```
1  ------------------------------ MODULE U3Inv_proof ------------------------------
2  EXTENDS Implementation, TypeSafety, Inv, Lemmas

4  THEOREM U3Inv ≜ Inv ∧ [Next]_varlist ∧ (∃ p ∈ PROCESSES : U3(p)) ⇒ Inv'
5    ⟨1⟩ SUFFICES ASSUME Inv, [Next]_varlist, NEW p ∈ PROCESSES, U3(p)
6              PROVE Inv'
7      OBVIOUS
8    ⟨1⟩1. TypeOK'
9      BY NextTypeOK DEF Inv
10   ⟨1⟩ USE ⟨1⟩1 DEF U3, Inv
11   ⟨1⟩2. InvDecide'
12     ⟨2⟩ SUFFICES ASSUME NEW p_1 ∈ PROCESSES',
13                         NEW t ∈ M',
14                         (pc[p_1] = "0")'
15                  PROVE  ( ∧ t.ret[p_1] = BOT
16                           ∧ t.op[p_1] = BOT
17                           ∧ t.arg[p_1] = BOT)'
18       BY DEF InvDecide
19     ⟨2⟩1.CASE u_U[p] = v_U[p]
20       ⟨3⟩ USE ⟨2⟩1
21       ⟨3⟩ PICK told ∈ M : ∧ told.ret[p] ∈ {BOT, ACK}
22                           ∧ t.sigma = told.sigma
23                           ∧ t.ret = [told.ret EXCEPT ![p] = ACK]
24                           ∧ t.op = told.op
25                           ∧ t.arg = told.arg
26         BY DEF Inv, InvU3, TypeOK, Valid_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va
27       ⟨3⟩ QED
28         BY DEF Inv, InvDecide, TypeOK, Valid_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot
29     ⟨2⟩2.CASE u_U[p] ≠ v_U[p]
30       BY ⟨2⟩2 DEF Inv, InvDecide, TypeOK, Valid_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot
31     ⟨2⟩ QED
32       BY ⟨2⟩1, ⟨2⟩2
33   ⟨1⟩3. InvF1'
34     ⟨2⟩ SUFFICES ASSUME NEW p_1 ∈ PROCESSES',
35                         NEW t ∈ M'
36                  PROVE  ( ∧ pc[p_1] = "F1"      ⇒  ∧ t.ret[p_1] = BOT
37                                                    ∧ t.op[p_1] = "F"
38                                                  ∧ t.arg[p_1] ∈ NodeSet
39                                                  ∧ SameRoot(t, c[p_1], t.arg[p_1])
40                           ∧ pc[p_1] = "F1U1"  ⇒  ∧ t.ret[p_1] = BOT
41                                                    ∧ t.op[p_1] = "U"
42                                                  ∧ t.arg[p_1] ∈ NodeSet × NodeSet
43                                                  ∧ SameRoot(t, c[p_1], u_U[p_1])
44                           ∧ pc[p_1] = "F1U2"  ⇒  ∧ t.ret[p_1] = BOT
45                                                    ∧ t.op[p_1] = "U"
```

$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ pc[p\_1] = \text{“F1U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ pc[p\_1] = \text{“F1U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1]))'$

BY DEF $InvF1$

$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 3\rangle$ USE $\langle 2\rangle 1$

$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va

$\langle 3\rangle$ QED

BY DEF Inv, $InvF1$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 2\rangle 2$ DEF Inv, $InvF1$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 2\rangle$ QED

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

$\langle 1\rangle 4$. $InvF2'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\wedge\ pc[p\_1] = \text{“F2”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF2All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F2U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF2All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F2U2”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p\_1,\ t)$

$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF2All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F2U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF2All(p\_1,\ t))'$

BY DEF $InvF2$

$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 3\rangle$ USE $\langle 2\rangle 1$

$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va

$\langle 3\rangle$ QED

BY DEF Inv, $InvF2$, $InvF2All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $Same$

$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 2\rangle 2$ DEF Inv, $InvF2$, $InvF2All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, Sam

$\langle 2\rangle$ QED

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

$\langle 1\rangle 5$. $InvF3'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\wedge\ pc[p\_1] = \text{“F3”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF3All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F3U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF3All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F3U2”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$

$\wedge\ InvU2All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF3All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F3U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF3All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F3U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF3All(p\_1,\ t))'$

