbpart[p] \neq nbpart'[p]$
  $\langle 4\rangle 1.$ $\wedge\ lnbpart[p] \quad \neq nbpart'[p]$
      $\wedge\ pc[p] = \text{“e”}$
      $\wedge\ nbpart' = [nbpart \text{ EXCEPT } ![p] = Cardinality(NUnion(A2))]$
      $\wedge\ pc' = [pc \text{ EXCEPT } ![p] = \text{“c”}]$
      $\wedge\ out' = out$
      $\wedge$ UNCHANGED $\langle result, A2, A3, myVals, known, notKnown, lnbpart,$
        $nextout\rangle$
    BY $\langle 3\rangle 2$ DEF e

$\langle 4\rangle 2.$ $lnbpart[p] \neq Cardinality(NUnion(A2))$
BY $\langle 4\rangle 1$, SMT DEF $TypeOK$
$\langle 4\rangle 3.$ $pcBar[p] = \text{"B"} \land pcBar'[p] = \text{"B"}$
BY $\langle 4\rangle 1$, $\langle 4\rangle 2$, SMT DEF $TypeOK$, $pcBar$
$\langle 4\rangle 4.$ $pcBar' = pcBar$
$\langle 5\rangle$ $\forall q \in Proc \setminus \{p\} : pcBar'[q] = pcBar[q]$
BY $\langle 4\rangle 1$ DEF $pcBar$, $TypeOK$
$\langle 5\rangle$ $\land pcBar = [q \in Proc \mapsto pcBar[q]]$
$\land pcBar' = [q \in Proc \mapsto pcBar'[q]]$
BY DEF $pcBar$
$\langle 5\rangle$ QED
BY $\langle 4\rangle 3$
$\langle 4\rangle 5.$ QED
BY $\langle 4\rangle 1$, $\langle 4\rangle 4$ DEF $S!vars$
$\langle 3\rangle 3.$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 2\rangle 8.$ QED
$\langle 3\rangle$ $S!Next \Rightarrow S!BigNext$
BY DEF $S!BigNext$
$\langle 3\rangle$ QED
BY $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$, $\langle 2\rangle 6$, $\langle 2\rangle 7$, SMT DEF $Next$, Pr

$\langle 1\rangle 3.$ QED
*** PROOF
BY $\langle 1\rangle 1$, $\langle 1\rangle 2$, *Invariance* and TLA reasoning.
*** OMITTED

* Modification History
* Last modified *Fri* May 31 09:38:40 *PDT* 2013 by *lamport*
* Last modified *Wed Jul* 04 18:46:31 *CEST* 2012 by *cd*
* Last modified *Wed Jul* 04 16:49:18 *CEST* 2012 by *hf*
* Created *Wed Jul* 04 11:46:40 *CEST* 2012 by *cd*