

```

1  ┌────────────────────────── MODULE U3Inv_proof ───────────────────────────┐
2  EXTENDS Implementation, TypeSafety, Inv, Lemmas

4  THEOREM  $U3Inv \triangleq Inv \wedge [Next]_{varlist} \wedge (\exists p \in PROCESSES : U3(p)) \Rightarrow Inv'$ 
5  ⟨1⟩ SUFFICES ASSUME  $Inv, [Next]_{varlist}, \text{NEW } p \in PROCESSES, U3(p)$ 
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  $p\_1 \in PROCESSES'$ ,
13                     NEW  $t \in M'$ ,
14                      $(pc[p\_1] = "0")'$ 
15     PROVE  $(\wedge t.ret[p\_1] = BOT$ 
16            $\wedge t.op[p\_1] = BOT$ 
17            $\wedge t.arg[p\_1] = BOT)'$ 
18     BY DEF InvDecide
19 ⟨2⟩1.CASE  $u\_U[p] = v\_U[p]$ 
20     ⟨3⟩ USE ⟨2⟩1
21     ⟨3⟩ PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$ 
22            $\wedge t.sigma = told.sigma$ 
23            $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$ 
24            $\wedge t.op = told.op$ 
25            $\wedge t.arg = told.arg$ 
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  $u\_U[p] \neq v\_U[p]$ 
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  $p\_1 \in PROCESSES'$ ,
35                     NEW  $t \in M'$ 
36     PROVE  $(\wedge pc[p\_1] = "F1" \Rightarrow \wedge t.ret[p\_1] = BOT$ 
37            $\wedge t.op[p\_1] = "F"$ 
38            $\wedge t.arg[p\_1] \in NodeSet$ 
39            $\wedge SameRoot(t, c[p\_1], t.arg[p\_1])$ 
40            $\wedge pc[p\_1] = "F1U1" \Rightarrow \wedge t.ret[p\_1] = BOT$ 
41            $\wedge t.op[p\_1] = "U"$ 
42            $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$ 
43            $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$ 
44            $\wedge pc[p\_1] = "F1U2" \Rightarrow \wedge t.ret[p\_1] = BOT$ 
45            $\wedge t.op[p\_1] = "U"$ 

```

46  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 47  $\wedge InvU2All(p-1, t)$   
 48  $\wedge SameRoot(t, c[p-1], v-U[p-1])$   
 49  $\wedge pc[p-1] = \text{"F1U7"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
 50  $\wedge t.op[p-1] = \text{"U"}$   
 51  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 52  $\wedge InvU7All(p-1, t)$   
 53  $\wedge SameRoot(t, c[p-1], u-U[p-1])$   
 54  $\wedge pc[p-1] = \text{"F1U8"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
 55  $\wedge t.op[p-1] = \text{"U"}$   
 56  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 57  $\wedge InvU8All(p-1, t)$   
 58  $\wedge SameRoot(t, c[p-1], v-U[p-1]))'$   
 59 BY DEF *InvF1*  
 60  $\langle 2 \rangle 1.CASE\ u-U[p] = v-U[p]$   
 61  $\langle 3 \rangle USE\ \langle 2 \rangle 1$   
 62  $\langle 3 \rangle PICK\ told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 63  $\wedge t.sigma = told.sigma$   
 64  $\wedge t.ret = [told.ret\ EXCEPT\ ![p] = ACK]$   
 65  $\wedge t.op = told.op$   
 66  $\wedge t.arg = told.arg$   
 67 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 68  $\langle 3 \rangle QED$   
 69 BY DEF *Inv, InvF1, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 70  $\langle 2 \rangle 2.CASE\ u-U[p] \neq v-U[p]$   
 71 BY  $\langle 2 \rangle 2$  DEF *Inv, InvF1, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 72  $\langle 2 \rangle QED$   
 73 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 74  $\langle 1 \rangle 4. InvF2'$   
 75  $\langle 2 \rangle SUFFICES\ ASSUME\ NEW\ p-1 \in PROCESSES',$   
 76  $NEW\ t \in M'$   
 77 PROVE  $(\wedge pc[p-1] = \text{"F2"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 78  $\wedge t.op[p-1] = \text{"F"}$   
 79  $\wedge t.arg[p-1] \in NodeSet$   
 80  $\wedge SameRoot(t, c[p-1], t.arg[p-1])$   
 81  $\wedge InvF2All(p-1, t)$   
 82  $\wedge pc[p-1] = \text{"F2U1"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 83  $\wedge t.op[p-1] = \text{"U"}$   
 84  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 85  $\wedge SameRoot(t, c[p-1], u-U[p-1])$   
 86  $\wedge InvF2All(p-1, t)$   
 87  $\wedge pc[p-1] = \text{"F2U2"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 88  $\wedge t.op[p-1] = \text{"U"}$   
 89  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 90  $\wedge InvU2All(p-1, t)$

91  $\wedge \text{SameRoot}(t, c[p_{-1}], v_{-U}[p_{-1}])$   
 92  $\wedge \text{InvF2All}(p_{-1}, t)$   
 93  $\wedge pc[p_{-1}] = \text{"F2U7"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
 94  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 95  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 96  $\wedge \text{InvU7All}(p_{-1}, t)$   
 97  $\wedge \text{SameRoot}(t, c[p_{-1}], u_{-U}[p_{-1}])$   
 98  $\wedge \text{InvF2All}(p_{-1}, t)$   
 99  $\wedge pc[p_{-1}] = \text{"F2U8"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
 100  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 101  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 102  $\wedge \text{InvU8All}(p_{-1}, t)$   
 103  $\wedge \text{SameRoot}(t, c[p_{-1}], v_{-U}[p_{-1}])$   
 104  $\wedge \text{InvF2All}(p_{-1}, t))'$   
 105 BY DEF *InvF2*  
 106  $\langle 2 \rangle 1.$ CASE  $u_{-U}[p] = v_{-U}[p]$   
 107  $\langle 3 \rangle$  USE  $\langle 2 \rangle 1$   
 108  $\langle 3 \rangle$  PICK  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
 109  $\wedge t.\text{sigma} = told.\text{sigma}$   
 110  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
 111  $\wedge t.\text{op} = told.\text{op}$   
 112  $\wedge t.\text{arg} = told.\text{arg}$   
 113 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 114  $\langle 3 \rangle$  QED  
 115 BY DEF *Inv, InvF2, InvF2All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Same*  
 116  $\langle 2 \rangle 2.$ CASE  $u_{-U}[p] \neq v_{-U}[p]$   
 117 BY  $\langle 2 \rangle 2$  DEF *Inv, InvF2, InvF2All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Sam*  
 118  $\langle 2 \rangle$  QED  
 119 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 120  $\langle 1 \rangle 5.$  *InvF3'*  
 121  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p_{-1} \in \text{PROCESSES'}$ ,  
 122 NEW  $t \in M'$   
 123 PROVE  $(\wedge pc[p_{-1}] = \text{"F3"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
 124  $\wedge t.\text{op}[p_{-1}] = \text{"F"}$   
 125  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet}$   
 126  $\wedge \text{SameRoot}(t, c[p_{-1}], t.\text{arg}[p_{-1}])$   
 127  $\wedge \text{InvF3All}(p_{-1}, t)$   
 128  $\wedge pc[p_{-1}] = \text{"F3U1"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
 129  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 130  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 131  $\wedge \text{SameRoot}(t, c[p_{-1}], u_{-U}[p_{-1}])$   
 132  $\wedge \text{InvF3All}(p_{-1}, t)$   
 133  $\wedge pc[p_{-1}] = \text{"F3U2"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
 134  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 135  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$