BY DEF $InvF3$

$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 3\rangle$ USE $\langle 2\rangle 1$

$\langle 3\rangle$ PICK $told \in M : \wedge told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va

$\langle 3\rangle$ QED

BY DEF Inv, $InvF3$, $InvF3All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $Same$

$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 2\rangle 2$ DEF Inv, $InvF3$, $InvF3All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, Sam

$\langle 2\rangle$ QED

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

$\langle 1\rangle 6$. $InvF4'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\wedge\ pc[p\_1] = \text{“F4”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF4All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F4U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF4All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F4U2”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$

$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF4All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F4U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF4All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F4U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF4All(p\_1,\ t))'$

BY DEF $InvF4$

$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 3\rangle$ USE $\langle 2\rangle 1$

$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va

$\langle 3\rangle$ QED

BY DEF Inv, $InvF4$, $InvF4All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $Same$

$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 2\rangle 2$ DEF Inv, $InvF4$, $InvF4All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, Sam

$\langle 2\rangle$ QED

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

$\langle 1\rangle 7$. $InvF5'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\wedge\ pc[p\_1] = \text{“F5”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF5All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F5U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF5All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F5U2”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$

$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF5All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F5U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF5All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F5U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF5All(p\_1,\ t))'$

BY DEF $InvF5$

$\langle 2\rangle 1.\ (pc[p\_1] = \text{“F5”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF5All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, I

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2.\ (pc[p\_1] = \text{“F5U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF5All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$

271 $\land\ t.sigma = told.sigma$
272 $\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
273 $\land\ t.op = told.op$
274 $\land\ t.arg = told.arg$
275 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,
276 $\langle 4\rangle$ QED
277 BY DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S
278 $\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
279 BY $\langle 3\rangle 2$ DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, I
280 $\langle 3\rangle$ QED
281 BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
282 $\langle 2\rangle 3$. $(pc[p\_1] = \text{“F5U2”} \Rightarrow \land\ t.ret[p\_1] = BOT$
283 $\land\ t.op[p\_1] = \text{“U”}$
284 $\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
285 $\land\ InvU2All(p\_1,\ t)$
286 $\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
287 $\land\ InvF5All(p\_1,\ t))'$
288 $\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$
289 $\langle 4\rangle$ USE $\langle 3\rangle 1$
290 $\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
291 $\land\ t.sigma = told.sigma$
292 $\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
293 $\land\ t.op = told.op$
294 $\land\ t.arg = told.arg$
295 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,
296 $\langle 4\rangle$ QED
297 BY DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S
298 $\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
299 BY $\langle 3\rangle 2$ DEF Inv, $InvF5$, $InvF5All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, I
300 $\langle 3\rangle$ QED
301 BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
302 $\langle 2\rangle 4$. $(pc[p\_1] = \text{“F5U7”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
303 $\land\ t.op[p\_1] = \text{“U”}$
304 $\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
305 $\land\ InvU7All(p\_1,\ t)$
306 $\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
307 $\land\ InvF5All(p\_1,\ t))'$
308 $\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$
309 $\langle 4\rangle$ USE $\langle 3\rangle 1$
310 $\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
311 $\land\ t.sigma = told.sigma$
312 $\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
313 $\land\ t.op = told.op$
314 $\land\ t.arg = told.arg$
315 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