136  $\wedge \text{InvU2All}(p_{-1}, t)$   
137  $\wedge \text{SameRoot}(t, c[p_{-1}], v_{-U}[p_{-1}])$   
138  $\wedge \text{InvF3All}(p_{-1}, t)$   
139  $\wedge pc[p_{-1}] = \text{"F3U7"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
140  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
141  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
142  $\wedge \text{InvU7All}(p_{-1}, t)$   
143  $\wedge \text{SameRoot}(t, c[p_{-1}], u_{-U}[p_{-1}])$   
144  $\wedge \text{InvF3All}(p_{-1}, t)$   
145  $\wedge pc[p_{-1}] = \text{"F3U8"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
146  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
147  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
148  $\wedge \text{InvU8All}(p_{-1}, t)$   
149  $\wedge \text{SameRoot}(t, c[p_{-1}], v_{-U}[p_{-1}])$   
150  $\wedge \text{InvF3All}(p_{-1}, t))'$   
151 BY DEF *InvF3*  
152  $\langle 2 \rangle 1.$ CASE  $u_{-U}[p] = v_{-U}[p]$   
153  $\langle 3 \rangle$  USE  $\langle 2 \rangle 1$   
154  $\langle 3 \rangle$  PICK  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
155  $\wedge t.\text{sigma} = told.\text{sigma}$   
156  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
157  $\wedge t.\text{op} = told.\text{op}$   
158  $\wedge t.\text{arg} = told.\text{arg}$   
159 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
160  $\langle 3 \rangle$  QED  
161 BY DEF *Inv, InvF3, InvF3All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Same*  
162  $\langle 2 \rangle 2.$ CASE  $u_{-U}[p] \neq v_{-U}[p]$   
163 BY  $\langle 2 \rangle 2$  DEF *Inv, InvF3, InvF3All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Sam*  
164  $\langle 2 \rangle$  QED  
165 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
166  $\langle 1 \rangle 6.$  *InvF4'*  
167  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p_{-1} \in \text{PROCESSES'}$ ,  
168 NEW  $t \in M'$   
169 PROVE  $(\wedge pc[p_{-1}] = \text{"F4"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
170  $\wedge t.\text{op}[p_{-1}] = \text{"F"}$   
171  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet}$   
172  $\wedge \text{SameRoot}(t, c[p_{-1}], t.\text{arg}[p_{-1}])$   
173  $\wedge \text{InvF4All}(p_{-1}, t)$   
174  $\wedge pc[p_{-1}] = \text{"F4U1"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
175  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
176  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
177  $\wedge \text{SameRoot}(t, c[p_{-1}], u_{-U}[p_{-1}])$   
178  $\wedge \text{InvF4All}(p_{-1}, t)$   
179  $\wedge pc[p_{-1}] = \text{"F4U2"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
180  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$

181  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
182  $\wedge InvU2All(p_{-1}, t)$   
183  $\wedge SameRoot(t, c[p_{-1}], v_{-}U[p_{-1}])$   
184  $\wedge InvF4All(p_{-1}, t)$   
185  $\wedge pc[p_{-1}] = \text{"F4U7"} \Rightarrow \wedge t.ret[p_{-1}] \in \{BOT, ACK\}$   
186  $\wedge t.op[p_{-1}] = \text{"U"}$   
187  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
188  $\wedge InvU7All(p_{-1}, t)$   
189  $\wedge SameRoot(t, c[p_{-1}], u_{-}U[p_{-1}])$   
190  $\wedge InvF4All(p_{-1}, t)$   
191  $\wedge pc[p_{-1}] = \text{"F4U8"} \Rightarrow \wedge t.ret[p_{-1}] \in \{BOT, ACK\}$   
192  $\wedge t.op[p_{-1}] = \text{"U"}$   
193  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
194  $\wedge InvU8All(p_{-1}, t)$   
195  $\wedge SameRoot(t, c[p_{-1}], v_{-}U[p_{-1}])$   
196  $\wedge InvF4All(p_{-1}, t))'$   
197 BY DEF *InvF4*  
198  $\langle 2 \rangle 1. \text{CASE } u_{-}U[p] = v_{-}U[p]$   
199  $\langle 3 \rangle \text{ USE } \langle 2 \rangle 1$   
200  $\langle 3 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
201  $\wedge t.sigma = told.sigma$   
202  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
203  $\wedge t.op = told.op$   
204  $\wedge t.arg = told.arg$   
205 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
206  $\langle 3 \rangle \text{ QED}$   
207 BY DEF *Inv, InvF4, InvF4All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Same*  
208  $\langle 2 \rangle 2. \text{CASE } u_{-}U[p] \neq v_{-}U[p]$   
209 BY  $\langle 2 \rangle 2$  DEF *Inv, InvF4, InvF4All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, Sam*  
210  $\langle 2 \rangle \text{ QED}$   
211 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
212  $\langle 1 \rangle 7. InvF5'$   
213  $\langle 2 \rangle \text{ SUFFICES ASSUME NEW } p_{-1} \in PROCESSES',$   
214  $\text{NEW } t \in M'$   
215 PROVE  $(\wedge pc[p_{-1}] = \text{"F5"} \Rightarrow \wedge t.ret[p_{-1}] = BOT$   
216  $\wedge t.op[p_{-1}] = \text{"F"}$   
217  $\wedge t.arg[p_{-1}] \in NodeSet$   
218  $\wedge SameRoot(t, c[p_{-1}], t.arg[p_{-1}])$   
219  $\wedge InvF5All(p_{-1}, t)$   
220  $\wedge pc[p_{-1}] = \text{"F5U1"} \Rightarrow \wedge t.ret[p_{-1}] = BOT$   
221  $\wedge t.op[p_{-1}] = \text{"U"}$   
222  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
223  $\wedge SameRoot(t, c[p_{-1}], u_{-}U[p_{-1}])$   
224  $\wedge InvF5All(p_{-1}, t)$   
225  $\wedge pc[p_{-1}] = \text{"F5U2"} \Rightarrow \wedge t.ret[p_{-1}] = BOT$

226  $\wedge t.op[p_{-1}] = \text{"U"}$   
 227  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 228  $\wedge InvU2All(p_{-1}, t)$   
 229  $\wedge SameRoot(t, c[p_{-1}], v\_U[p_{-1}])$   
 230  $\wedge InvF5All(p_{-1}, t)$   
 231  $\wedge pc[p_{-1}] = \text{"F5U7"} \Rightarrow \wedge t.ret[p_{-1}] \in \{BOT, ACK\}$   
 232  $\wedge t.op[p_{-1}] = \text{"U"}$   
 233  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 234  $\wedge InvU7All(p_{-1}, t)$   
 235  $\wedge SameRoot(t, c[p_{-1}], u\_U[p_{-1}])$   
 236  $\wedge InvF5All(p_{-1}, t)$   
 237  $\wedge pc[p_{-1}] = \text{"F5U8"} \Rightarrow \wedge t.ret[p_{-1}] \in \{BOT, ACK\}$   
 238  $\wedge t.op[p_{-1}] = \text{"U"}$   
 239  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 240  $\wedge InvU8All(p_{-1}, t)$   
 241  $\wedge SameRoot(t, c[p_{-1}], v\_U[p_{-1}])$   
 242  $\wedge InvF5All(p_{-1}, t))'$   
 243 BY DEF  $InvF5$   
 244  $\langle 2 \rangle 1. (pc[p_{-1}] = \text{"F5"} \Rightarrow \wedge t.ret[p_{-1}] = BOT$   
 245  $\wedge t.op[p_{-1}] = \text{"F"}$   
 246  $\wedge t.arg[p_{-1}] \in NodeSet$   
 247  $\wedge SameRoot(t, c[p_{-1}], t.arg[p_{-1}])$   
 248  $\wedge InvF5All(p_{-1}, t))'$   
 249  $\langle 3 \rangle 1. CASE \ u\_U[p] = v\_U[p]$   
 250  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 251  $\langle 4 \rangle PICK \ told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 252  $\wedge t.sigma = told.sigma$   
 253  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 254  $\wedge t.op = told.op$   
 255  $\wedge t.arg = told.arg$   
 256 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet$   
 257  $\langle 4 \rangle QED$   
 258 BY DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 259  $\langle 3 \rangle 2. CASE \ u\_U[p] \neq v\_U[p]$   
 260 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 261  $\langle 3 \rangle QED$   
 262 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 263  $\langle 2 \rangle 2. (pc[p_{-1}] = \text{"F5U1"} \Rightarrow \wedge t.ret[p_{-1}] = BOT$   
 264  $\wedge t.op[p_{-1}] = \text{"U"}$   
 265  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 266  $\wedge SameRoot(t, c[p_{-1}], u\_U[p_{-1}])$   
 267  $\wedge InvF5All(p_{-1}, t))'$   
 268  $\langle 3 \rangle 1. CASE \ u\_U[p] = v\_U[p]$   
 269  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 270  $\langle 4 \rangle PICK \ told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$

271  $\wedge t.\sigma = told.\sigma$   
 272  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 273  $\wedge t.op = told.op$   
 274  $\wedge t.arg = told.arg$   
 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  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 280  $\langle 3 \rangle$  QED  
 281 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 282  $\langle 2 \rangle 3$ .  $(pc[p\_1] = "F5U2" \Rightarrow \wedge t.ret[p\_1] = BOT$   
 283  $\wedge t.op[p\_1] = "U"$   
 284  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 285  $\wedge InvU2All(p\_1, t)$   
 286  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 287  $\wedge InvF5All(p\_1, t))'$   
 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  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 291  $\wedge t.\sigma = told.\sigma$   
 292  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 293  $\wedge t.op = told.op$   
 294  $\wedge t.arg = told.arg$   
 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  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 300  $\langle 3 \rangle$  QED  
 301 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 302  $\langle 2 \rangle 4$ .  $(pc[p\_1] = "F5U7" \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 303  $\wedge t.op[p\_1] = "U"$   
 304  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 305  $\wedge InvU7All(p\_1, t)$   
 306  $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$   
 307  $\wedge InvF5All(p\_1, t))'$   
 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  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 311  $\wedge t.\sigma = told.\sigma$   
 312  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 313  $\wedge t.op = told.op$   
 314  $\wedge t.arg = told.arg$   
 315 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet$ .

316  $\langle 4 \rangle$  QED  
 317 BY DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 318  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 319 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 320  $\langle 3 \rangle$  QED  
 321 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 322  $\langle 2 \rangle 5$ .  $(pc[p\_1] = \text{"F5U8"} \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 323  $\wedge t.op[p\_1] = \text{"U"}$   
 324  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 325  $\wedge InvU8All(p\_1, t)$   
 326  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 327  $\wedge InvF5All(p\_1, t))'$   
 328  $\langle 3 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
 329  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 330  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 331  $\wedge t.sigma = told.sigma$   
 332  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 333  $\wedge t.op = told.op$   
 334  $\wedge t.arg = told.arg$   
 335 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet$   
 336  $\langle 4 \rangle$  QED  
 337 BY DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 338  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 339 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF5, InvF5All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 340  $\langle 3 \rangle$  QED  
 341 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 342  $\langle 2 \rangle 6$ . QED  
 343 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3, \langle 2 \rangle 4, \langle 2 \rangle 5$   
 344  $\langle 1 \rangle 8$ .  $InvF6'$   
 345  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,  
 346 NEW  $t \in M'$   
 347 PROVE  $(\wedge pc[p\_1] = \text{"F6"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 348  $\wedge t.op[p\_1] = \text{"F"}$   
 349  $\wedge t.arg[p\_1] \in NodeSet$   
 350  $\wedge SameRoot(t, c[p\_1], t.arg[p\_1])$   
 351  $\wedge InvF6All(p\_1, t)$   
 352  $\wedge pc[p\_1] = \text{"F6U1"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 353  $\wedge t.op[p\_1] = \text{"U"}$   
 354  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 355  $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$   
 356  $\wedge InvF6All(p\_1, t)$   
 357  $\wedge pc[p\_1] = \text{"F6U2"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 358  $\wedge t.op[p\_1] = \text{"U"}$   
 359  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 360  $\wedge InvU2All(p\_1, t)$



361  $\wedge \text{SameRoot}(t, c[p_{-1}], v\_U[p_{-1}])$   
 362  $\wedge \text{InvF6All}(p_{-1}, t)$   
 363  $\wedge pc[p_{-1}] = \text{"F6U7"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
 364  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 365  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 366  $\wedge \text{InvU7All}(p_{-1}, t)$   
 367  $\wedge \text{SameRoot}(t, c[p_{-1}], u\_U[p_{-1}])$   
 368  $\wedge \text{InvF6All}(p_{-1}, t)$   
 369  $\wedge pc[p_{-1}] = \text{"F6U8"} \Rightarrow \wedge t.\text{ret}[p_{-1}] \in \{BOT, ACK\}$   
 370  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 371  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 372  $\wedge \text{InvU8All}(p_{-1}, t)$   
 373  $\wedge \text{SameRoot}(t, c[p_{-1}], v\_U[p_{-1}])$   
 374  $\wedge \text{InvF6All}(p_{-1}, t))'$   
 375 BY DEF *InvF6*  
 376  $\langle 2 \rangle 1. (pc[p_{-1}] = \text{"F6"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
 377  $\wedge t.\text{op}[p_{-1}] = \text{"F"}$   
 378  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet}$   
 379  $\wedge \text{SameRoot}(t, c[p_{-1}], t.\text{arg}[p_{-1}])$   
 380  $\wedge \text{InvF6All}(p_{-1}, t))'$   
 381  $\langle 3 \rangle 1. \text{CASE } u\_U[p] = v\_U[p]$   
 382  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
 383  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
 384  $\wedge t.\text{sigma} = told.\text{sigma}$   
 385  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
 386  $\wedge t.\text{op} = told.\text{op}$   
 387  $\wedge t.\text{arg} = told.\text{arg}$   
 388 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet*  
 389  $\langle 4 \rangle \text{ QED}$   
 390 BY DEF *Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S*  
 391  $\langle 3 \rangle 2. \text{CASE } u\_U[p] \neq v\_U[p]$   
 392 BY  $\langle 3 \rangle 2$  DEF *Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S*  
 393  $\langle 3 \rangle \text{ QED}$   
 394 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 395  $\langle 2 \rangle 2. (pc[p_{-1}] = \text{"F6U1"} \Rightarrow \wedge t.\text{ret}[p_{-1}] = BOT$   
 396  $\wedge t.\text{op}[p_{-1}] = \text{"U"}$   
 397  $\wedge t.\text{arg}[p_{-1}] \in \text{NodeSet} \times \text{NodeSet}$   
 398  $\wedge \text{SameRoot}(t, c[p_{-1}], u\_U[p_{-1}])$   
 399  $\wedge \text{InvF6All}(p_{-1}, t))'$   
 400  $\langle 3 \rangle 1. \text{CASE } u\_U[p] = v\_U[p]$   
 401  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
 402  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
 403  $\wedge t.\text{sigma} = told.\text{sigma}$   
 404  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
 405  $\wedge t.\text{op} = told.\text{op}$