⟨4⟩ QED
BY DEF *Inv*, *InvF*5, *InvF*5*All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *S*
⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨3⟩2 DEF *Inv*, *InvF*5, *InvF*5*All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*,
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩5. $(pc[p\_1] = \text{“F5U8”} \Rightarrow \land\, t.ret[p\_1] \in \{BOT, ACK\}$
$\land\, t.op[p\_1] = \text{“U”}$
$\land\, t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\, InvU8All(p\_1, t)$
$\land\, SameRoot(t, c[p\_1], v\_U[p\_1])$
$\land\, InvF5All(p\_1, t))'$
⟨3⟩1.CASE $u\_U[p] = v\_U[p]$
⟨4⟩ USE ⟨3⟩1
⟨4⟩ PICK $told \in M : \land\, told.ret[p] \in \{BOT, ACK\}$
$\land\, t.sigma = told.sigma$
$\land\, t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\, t.op = told.op$
$\land\, t.arg = told.arg$
BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,
⟨4⟩ QED
BY DEF *Inv*, *InvF*5, *InvF*5*All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *S*
⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨3⟩2 DEF *Inv*, *InvF*5, *InvF*5*All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*,
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩6. QED
BY ⟨2⟩1, ⟨2⟩2, ⟨2⟩3, ⟨2⟩4, ⟨2⟩5
⟨1⟩8. *InvF*6′
⟨2⟩ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\land\, pc[p\_1] = \text{“F6”} \Rightarrow \land\, t.ret[p\_1] = BOT$
$\land\, t.op[p\_1] = \text{“F”}$
$\land\, t.arg[p\_1] \in NodeSet$
$\land\, SameRoot(t, c[p\_1], t.arg[p\_1])$
$\land\, InvF6All(p\_1, t)$
$\land\, pc[p\_1] = \text{“F6U1”} \Rightarrow \land\, t.ret[p\_1] = BOT$
$\land\, t.op[p\_1] = \text{“U”}$
$\land\, t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\, SameRoot(t, c[p\_1], u\_U[p\_1])$
$\land\, InvF6All(p\_1, t)$
$\land\, pc[p\_1] = \text{“F6U2”} \Rightarrow \land\, t.ret[p\_1] = BOT$
$\land\, t.op[p\_1] = \text{“U”}$
$\land\, t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\, InvU2All(p\_1, t)$

$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF6All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F6U7”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF6All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F6U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF6All(p\_1,\ t))'$

BY DEF $InvF6$

$\langle 2\rangle 1.\ (pc[p\_1] = \text{“F6”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF6All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, I

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2.\ (pc[p\_1] = \text{“F6U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF6All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$

406 $\land\ t.arg = told.arg$
407 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$
408 $\langle 4\rangle$ QED
409 BY DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S
410 $\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
411 BY $\langle 3\rangle 2$ DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$,
412 $\langle 3\rangle$ QED
413 BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
414 $\langle 2\rangle 3$. $(pc[p\_1] = \text{“F6U2”} \Rightarrow \land\ t.ret[p\_1] = BOT$
415 $\land\ t.op[p\_1] = \text{“U”}$
416 $\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
417 $\land\ InvU2All(p\_1,\ t)$
418 $\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
419 $\land\ InvF6All(p\_1,\ t))'$
420 $\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$
421 $\langle 4\rangle$ USE $\langle 3\rangle 1$
422 $\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
423 $\land\ t.sigma = told.sigma$
424 $\land\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
425 $\land\ t.op = told.op$
426 $\land\ t.arg = told.arg$
427 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$
428 $\langle 4\rangle$ QED
429 BY DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S
430 $\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
431 BY $\langle 3\rangle 2$ DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$,
432 $\langle 3\rangle$ QED
433 BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
434 $\langle 2\rangle 4$. $(pc[p\_1] = \text{“F6U7”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
435 $\land\ t.op[p\_1] = \text{“U”}$
436 $\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
437 $\land\ InvU7All(p\_1,\ t)$
438 $\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
439 $\land\ InvF6All(p\_1,\ t))'$
440 $\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$
441 $\langle 4\rangle$ USE $\langle 3\rangle 1$
442 $\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
443 $\land\ t.sigma = told.sigma$
444 $\land\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
445 $\land\ t.op = told.op$
446 $\land\ t.arg = told.arg$
447 BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$
448 $\langle 4\rangle$ QED
449 BY DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S
450 $\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$,

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

$\langle 2\rangle 5$. $(pc[p\_1] = \text{“F6U8”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT, ACK\}$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU8All(p\_1, t)$
$\land\ SameRoot(t, c[p\_1], v\_U[p\_1])$
$\land\ InvF6All(p\_1, t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 4\rangle$ USE $\langle 3\rangle 1$
$\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT, ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,
$\langle 4\rangle$ QED
BY DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 3\rangle 2$ DEF Inv, $InvF6$, $InvF6All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$,