406  $\wedge t.arg = told.arg$   
 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  $Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 412  $\langle 3 \rangle$  QED  
 413 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 414  $\langle 2 \rangle 3. (pc[p\_1] = \text{"F6U2"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 415  $\wedge t.op[p\_1] = \text{"U"}$   
 416  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 417  $\wedge InvU2All(p\_1, t)$   
 418  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 419  $\wedge InvF6All(p\_1, t))'$   
 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  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 423  $\wedge t.sigma = told.sigma$   
 424  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 425  $\wedge t.op = told.op$   
 426  $\wedge t.arg = told.arg$   
 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  $Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 432  $\langle 3 \rangle$  QED  
 433 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 434  $\langle 2 \rangle 4. (pc[p\_1] = \text{"F6U7"} \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 435  $\wedge t.op[p\_1] = \text{"U"}$   
 436  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 437  $\wedge InvU7All(p\_1, t)$   
 438  $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$   
 439  $\wedge InvF6All(p\_1, t))'$   
 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  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 443  $\wedge t.sigma = told.sigma$   
 444  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 445  $\wedge t.op = told.op$   
 446  $\wedge t.arg = told.arg$   
 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  $u\_U[p] \neq v\_U[p]$

451 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 452  $\langle 3 \rangle$  QED  
 453 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 454  $\langle 2 \rangle 5. (pc[p\_1] = \text{"F6U8"} \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 455  $\wedge t.op[p\_1] = \text{"U"}$   
 456  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 457  $\wedge InvU8All(p\_1, t)$   
 458  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 459  $\wedge InvF6All(p\_1, t))'$   
 460  $\langle 3 \rangle 1.CASE u\_U[p] = v\_U[p]$   
 461  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 462  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 463  $\wedge t.sigma = told.sigma$   
 464  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 465  $\wedge t.op = told.op$   
 466  $\wedge t.arg = told.arg$   
 467 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, S$   
 468  $\langle 4 \rangle$  QED  
 469 BY DEF  $Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 470  $\langle 3 \rangle 2.CASE u\_U[p] \neq v\_U[p]$   
 471 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF6, InvF6All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 472  $\langle 3 \rangle$  QED  
 473 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 474  $\langle 2 \rangle 6.$  QED  
 475 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3, \langle 2 \rangle 4, \langle 2 \rangle 5$   
 476  $\langle 1 \rangle 9. InvF7'$   
 477  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,  
 478 NEW  $t \in M'$   
 479 PROVE  $(\wedge pc[p\_1] = \text{"F7"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 480  $\wedge t.op[p\_1] = \text{"F"}$   
 481  $\wedge t.arg[p\_1] \in NodeSet$   
 482  $\wedge SameRoot(t, c[p\_1], t.arg[p\_1])$   
 483  $\wedge InvF7All(p\_1, t)$   
 484  $\wedge pc[p\_1] = \text{"F7U1"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 485  $\wedge t.op[p\_1] = \text{"U"}$   
 486  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 487  $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$   
 488  $\wedge InvF7All(p\_1, t)$   
 489  $\wedge pc[p\_1] = \text{"F7U2"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 490  $\wedge t.op[p\_1] = \text{"U"}$   
 491  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 492  $\wedge InvU2All(p\_1, t)$   
 493  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 494  $\wedge InvF7All(p\_1, t)$   
 495  $\wedge pc[p\_1] = \text{"F7U7"} \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$

496  $\wedge t.op[p-1] = \text{"U"}$   
 497  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 498  $\wedge InvU7All(p-1, t)$   
 499  $\wedge SameRoot(t, c[p-1], u\_U[p-1])$   
 500  $\wedge InvF7All(p-1, t)$   
 501  $\wedge pc[p-1] = \text{"F7U8"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
 502  $\wedge t.op[p-1] = \text{"U"}$   
 503  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 504  $\wedge InvU8All(p-1, t)$   
 505  $\wedge SameRoot(t, c[p-1], v\_U[p-1])$   
 506  $\wedge InvF7All(p-1, t))'$   
 507 BY DEF *InvF7*  
 508  $\langle 2 \rangle 1. (pc[p-1] = \text{"F7"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 509  $\wedge t.op[p-1] = \text{"F"}$   
 510  $\wedge t.arg[p-1] \in NodeSet$   
 511  $\wedge SameRoot(t, c[p-1], t.arg[p-1])$   
 512  $\wedge InvF7All(p-1, t))'$   
 513  $\langle 3 \rangle 1. CASE u\_U[p] = v\_U[p]$   
 514  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 515  $\langle 4 \rangle PICK told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 516  $\wedge t.sigma = told.sigma$   
 517  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 518  $\wedge t.op = told.op$   
 519  $\wedge t.arg = told.arg$   
 520 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet*  
 521  $\langle 4 \rangle QED$   
 522 BY DEF *Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S*  
 523  $\langle 3 \rangle 2. CASE u\_U[p] \neq v\_U[p]$   
 524 BY  $\langle 3 \rangle 2$  DEF *Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S*  
 525  $\langle 3 \rangle QED$   
 526 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 527  $\langle 2 \rangle 2. (pc[p-1] = \text{"F7U1"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 528  $\wedge t.op[p-1] = \text{"U"}$   
 529  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 530  $\wedge SameRoot(t, c[p-1], u\_U[p-1])$   
 531  $\wedge InvF7All(p-1, t))'$   
 532  $\langle 3 \rangle 1. CASE u\_U[p] = v\_U[p]$   
 533  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 534  $\langle 4 \rangle PICK told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 535  $\wedge t.sigma = told.sigma$   
 536  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 537  $\wedge t.op = told.op$   
 538  $\wedge t.arg = told.arg$   
 539 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet*  
 540  $\langle 4 \rangle QED$