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

$\langle 2\rangle 6$. QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$

$\langle 1\rangle 9$. $InvF7'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\land\ pc[p\_1] = \text{“F7”} \Rightarrow \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“F”}$
$\land\ t.arg[p\_1] \in NodeSet$
$\land\ SameRoot(t, c[p\_1], t.arg[p\_1])$
$\land\ InvF7All(p\_1, t)$
$\land\ pc[p\_1] = \text{“F7U1”} \Rightarrow \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ SameRoot(t, c[p\_1], u\_U[p\_1])$
$\land\ InvF7All(p\_1, t)$
$\land\ pc[p\_1] = \text{“F7U2”} \Rightarrow \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU2All(p\_1, t)$
$\land\ SameRoot(t, c[p\_1], v\_U[p\_1])$
$\land\ InvF7All(p\_1, t)$
$\land\ pc[p\_1] = \text{“F7U7”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT, ACK\}$

$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF7All(p\_1,\ t)$
$\wedge\ pc[p\_1] = \text{“F7U8”} \Rightarrow \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\wedge\ InvF7All(p\_1,\ t))'$

BY DEF $InvF7$

$\langle 2\rangle 1.\ (pc[p\_1] = \text{“F7”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“F”}$
$\wedge\ t.arg[p\_1] \in NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ t.arg[p\_1])$
$\wedge\ InvF7All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvF7$, $InvF7All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvF7$, $InvF7All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$,

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2.\ (pc[p\_1] = \text{“F7U1”} \Rightarrow \wedge\ t.ret[p\_1] = BOT$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\wedge\ InvF7All(p\_1,\ t))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *S*

⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$

BY ⟨3⟩2 DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *I*

⟨3⟩ QED

BY ⟨3⟩1, ⟨3⟩2

⟨2⟩3. $(pc[p\_1] = \text{“F7U2”} \Rightarrow \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU2All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\land\ InvF7All(p\_1,\ t))'$

⟨3⟩1.CASE $u\_U[p] = v\_U[p]$

⟨4⟩ USE ⟨3⟩1

⟨4⟩ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$

BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,

⟨4⟩ QED

BY DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *S*

⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$

BY ⟨3⟩2 DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *I*

⟨3⟩ QED

BY ⟨3⟩1, ⟨3⟩2

⟨2⟩4. $(pc[p\_1] = \text{“F7U7”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU7All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\land\ InvF7All(p\_1,\ t))'$

⟨3⟩1.CASE $u\_U[p] = v\_U[p]$

⟨4⟩ USE ⟨3⟩1

⟨4⟩ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$

BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,

⟨4⟩ QED

BY DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *S*

⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$

BY ⟨3⟩2 DEF *Inv*, *InvF7*, *InvF7All*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *I*

⟨3⟩ QED

BY ⟨3⟩1, ⟨3⟩2

$\langle 2\rangle 5.\ (pc[p\_1] = \text{“F7U8”} \ \Rightarrow\ \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU8All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\land\ InvF7All(p\_1,\ t))'$

$\langle 3\rangle 1.$CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M :\ \land\ told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvF7$, $InvF7All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle 2.$CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvF7$, $InvF7All$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, S

$\langle 3\rangle$ QED

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

$\langle 2\rangle 6.$ QED

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

$\langle 1\rangle 10.\ InvFR'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$
PROVE $(\land\ pc[p\_1] = \text{“FR”} \ \Rightarrow\ \land\ t.ret[p\_1] = u\_F[p\_1]$
$\land\ t.op[p\_1] = \text{“F”}$
$\land\ t.arg[p\_1] \in NodeSet$
$\land\ SameRoot(t,\ t.arg[p\_1],\ u\_F[p\_1])$
$\land\ SameRoot(t,\ c[p\_1],\ u\_F[p\_1])$
$\land\ pc[p\_1] = \text{“FRU1”} \ \Rightarrow\ \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\land\ SameRoot(t,\ c[p\_1],\ u\_F[p\_1])$
$\land\ pc[p\_1] = \text{“FRU2”} \ \Rightarrow\ \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU2All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1])$
$\land\ pc[p\_1] = \text{“FRU7”} \ \Rightarrow\ \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU7All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$

$\land\ pc[p\_1] = \text{“FRU8”} \Rightarrow \land\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU8All(p\_1,\ t)$
$\land\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1]))'$

BY DEF *InvFR*

$\langle 2\rangle 1.\ (pc[p\_1] = \text{“FR”} \Rightarrow \land\ t.ret[p\_1] = u\_F[p\_1]$
$\land\ t.op[p\_1] = \text{“F”}$
$\land\ t.arg[p\_1] \in NodeSet$
$\land\ SameRoot(t,\ t.arg[p\_1],\ u\_F[p\_1])$
$\land\ SameRoot(t,\ c[p\_1],\ u\_F[p\_1]))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$

BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*

$\langle 4\rangle$ QED

BY DEF *Inv*, *InvFR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF *Inv*, *InvFR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*,

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2.\ (pc[p\_1] = \text{“FRU1”} \Rightarrow \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1])$
$\land\ SameRoot(t,\ c[p\_1],\ u\_F[p\_1]))'$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$

BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*

$\langle 4\rangle$ QED

BY DEF *Inv*, *InvFR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF *Inv*, *InvFR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*,

$\langle 3\rangle$ QED

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

$\langle 2\rangle 3.\ (pc[p\_1] = \text{“FRU2”} \Rightarrow \land\ t.ret[p\_1] = BOT$

$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1]))'$

$\langle 3\rangle 1.\text{CASE}\ u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret\ \text{EXCEPT}\ ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$

$\langle 4\rangle$ QED

BY DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 3\rangle 2.\text{CASE}\ u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$,

$\langle 3\rangle$ QED

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

$\langle 2\rangle 4.\ (pc[p\_1] = \text{“FRU7”}\ \Rightarrow\ \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ u\_U[p\_1]))'$

$\langle 3\rangle 1.\text{CASE}\ u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret\ \text{EXCEPT}\ ![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$

$\langle 4\rangle$ QED

BY DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 3\rangle 2.\text{CASE}\ u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$,

$\langle 3\rangle$ QED

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

$\langle 2\rangle 5.\ (pc[p\_1] = \text{“FRU8”}\ \Rightarrow\ \wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t)$
$\wedge\ SameRoot(t,\ c[p\_1],\ v\_U[p\_1]))'$

$\langle 3\rangle 1.\text{CASE}\ u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$

$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,
$\langle 4\rangle$ QED
BY DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 3\rangle 2$ DEF Inv, $InvFR$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$,
$\langle 3\rangle$ QED
BY $\langle 3\rangle 1$, $\langle 3\rangle 2$
$\langle 2\rangle 6$. QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$, $\langle 2\rangle 3$, $\langle 2\rangle 4$, $\langle 2\rangle 5$
$\langle 1\rangle 11$. $InvU1'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U1”})'$
PROVE $(\quad \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet)'$
BY DEF $InvU1$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 3\rangle$ USE $\langle 2\rangle 1$
$\langle 3\rangle$ PICK $told \in M : \land\ told.ret[p] \in \{BOT, ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
$\langle 3\rangle$ QED
BY DEF Inv, $InvU1$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 2\rangle 2$ DEF Inv, $InvU1$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 12$. $InvU2'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U2”})'$
PROVE $(\quad \land\ t.ret[p\_1] = BOT$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ InvU2All(p\_1,\ t))'$
BY DEF $InvU2$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$

⟨3⟩ USE ⟨2⟩1
⟨3⟩ PICK $told \in M : \land told.ret[p] \in \{BOT, ACK\}$
$\land t.sigma = told.sigma$
$\land t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land t.op = told.op$
$\land t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
⟨3⟩ QED
BY DEF Inv, $InvU2$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
⟨2⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨2⟩2 DEF Inv, $InvU2$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩13. $InvU3'$
⟨2⟩ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U3”})'$
PROVE $(\land t.ret[p\_1] \in \{BOT, ACK\}$
$\land t.op[p\_1] = \text{“U”}$
$\land t.arg[p\_1] \in NodeSet \times NodeSet$
$\land SameRoot(t, t.arg[p\_1][1], u\_U[p\_1])$
$\land SameRoot(t, t.arg[p\_1][2], v\_U[p\_1])$
$\land t.ret[p\_1] = ACK \Rightarrow SameRoot(t, u\_U[p\_1], v\_U[p\_1]))'$
BY DEF $InvU3$
⟨2⟩1.CASE $u\_U[p] = v\_U[p]$
⟨3⟩ USE ⟨2⟩1
⟨3⟩ PICK $told \in M : \land told.ret[p] \in \{BOT, ACK\}$
$\land t.sigma = told.sigma$
$\land t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land t.op = told.op$
$\land t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
⟨3⟩ QED
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
⟨2⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨2⟩2 DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2
⟨1⟩14. $InvU4'$
⟨2⟩ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U4”})'$
PROVE $(\quad \land t.ret[p\_1] \in \{BOT, ACK\}$
$\land t.op[p\_1] = \text{“U”}$
$\land t.arg[p\_1] \in NodeSet \times NodeSet$