541 BY DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 542  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 543 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 544  $\langle 3 \rangle$  QED  
 545 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 546  $\langle 2 \rangle 3$ .  $(pc[p\_1] = \text{"F7U2"} \Rightarrow \wedge t.ret[p\_1] = BOT$   
 547  $\wedge t.op[p\_1] = \text{"U"}$   
 548  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 549  $\wedge InvU2All(p\_1, t)$   
 550  $\wedge SameRoot(t, c[p\_1], v\_U[p\_1])$   
 551  $\wedge InvF7All(p\_1, t))'$   
 552  $\langle 3 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
 553  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 554  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 555  $\wedge t.sigma = told.sigma$   
 556  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 557  $\wedge t.op = told.op$   
 558  $\wedge t.arg = told.arg$   
 559 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet$   
 560  $\langle 4 \rangle$  QED  
 561 BY DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 562  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 563 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 564  $\langle 3 \rangle$  QED  
 565 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 566  $\langle 2 \rangle 4$ .  $(pc[p\_1] = \text{"F7U7"} \Rightarrow \wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 567  $\wedge t.op[p\_1] = \text{"U"}$   
 568  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 569  $\wedge InvU7All(p\_1, t)$   
 570  $\wedge SameRoot(t, c[p\_1], u\_U[p\_1])$   
 571  $\wedge InvF7All(p\_1, t))'$   
 572  $\langle 3 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
 573  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 574  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 575  $\wedge t.sigma = told.sigma$   
 576  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 577  $\wedge t.op = told.op$   
 578  $\wedge t.arg = told.arg$   
 579 BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet$   
 580  $\langle 4 \rangle$  QED  
 581 BY DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 582  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 583 BY  $\langle 3 \rangle 2$  DEF  $Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
 584  $\langle 3 \rangle$  QED  
 585 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$

586  $\langle 2 \rangle 5. (pc[p-1] = \text{"F7U8"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
587  $\wedge t.op[p-1] = \text{"U"}$   
588  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
589  $\wedge InvU8All(p-1, t)$   
590  $\wedge SameRoot(t, c[p-1], v_U[p-1])$   
591  $\wedge InvF7All(p-1, t))'$   
592  $\langle 3 \rangle 1. CASE \ u_U[p] = v_U[p]$   
593  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
594  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
595  $\wedge t.sigma = told.sigma$   
596  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
597  $\wedge t.op = told.op$   
598  $\wedge t.arg = told.arg$   
599  $\text{BY DEF } Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.$   
600  $\langle 4 \rangle \text{ QED}$   
601  $\text{BY DEF } Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
602  $\langle 3 \rangle 2. CASE \ u_U[p] \neq v_U[p]$   
603  $\text{BY } \langle 3 \rangle 2 \text{ DEF } Inv, InvF7, InvF7All, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, S$   
604  $\langle 3 \rangle \text{ QED}$   
605  $\text{BY } \langle 3 \rangle 1, \langle 3 \rangle 2$   
606  $\langle 2 \rangle 6. \text{ QED}$   
607  $\text{BY } \langle 2 \rangle 1, \langle 2 \rangle 2, \langle 2 \rangle 3, \langle 2 \rangle 4, \langle 2 \rangle 5$   
608  $\langle 1 \rangle 10. InvFR'$   
609  $\langle 2 \rangle \text{ SUFFICES ASSUME NEW } p-1 \in PROCESSES',$   
610  $\text{NEW } t \in M'$   
611  $\text{PROVE } (\wedge pc[p-1] = \text{"FR"} \Rightarrow \wedge t.ret[p-1] = u_F[p-1]$   
612  $\wedge t.op[p-1] = \text{"F"}$   
613  $\wedge t.arg[p-1] \in NodeSet$   
614  $\wedge SameRoot(t, t.arg[p-1], u_F[p-1])$   
615  $\wedge SameRoot(t, c[p-1], u_F[p-1])$   
616  $\wedge pc[p-1] = \text{"FRU1"} \Rightarrow \wedge t.ret[p-1] = BOT$   
617  $\wedge t.op[p-1] = \text{"U"}$   
618  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
619  $\wedge SameRoot(t, c[p-1], u_U[p-1])$   
620  $\wedge SameRoot(t, c[p-1], u_F[p-1])$   
621  $\wedge pc[p-1] = \text{"FRU2"} \Rightarrow \wedge t.ret[p-1] = BOT$   
622  $\wedge t.op[p-1] = \text{"U"}$   
623  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
624  $\wedge InvU2All(p-1, t)$   
625  $\wedge SameRoot(t, c[p-1], v_U[p-1])$   
626  $\wedge pc[p-1] = \text{"FRU7"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
627  $\wedge t.op[p-1] = \text{"U"}$   
628  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
629  $\wedge InvU7All(p-1, t)$   
630  $\wedge SameRoot(t, c[p-1], u_U[p-1])$

631  $\wedge pc[p-1] = \text{"FRU8"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
 632  $\wedge t.op[p-1] = \text{"U"}$   
 633  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 634  $\wedge InvU8All(p-1, t)$   
 635  $\wedge SameRoot(t, c[p-1], v-U[p-1]))'$   
 636 BY DEF *InvFR*  
 637  $\langle 2 \rangle 1. (pc[p-1] = \text{"FR"} \Rightarrow \wedge t.ret[p-1] = u-F[p-1]$   
 638  $\wedge t.op[p-1] = \text{"F"}$   
 639  $\wedge t.arg[p-1] \in NodeSet$   
 640  $\wedge SameRoot(t, t.arg[p-1], u-F[p-1])$   
 641  $\wedge SameRoot(t, c[p-1], u-F[p-1]))'$   
 642  $\langle 3 \rangle 1. CASE u-U[p] = v-U[p]$   
 643  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 644  $\langle 4 \rangle PICK told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 645  $\wedge t.sigma = told.sigma$   
 646  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 647  $\wedge t.op = told.op$   
 648  $\wedge t.arg = told.arg$   
 649 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
 650  $\langle 4 \rangle QED$   
 651 BY DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 652  $\langle 3 \rangle 2. CASE u-U[p] \neq v-U[p]$   
 653 BY  $\langle 3 \rangle 2$  DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot,*  
 654  $\langle 3 \rangle QED$   
 655 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 656  $\langle 2 \rangle 2. (pc[p-1] = \text{"FRU1"} \Rightarrow \wedge t.ret[p-1] = BOT$   
 657  $\wedge t.op[p-1] = \text{"U"}$   
 658  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 659  $\wedge SameRoot(t, c[p-1], u-U[p-1])$   
 660  $\wedge SameRoot(t, c[p-1], u-F[p-1]))'$   
 661  $\langle 3 \rangle 1. CASE u-U[p] = v-U[p]$   
 662  $\langle 4 \rangle USE \langle 3 \rangle 1$   
 663  $\langle 4 \rangle PICK told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 664  $\wedge t.sigma = told.sigma$   
 665  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 666  $\wedge t.op = told.op$   
 667  $\wedge t.arg = told.arg$   
 668 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
 669  $\langle 4 \rangle QED$   
 670 BY DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 671  $\langle 3 \rangle 2. CASE u-U[p] \neq v-U[p]$   
 672 BY  $\langle 3 \rangle 2$  DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot,*  
 673  $\langle 3 \rangle QED$   
 674 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 675  $\langle 2 \rangle 3. (pc[p-1] = \text{"FRU2"} \Rightarrow \wedge t.ret[p-1] = BOT$

676  $\wedge t.op[p-1] = \text{"U"}$   
677  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
678  $\wedge InvU2All(p-1, t)$   
679  $\wedge SameRoot(t, c[p-1], v_U[p-1]))'$   
680  $\langle 3 \rangle 1.CASE \ u_U[p] = v_U[p]$   
681  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
682  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
683  $\wedge t.sigma = told.sigma$   
684  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
685  $\wedge t.op = told.op$   
686  $\wedge t.arg = told.arg$   
687 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
688  $\langle 4 \rangle \text{ QED}$   
689 BY DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
690  $\langle 3 \rangle 2.CASE \ u_U[p] \neq v_U[p]$   
691 BY  $\langle 3 \rangle 2$  DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot,*  
692  $\langle 3 \rangle \text{ QED}$   
693 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
694  $\langle 2 \rangle 4. (pc[p-1] = \text{"FRU7"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
695  $\wedge t.op[p-1] = \text{"U"}$   
696  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
697  $\wedge InvU7All(p-1, t)$   
698  $\wedge SameRoot(t, c[p-1], u_U[p-1]))'$   
699  $\langle 3 \rangle 1.CASE \ u_U[p] = v_U[p]$   
700  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
701  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
702  $\wedge t.sigma = told.sigma$   
703  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
704  $\wedge t.op = told.op$   
705  $\wedge t.arg = told.arg$   
706 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
707  $\langle 4 \rangle \text{ QED}$   
708 BY DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
709  $\langle 3 \rangle 2.CASE \ u_U[p] \neq v_U[p]$   
710 BY  $\langle 3 \rangle 2$  DEF *Inv, InvFR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot,*  
711  $\langle 3 \rangle \text{ QED}$   
712 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
713  $\langle 2 \rangle 5. (pc[p-1] = \text{"FRU8"} \Rightarrow \wedge t.ret[p-1] \in \{BOT, ACK\}$   
714  $\wedge t.op[p-1] = \text{"U"}$   
715  $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
716  $\wedge InvU8All(p-1, t)$   
717  $\wedge SameRoot(t, c[p-1], v_U[p-1]))'$   
718  $\langle 3 \rangle 1.CASE \ u_U[p] = v_U[p]$   
719  $\langle 4 \rangle \text{ USE } \langle 3 \rangle 1$   
720  $\langle 4 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$



721  $\wedge t.\sigma = told.\sigma$   
722  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
723  $\wedge t.op = told.op$   
724  $\wedge t.arg = told.arg$   
725 BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid\_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*,  
726  $\langle 4 \rangle$  QED  
727 BY DEF *Inv*, *InvFR*, *TypeOK*, *Valid\_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*  
728  $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
729 BY  $\langle 3 \rangle 2$  DEF *Inv*, *InvFR*, *TypeOK*, *Valid\_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*,  
730  $\langle 3 \rangle$  QED  
731 BY  $\langle 3 \rangle 1$ ,  $\langle 3 \rangle 2$   
732  $\langle 2 \rangle 6$ . QED  
733 BY  $\langle 2 \rangle 1$ ,  $\langle 2 \rangle 2$ ,  $\langle 2 \rangle 3$ ,  $\langle 2 \rangle 4$ ,  $\langle 2 \rangle 5$   
734  $\langle 1 \rangle 11$ . *InvU1'*  
735  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,  
736 NEW  $t \in M'$ ,  
737  $(pc[p\_1] = "U1")'$   
738 PROVE (  $\wedge t.ret[p\_1] = BOT$   
739  $\wedge t.op[p\_1] = "U"$   
740  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$ )'  
741 BY DEF *InvU1*  
742  $\langle 2 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
743  $\langle 3 \rangle$  USE  $\langle 2 \rangle 1$   
744  $\langle 3 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
745  $\wedge t.\sigma = told.\sigma$   
746  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
747  $\wedge t.op = told.op$   
748  $\wedge t.arg = told.arg$   
749 BY DEF *Inv*, *InvU3*, *TypeOK*, *Valid\_pc*, *PCSet*, *Configs*, *StateSet*, *OpSet*, *ArgSet*, *ReturnSet*, *Va*,  
750  $\langle 3 \rangle$  QED  
751 BY DEF *Inv*, *InvU1*, *TypeOK*, *Valid\_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*  
752  $\langle 2 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
753 BY  $\langle 2 \rangle 2$  DEF *Inv*, *InvU1*, *TypeOK*, *Valid\_pc*, *PCSet*, *InvU2All*, *InvU7All*, *InvU8All*, *SameRoot*  
754  $\langle 2 \rangle$  QED  
755 BY  $\langle 2 \rangle 1$ ,  $\langle 2 \rangle 2$   
756  $\langle 1 \rangle 12$ . *InvU2'*  
757  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,  
758 NEW  $t \in M'$ ,  
759  $(pc[p\_1] = "U2")'$   
760 PROVE (  $\wedge t.ret[p\_1] = BOT$   
761  $\wedge t.op[p\_1] = "U"$   
762  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
763  $\wedge InvU2All(p\_1, t))'$   
764 BY DEF *InvU2*  
765  $\langle 2 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$

```

766      <3> USE <2>1
767      <3> PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$ 
768               $\wedge t.sigma = told.sigma$ 
769               $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$ 
770               $\wedge t.op = told.op$ 
771               $\wedge t.arg = told.arg$ 
772      BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va$ 
773      <3> QED
774      BY DEF  $Inv, InvU2, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot$ 
775      <2>2.CASE  $u\_U[p] \neq v\_U[p]$ 
776      BY <2>2 DEF  $Inv, InvU2, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot$ 
777      <2> QED
778      BY <2>1, <2>2
779      <1>13.  $InvU3'$ 
780      <2> SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,
781              NEW  $t \in M'$ ,
782               $(pc[p\_1] = "U3")'$ 
783      PROVE  $(\wedge t.ret[p\_1] \in \{BOT, ACK\}$ 
784               $\wedge t.op[p\_1] = "U"$ 
785               $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$ 
786               $\wedge SameRoot(t, t.arg[p\_1][1], u\_U[p\_1])$ 
787               $\wedge SameRoot(t, t.arg[p\_1][2], v\_U[p\_1])$ 
788               $\wedge t.ret[p\_1] = ACK \Rightarrow SameRoot(t, u\_U[p\_1], v\_U[p\_1]))'$ 
789      BY DEF  $InvU3$ 
790      <2>1.CASE  $u\_U[p] = v\_U[p]$ 
791      <3> USE <2>1
792      <3> PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$ 
793               $\wedge t.sigma = told.sigma$ 
794               $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$ 
795               $\wedge t.op = told.op$ 
796               $\wedge t.arg = told.arg$ 
797      BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va$ 
798      <3> QED
799      BY DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot$ 
800      <2>2.CASE  $u\_U[p] \neq v\_U[p]$ 
801      BY <2>2 DEF  $Inv, InvU3, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot$ 
802      <2> QED
803      BY <2>1, <2>2
804      <1>14.  $InvU4'$ 
805      <2> SUFFICES ASSUME NEW  $p\_1 \in PROCESSES'$ ,
806              NEW  $t \in M'$ ,
807               $(pc[p\_1] = "U4")'$ 
808      PROVE  $(\wedge t.ret[p\_1] \in \{BOT, ACK\}$ 
809               $\wedge t.op[p\_1] = "U"$ 
810               $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$ 