$\land$ $SameRoot(t,\ t.arg[p\_1][1],\ u\_U[p\_1])$
$\land$ $SameRoot(t,\ t.arg[p\_1][2],\ v\_U[p\_1])$
$\land$ $(t.ret[p\_1] = ACK \Rightarrow SameRoot(t,\ u\_U[p\_1],\ v\_U[p\_1]))$
$\land$ $u\_U[p\_1] \neq v\_U[p\_1])'$

BY DEF $InvU4$

$\langle 2\rangle 1$.CASE $pc[p\_1] =$ "U3"

$\langle 3\rangle$ USE $\langle 2\rangle 1$

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M$: $\land$ $told.ret[p] \in \{BOT,\ ACK\}$
$\land$ $t.sigma = told.sigma$
$\land$ $t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\land$ $t.op = told.op$
$\land$ $t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvU4$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvU3$, $InvU4$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, Sa

$\langle 3\rangle$ QED

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

$\langle 2\rangle 2$.CASE $pc[p\_1] =$ "U4"

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

$\langle 3\rangle 1$.CASE $u\_U[p] = v\_U[p]$

$\langle 4\rangle$ USE $\langle 3\rangle 1$

$\langle 4\rangle$ PICK $told \in M$: $\land$ $told.ret[p] \in \{BOT,\ ACK\}$
$\land$ $t.sigma = told.sigma$
$\land$ $t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\land$ $t.op = told.op$
$\land$ $t.arg = told.arg$

BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$,

$\langle 4\rangle$ QED

BY DEF Inv, $InvU4$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$

$\langle 3\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$

BY $\langle 3\rangle 2$ DEF Inv, $InvU4$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$,

$\langle 3\rangle$ QED

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

$\langle 2\rangle$ QED

BY $\langle 2\rangle 1$, $\langle 2\rangle 2$ DEF Inv, $TypeOK$, $Valid\_pc$, $PCSet$

$\langle 1\rangle 15$. $InvU5'$

$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] =$ "U5"$)'$
PROVE ($\land$ $t.ret[p\_1] \in \{BOT,\ ACK\}$
$\land$ $t.op[p\_1] =$ "U"

$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU5All(p\_1,\ t))'$
BY DEF $InvU5$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 3\rangle$ USE $\langle 2\rangle 1$
$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
$\langle 3\rangle$ QED
BY DEF Inv, $InvU5$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$, $InvU$
$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 2\rangle 2$ DEF Inv, $InvU5$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$, Inv
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 16$. $InvU6'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U6”})'$
PROVE $(\wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU6All(p\_1,\ t))'$
BY DEF $InvU6$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 3\rangle$ USE $\langle 2\rangle 1$
$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
$\langle 3\rangle$ QED
BY DEF Inv, $InvU6$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$, $InvU$
$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 2\rangle 2$ DEF Inv, $InvU6$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$, Inv
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 17$. $InvU7'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U7”})'$
PROVE $(\wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$

$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p\_1,\ t))'$
BY DEF $InvU7$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 3\rangle$ USE $\langle 2\rangle 1$
$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
$\langle 3\rangle$ QED
BY DEF Inv, $InvU7$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 2\rangle 2$ DEF Inv, $InvU7$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 18$. $InvU8'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“U8”})'$
PROVE $(\wedge\ t.ret[p\_1] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p\_1] = \text{“U”}$
$\wedge\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p\_1,\ t))'$
BY DEF $InvU8$
$\langle 2\rangle 1$.CASE $u\_U[p] = v\_U[p]$
$\langle 3\rangle$ USE $\langle 2\rangle 1$
$\langle 3\rangle$ PICK $told \in M : \wedge\ told.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.sigma = told.sigma$
$\wedge\ t.ret = [told.ret$ EXCEPT $![p] = ACK]$
$\wedge\ t.op = told.op$
$\wedge\ t.arg = told.arg$
BY DEF Inv, $InvU3$, $TypeOK$, $Valid\_pc$, $PCSet$, $Configs$, $StateSet$, $OpSet$, $ArgSet$, $ReturnSet$, Va
$\langle 3\rangle$ QED
BY DEF Inv, $InvU8$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle 2$.CASE $u\_U[p] \neq v\_U[p]$
BY $\langle 2\rangle 2$ DEF Inv, $InvU8$, $TypeOK$, $Valid\_pc$, $PCSet$, $InvU2All$, $InvU7All$, $InvU8All$, $SameRoot$
$\langle 2\rangle$ QED
BY $\langle 2\rangle 1$, $\langle 2\rangle 2$
$\langle 1\rangle 19$. $InvUR'$
$\langle 2\rangle$ SUFFICES ASSUME NEW $p\_1 \in PROCESSES'$,
NEW $t \in M'$,
$(pc[p\_1] = \text{“UR”})'$