```

811  $\wedge \text{SameRoot}(t, t.\text{arg}[p-1][1], u\_U[p-1])$   
812  $\wedge \text{SameRoot}(t, t.\text{arg}[p-1][2], v\_U[p-1])$   
813  $\wedge (t.\text{ret}[p-1] = \text{ACK} \Rightarrow \text{SameRoot}(t, u\_U[p-1], v\_U[p-1]))$   
814  $\wedge u\_U[p-1] \neq v\_U[p-1])'$   
815 BY DEF *InvU4*  
816  $\langle 2 \rangle 1.$ CASE  $pc[p-1] = \text{"U3"}$   
817  $\langle 3 \rangle$  USE  $\langle 2 \rangle 1$   
818  $\langle 3 \rangle 1.$ CASE  $u\_U[p] = v\_U[p]$   
819  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
820  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
821  $\wedge t.\text{sigma} = told.\text{sigma}$   
822  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = \text{ACK}]$   
823  $\wedge t.\text{op} = told.\text{op}$   
824  $\wedge t.\text{arg} = told.\text{arg}$   
825 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
826  $\langle 4 \rangle$  QED  
827 BY DEF *Inv, InvU4, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
828  $\langle 3 \rangle 2.$ CASE  $u\_U[p] \neq v\_U[p]$   
829 BY  $\langle 3 \rangle 2$  DEF *Inv, InvU3, InvU4, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot.*  
830  $\langle 3 \rangle$  QED  
831 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
832  $\langle 2 \rangle 2.$ CASE  $pc[p-1] = \text{"U4"}$   
833  $\langle 3 \rangle$  USE  $\langle 2 \rangle 2$   
834  $\langle 3 \rangle 1.$ CASE  $u\_U[p] = v\_U[p]$   
835  $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
836  $\langle 4 \rangle$  PICK  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
837  $\wedge t.\text{sigma} = told.\text{sigma}$   
838  $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = \text{ACK}]$   
839  $\wedge t.\text{op} = told.\text{op}$   
840  $\wedge t.\text{arg} = told.\text{arg}$   
841 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet.*  
842  $\langle 4 \rangle$  QED  
843 BY DEF *Inv, InvU4, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
844  $\langle 3 \rangle 2.$ CASE  $u\_U[p] \neq v\_U[p]$   
845 BY  $\langle 3 \rangle 2$  DEF *Inv, InvU4, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot.*  
846  $\langle 3 \rangle$  QED  
847 BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
848  $\langle 2 \rangle$  QED  
849 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$  DEF *Inv, TypeOK, Valid\_pc, PCSet*  
850  $\langle 1 \rangle 15.$  *InvU5'*  
851  $\langle 2 \rangle$  SUFFICES ASSUME NEW  $p-1 \in PROCESSES'$ ,  
852 NEW  $t \in M'$ ,  
853  $(pc[p-1] = \text{"U5"})'$   
854 PROVE  $(\wedge t.\text{ret}[p-1] \in \{BOT, ACK\}$   
855  $\wedge t.\text{op}[p-1] = \text{"U"})'$

856  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 857  $\wedge InvU5All(p\_1, t))'$   
 858 BY DEF *InvU5*  
 859  $\langle 2 \rangle 1.CASE\ u\_U[p] = v\_U[p]$   
 860  $\langle 3 \rangle USE\ \langle 2 \rangle 1$   
 861  $\langle 3 \rangle PICK\ told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 862  $\wedge t.sigma = told.sigma$   
 863  $\wedge t.ret = [told.ret\ EXCEPT\ ![p] = ACK]$   
 864  $\wedge t.op = told.op$   
 865  $\wedge t.arg = told.arg$   
 866 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 867  $\langle 3 \rangle QED$   
 868 BY DEF *Inv, InvU5, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot, InvU*  
 869  $\langle 2 \rangle 2.CASE\ u\_U[p] \neq v\_U[p]$   
 870 BY  $\langle 2 \rangle 2$  DEF *Inv, InvU5, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot, InvU*  
 871  $\langle 2 \rangle QED$   
 872 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 873  $\langle 1 \rangle 16. InvU6'$   
 874  $\langle 2 \rangle SUFFICES\ ASSUME\ NEW\ p\_1 \in PROCESSES',$   
 875  $NEW\ t \in M',$   
 876  $(pc[p\_1] = "U6")'$   
 877 PROVE  $(\wedge t.ret[p\_1] \in \{BOT, ACK\}$   
 878  $\wedge t.op[p\_1] = "U"$   
 879  $\wedge t.arg[p\_1] \in NodeSet \times NodeSet$   
 880  $\wedge InvU6All(p\_1, t))'$   
 881 BY DEF *InvU6*  
 882  $\langle 2 \rangle 1.CASE\ u\_U[p] = v\_U[p]$   
 883  $\langle 3 \rangle USE\ \langle 2 \rangle 1$   
 884  $\langle 3 \rangle PICK\ told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 885  $\wedge t.sigma = told.sigma$   
 886  $\wedge t.ret = [told.ret\ EXCEPT\ ![p] = ACK]$   
 887  $\wedge t.op = told.op$   
 888  $\wedge t.arg = told.arg$   
 889 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 890  $\langle 3 \rangle QED$   
 891 BY DEF *Inv, InvU6, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot, InvU*  
 892  $\langle 2 \rangle 2.CASE\ u\_U[p] \neq v\_U[p]$   
 893 BY  $\langle 2 \rangle 2$  DEF *Inv, InvU6, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot, InvU*  
 894  $\langle 2 \rangle QED$   
 895 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 896  $\langle 1 \rangle 17. InvU7'$   
 897  $\langle 2 \rangle SUFFICES\ ASSUME\ NEW\ p\_1 \in PROCESSES',$   
 898  $NEW\ t \in M',$   
 899  $(pc[p\_1] = "U7")'$   
 900 PROVE  $(\wedge t.ret[p\_1] \in \{BOT, ACK\}$

901  $\wedge t.op[p_{-1}] = \text{"U"}$   
 902  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 903  $\wedge InvU7All(p_{-1}, t))'$   
 904 BY DEF *InvU7*  
 905  $\langle 2 \rangle 1. \text{CASE } u\_U[p] = v\_U[p]$   
 906  $\langle 3 \rangle \text{ USE } \langle 2 \rangle 1$   
 907  $\langle 3 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 908  $\wedge t.sigma = told.sigma$   
 909  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 910  $\wedge t.op = told.op$   
 911  $\wedge t.arg = told.arg$   
 912 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 913  $\langle 3 \rangle \text{ QED}$   
 914 BY DEF *Inv, InvU7, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 915  $\langle 2 \rangle 2. \text{CASE } u\_U[p] \neq v\_U[p]$   
 916 BY  $\langle 2 \rangle 2$  DEF *Inv, InvU7, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 917  $\langle 2 \rangle \text{ QED}$   
 918 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 919  $\langle 1 \rangle 18. InvU8'$   
 920  $\langle 2 \rangle \text{ SUFFICES ASSUME NEW } p_{-1} \in PROCESSES',$   
 921  $\text{NEW } t \in M',$   
 922  $(pc[p_{-1}] = \text{"U8"})'$   
 923 PROVE  $(\wedge t.ret[p_{-1}] \in \{BOT, ACK\}$   
 924  $\wedge t.op[p_{-1}] = \text{"U"}$   
 925  $\wedge t.arg[p_{-1}] \in NodeSet \times NodeSet$   
 926  $\wedge InvU8All(p_{-1}, t))'$   
 927 BY DEF *InvU8*  
 928  $\langle 2 \rangle 1. \text{CASE } u\_U[p] = v\_U[p]$   
 929  $\langle 3 \rangle \text{ USE } \langle 2 \rangle 1$   
 930  $\langle 3 \rangle \text{ PICK } told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 931  $\wedge t.sigma = told.sigma$   
 932  $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 933  $\wedge t.op = told.op$   
 934  $\wedge t.arg = told.arg$   
 935 BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 936  $\langle 3 \rangle \text{ QED}$   
 937 BY DEF *Inv, InvU8, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 938  $\langle 2 \rangle 2. \text{CASE } u\_U[p] \neq v\_U[p]$   
 939 BY  $\langle 2 \rangle 2$  DEF *Inv, InvU8, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 940  $\langle 2 \rangle \text{ QED}$   
 941 BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$   
 942  $\langle 1 \rangle 19. InvUR'$   
 943  $\langle 2 \rangle \text{ SUFFICES ASSUME NEW } p_{-1} \in PROCESSES',$   
 944  $\text{NEW } t \in M',$   
 945  $(pc[p_{-1}] = \text{"UR"})'$

946                   PROVE (    $\wedge t.ret[p-1] = ACK$   
 947                                $\wedge t.op[p-1] = "U"$   
 948                                $\wedge t.arg[p-1] \in NodeSet \times NodeSet$   
 949                                $\wedge SameRoot(t, t.arg[p-1][1], u\_U[p-1])$   
 950                                $\wedge SameRoot(t, t.arg[p-1][2], v\_U[p-1])$   
 951                                $\wedge SameRoot(t, u\_U[p-1], v\_U[p-1]))'$   
 952       BY DEF *InvUR*  
 953    $\langle 2 \rangle 1$ .CASE  $pc[p-1] = "U3"$   
 954      $\langle 3 \rangle$  USE  $\langle 2 \rangle 1$   
 955      $\langle 3 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
 956        $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 957        $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 958                                $\wedge t.sigma = told.sigma$   
 959                                $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 960                                $\wedge t.op = told.op$   
 961                                $\wedge t.arg = told.arg$   
 962       BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet*  
 963        $\langle 4 \rangle p = p-1$   
 964       BY DEF *Inv, TypeOK, Valid\_pc, PCSet*  
 965        $\langle 4 \rangle$  QED  
 966       BY DEF *Inv, InvU3, InvUR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 967        $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 968       BY  $\langle 3 \rangle 2$  DEF *Inv, InvU3, InvUR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 969        $\langle 3 \rangle$  QED  
 970       BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 971    $\langle 2 \rangle 2$ .CASE  $pc[p-1] = "UR"$   
 972      $\langle 3 \rangle$  USE  $\langle 2 \rangle 2$   
 973      $\langle 3 \rangle 1$ .CASE  $u\_U[p] = v\_U[p]$   
 974        $\langle 4 \rangle$  USE  $\langle 3 \rangle 1$   
 975        $\langle 4 \rangle$  PICK  $told \in M : \wedge told.ret[p] \in \{BOT, ACK\}$   
 976                                $\wedge t.sigma = told.sigma$   
 977                                $\wedge t.ret = [told.ret \text{ EXCEPT } ![p] = ACK]$   
 978                                $\wedge t.op = told.op$   
 979                                $\wedge t.arg = told.arg$   
 980       BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet*  
 981        $\langle 4 \rangle$  QED  
 982       BY DEF *Inv, InvUR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 983        $\langle 3 \rangle 2$ .CASE  $u\_U[p] \neq v\_U[p]$   
 984       BY  $\langle 3 \rangle 2$  DEF *Inv, InvUR, TypeOK, Valid\_pc, PCSet, InvU2All, InvU7All, InvU8All, SameRoot*  
 985        $\langle 3 \rangle$  QED  
 986       BY  $\langle 3 \rangle 1, \langle 3 \rangle 2$   
 987    $\langle 2 \rangle$  QED  
 988   BY  $\langle 2 \rangle 1, \langle 2 \rangle 2$  DEF *Inv, TypeOK, Valid\_pc, PCSet*  
 989    $\langle 1 \rangle 20$ . *SigmaRespectsShared'*  
 990

991      $\langle 2 \rangle$  SUFFICES ASSUME NEW  $t \in M'$ ,  
 992             NEW  $i \in \text{NodeSet}'$   
 993             PROVE    $(\wedge F[i].\text{bit} = 0 \Rightarrow t.\text{sigma}[i] = t.\text{sigma}[F[i].\text{parent}]$   
 994                      $\wedge F[i].\text{bit} = 1 \Rightarrow t.\text{sigma}[i] = i)'$   
 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  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
 999              $\wedge t.\text{sigma} = told.\text{sigma}$   
 1000              $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
 1001              $\wedge t.\text{op} = told.\text{op}$   
 1002              $\wedge t.\text{arg} = told.\text{arg}$   
 1003         BY DEF *Inv, InvU3, 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  $i \in \text{NodeSet}'$ ,  
 1013              $(t.\text{sigma}[i] = i)'$   
 1014             PROVE    $(F[i].\text{bit} = 1)'$   
 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  $told \in M : \wedge told.\text{ret}[p] \in \{BOT, ACK\}$   
 1019              $\wedge t.\text{sigma} = told.\text{sigma}$   
 1020              $\wedge t.\text{ret} = [told.\text{ret} \text{ EXCEPT } ![p] = ACK]$   
 1021              $\wedge t.\text{op} = told.\text{op}$   
 1022              $\wedge t.\text{arg} = told.\text{arg}$   
 1023         BY DEF *Inv, InvU3, 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  $told \in M : told.\text{ret}[p] = BOT \vee told.\text{ret}[p] = ACK$   
 1034             BY DEF *Inv, InvU3, TypeOK, Valid\_pc, PCSet, Configs, StateSet, OpSet, ArgSet, ReturnSet, Va*  
 1035          $\langle 3 \rangle a$ .  $told \in \text{Configs}$

```

1036         BY DEF Inv, TypeOK, Valid_M
1037     <3>1.CASE told.ret[p] = BOT
1038         <4> DEFINE t  $\triangleq$  [sigma  $\mapsto$  told.sigma,
1039             ret  $\mapsto$  [told.ret EXCEPT ![p] = ACK],
1040             op  $\mapsto$  told.op,
1041             arg  $\mapsto$  told.arg]
1042         <4> t  $\in$  M'
1043         BY <3>1 DEF Inv, Configs, StateSet, OpSet, ArgSet, ReturnSet, TypeOK, t, Valid_M
1044         <4> QED
1045         BY DEF Inv, Linearizable
1046     <3>2.CASE told.ret[p] = ACK
1047         <4> told  $\in$  M'
1048         BY <3>2 DEF Inv, Configs, StateSet, OpSet, ArgSet, ReturnSet, TypeOK, Valid_M
1049         <4> QED
1050         BY DEF Inv, Linearizable
1051     <3> QED
1052     BY <3>1, <3>2
1053 <2>2.CASE u_U[p]  $\neq$  v_U[p]
1054     BY <2>2 DEF Inv, Linearizable
1055 <2> QED
1056     BY <2>1, <2>2
1057 <1>23. QED
1058     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,
1060 |
    \ * 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

```