PROVE ($\land\ t.ret[p\_1] = ACK$
$\land\ t.op[p\_1] = \text{“U”}$
$\land\ t.arg[p\_1] \in NodeSet \times NodeSet$
$\land\ SameRoot(t,\ t.arg[p\_1][1],\ u\_U[p\_1])$
$\land\ SameRoot(t,\ t.arg[p\_1][2],\ v\_U[p\_1])$
$\land\ SameRoot(t,\ u\_U[p\_1],\ v\_U[p\_1]))'$
BY DEF *InvUR*
⟨2⟩1.CASE $pc[p\_1] = \text{“U3”}$
⟨3⟩ USE ⟨2⟩1
⟨3⟩1.CASE $u\_U[p] = v\_U[p]$
⟨4⟩ USE ⟨3⟩1
⟨4⟩ PICK $told \in M : \land told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$
BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,
⟨4⟩ $p = p\_1$
BY DEF *Inv*, *TypeOK*, *Valid_pc*, *PCSet*
⟨4⟩ QED
BY DEF *Inv*, *InvU*3, *InvUR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *Sam*
⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨3⟩2 DEF *Inv*, *InvU*3, *InvUR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *Sa*
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩2.CASE $pc[p\_1] = \text{“UR”}$
⟨3⟩ USE ⟨2⟩2
⟨3⟩1.CASE $u\_U[p] = v\_U[p]$
⟨4⟩ USE ⟨3⟩1
⟨4⟩ PICK $told \in M : \land told.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.sigma = told.sigma$
$\land\ t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$
$\land\ t.op = told.op$
$\land\ t.arg = told.arg$
BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,
⟨4⟩ QED
BY DEF *Inv*, *InvUR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *SameRoot*
⟨3⟩2.CASE $u\_U[p] \neq v\_U[p]$
BY ⟨3⟩2 DEF *Inv*, *InvUR*, *TypeOK*, *Valid_pc*, *PCSet*, *InvU*2*All*, *InvU*7*All*, *InvU*8*All*, *SameRoot*,
⟨3⟩ QED
BY ⟨3⟩1, ⟨3⟩2
⟨2⟩ QED
BY ⟨2⟩1, ⟨2⟩2 DEF *Inv*, *TypeOK*, *Valid_pc*, *PCSet*
⟨1⟩20. *SigmaRespectsShared'*

991 $\langle 2\rangle$ SUFFICES ASSUME NEW $t \in M'$,
992 NEW $i \in NodeSet'$
993 PROVE $(\land F[i].bit = 0 \quad \Rightarrow t.sigma[i] = t.sigma[F[i].parent]$
994 $\land F[i].bit = 1 \quad \Rightarrow t.sigma[i] = i)'$
995 BY DEF *SigmaRespectsShared*
996 $\langle 2\rangle$1.CASE $u\_U[p] = v\_U[p]$
997 $\langle 3\rangle$ USE $\langle 2\rangle$1
998 $\langle 3\rangle$ PICK $told \in M : \land told.ret[p] \in \{BOT, ACK\}$
999 $\land t.sigma = told.sigma$
1000 $\land t.ret = [told.ret$ EXCEPT $![p] = ACK]$
1001 $\land t.op = told.op$
1002 $\land t.arg = told.arg$
1003 BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*, *Va*
1004 $\langle 3\rangle$ QED
1005 BY DEF *Inv*, *SigmaRespectsShared*, *TypeOK*, *Valid_F*, *Valid_M*, *Configs*, *StateSet*
1006 $\langle 2\rangle$2.CASE $u\_U[p] \neq v\_U[p]$
1007 BY $\langle 2\rangle$2 DEF *Inv*, *SigmaRespectsShared*, *TypeOK*, *Valid_F*, *Valid_M*, *Configs*, *StateSet*
1008 $\langle 2\rangle$ QED
1009 BY $\langle 2\rangle$1, $\langle 2\rangle$2
1010 $\langle 1\rangle$21. $SharedRespectsSigma'$
1011 $\langle 2\rangle$ SUFFICES ASSUME NEW $t \in M'$,
1012 NEW $i \in NodeSet'$,
1013 $(t.sigma[i] = i)'$
1014 PROVE $(F[i].bit = 1)'$
1015 BY DEF *SharedRespectsSigma*
1016 $\langle 2\rangle$1.CASE $u\_U[p] = v\_U[p]$
1017 $\langle 3\rangle$ USE $\langle 2\rangle$1
1018 $\langle 3\rangle$ PICK $told \in M : \land told.ret[p] \in \{BOT, ACK\}$
1019 $\land t.sigma = told.sigma$
1020 $\land t.ret = [told.ret$ EXCEPT $![p] = ACK]$
1021 $\land t.op = told.op$
1022 $\land t.arg = told.arg$
1023 BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*, *Va*
1024 $\langle 3\rangle$ QED
1025 BY DEF *Inv*, *SharedRespectsSigma*, *TypeOK*, *Valid_F*, *Valid_M*, *Configs*, *StateSet*
1026 $\langle 2\rangle$2.CASE $u\_U[p] \neq v\_U[p]$
1027 BY $\langle 2\rangle$2 DEF *Inv*, *SharedRespectsSigma*, *TypeOK*, *Valid_F*, *Valid_M*, *Configs*, *StateSet*
1028 $\langle 2\rangle$ QED
1029 BY $\langle 2\rangle$1, $\langle 2\rangle$2
1030 $\langle 1\rangle$22. $Linearizable'$
1031 $\langle 2\rangle$1.CASE $u\_U[p] = v\_U[p]$
1032 $\langle 3\rangle$ USE $\langle 2\rangle$1
1033 $\langle 3\rangle$ PICK $told \in M : told.ret[p] = BOT \lor told.ret[p] = ACK$
1034 BY DEF *Inv*, *InvU*3, *TypeOK*, *Valid_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*, *Va*
1035 $\langle 3\rangle$a. $told \in Configs$

```
            BY DEF Inv, TypeOK, Valid_M
        ⟨3⟩1.CASE told.ret[p] = BOT
            ⟨4⟩ DEFINE t ≜ [sigma ↦ told.sigma,
                           ret ↦ [told.ret EXCEPT ![p] = ACK],
                           op ↦ told.op,
                           arg ↦ told.arg]
            ⟨4⟩ t ∈ M′
                BY ⟨3⟩1 DEF Inv, Configs, StateSet, OpSet, ArgSet, ReturnSet, TypeOK, t, Valid_M
            ⟨4⟩ QED
                BY DEF Inv, Linearizable
        ⟨3⟩2.CASE told.ret[p] = ACK
            ⟨4⟩ told ∈ M′
                BY ⟨3⟩2 DEF Inv, Configs, StateSet, OpSet, ArgSet, ReturnSet, TypeOK, Valid_M
            ⟨4⟩ QED
                BY DEF Inv, Linearizable
        ⟨3⟩ QED
            BY ⟨3⟩1, ⟨3⟩2
    ⟨2⟩2.CASE u_U[p] ≠ v_U[p]
        BY ⟨2⟩2 DEF Inv, Linearizable
    ⟨2⟩ QED
        BY ⟨2⟩1, ⟨2⟩2
⟨1⟩23. QED
    BY ⟨1⟩1, ⟨1⟩10, ⟨1⟩11, ⟨1⟩12, ⟨1⟩13, ⟨1⟩14, ⟨1⟩15, ⟨1⟩16, ⟨1⟩17, ⟨1⟩18, ⟨1⟩19, ⟨1⟩2, ⟨1⟩20, ⟨1⟩21, ⟨1⟩22, ⟨1⟩3,
```

* Modification History
* Last modified *Wed Apr* 23 23:17:39 *EDT* 2025 by *karunram*
* Created *Wed Apr* 23 23:17:25 *EDT* 2025 by *karunram*