

1 MODULE *Inv*

2 EXTENDS *Implementation*, *TypeSafety*

4 $\text{SameRoot}(t, i, j) \triangleq t.\text{sigma}[i] = t.\text{sigma}[j]$

6 $\text{SigmaRespectsShared} \triangleq \forall t \in M : \forall i \in \text{NodeSet} : \begin{array}{ll} \wedge F[i].\text{bit} = 0 & \Rightarrow t.\text{sigma}[i] = t.\text{sigma}[F[i].\text{parent}] \\ \wedge F[i].\text{bit} = 1 & \Rightarrow t.\text{sigma}[i] = i \end{array}$

9 $\text{SharedRespectsSigma} \triangleq \forall t \in M : \forall i \in \text{NodeSet} : \wedge t.\text{sigma}[i] = i \Rightarrow F[i].\text{bit} = 1$

13 $\text{InvF2All}(p, t) \triangleq \wedge \text{SameRoot}(t, c[p], u_F[p])$

15 $\text{InvF3All}(p, t) \triangleq \wedge F[u_F[p]].\text{bit} = 0$
16 $\wedge \text{SameRoot}(t, c[p], u_F[p])$

18 $\text{InvF4All}(p, t) \triangleq \wedge F[u_F[p]].\text{bit} = 0$
19 $\wedge a_F[p].\text{bit} = 0$
20 $\wedge \text{SameRoot}(t, c[p], a_F[p].\text{parent})$
21 $\wedge \text{SameRoot}(t, c[p], u_F[p])$

23 $\text{InvF5All}(p, t) \triangleq \wedge F[u_F[p]].\text{bit} = 0$
24 $\wedge a_F[p].\text{bit} = 0$
25 $\wedge \text{SameRoot}(t, c[p], a_F[p].\text{parent})$
26 $\wedge \text{SameRoot}(t, c[p], u_F[p])$
27 $\wedge b_F[p].\text{bit} = 0 \Rightarrow \text{SameRoot}(t, a_F[p].\text{parent}, b_F[p].\text{parent})$
28 $\wedge b_F[p].\text{bit} = 1 \Rightarrow t.\text{sigma}[a_F[p].\text{parent}] = a_F[p].\text{parent}$

30 $\text{InvF6All}(p, t) \triangleq \wedge F[u_F[p]].\text{bit} = 0$
31 $\wedge a_F[p].\text{bit} = 0$
32 $\wedge F[a_F[p].\text{parent}].\text{bit} = 0$
33 $\wedge b_F[p].\text{bit} = 0$
34 $\wedge \text{SameRoot}(t, c[p], a_F[p].\text{parent})$
35 $\wedge \text{SameRoot}(t, c[p], u_F[p])$
36 $\wedge \text{SameRoot}(t, a_F[p].\text{parent}, b_F[p].\text{parent})$

38 $\text{InvF7All}(p, t) \triangleq \wedge F[u_F[p]].\text{bit} = 0$
39 $\wedge a_F[p].\text{bit} = 0$
40 $\wedge \text{SameRoot}(t, c[p], a_F[p].\text{parent})$
41 $\wedge \text{SameRoot}(t, c[p], u_F[p])$

43 $\text{InvU2All}(p, t) \triangleq \wedge \text{SameRoot}(t, t.\text{arg}[p][1], u_U[p])$
44 $\wedge \text{SameRoot}(t, t.\text{arg}[p][2], v_U[p])$

47 $\text{InvU5All}(p, t) \triangleq \wedge \text{SameRoot}(t, t.\text{arg}[p][1], u_U[p])$
48 $\wedge \text{SameRoot}(t, t.\text{arg}[p][2], v_U[p])$
49 $\wedge u_U[p] \neq v_U[p]$

50		$\wedge a_U[p].bit = 0 \Rightarrow SameRoot(t, a_U[p].parent, u_U[p])$
51		$\wedge a_U[p].bit = 1 \Rightarrow t.sigma[u_U[p]] = u_U[p]$
53	$InvU6All(p, t) \triangleq$	$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
54		$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
55		$\wedge u_U[p] \neq v_U[p]$
56		$\wedge a_U[p].bit = 0 \Rightarrow SameRoot(t, a_U[p].parent, u_U[p])$
57		$\wedge a_U[p].bit = 1 \Rightarrow t.sigma[u_U[p]] = u_U[p]$
58		$\wedge b_U[p].bit = 0 \Rightarrow SameRoot(t, b_U[p].parent, v_U[p])$
59		$\wedge b_U[p].bit = 1 \Rightarrow t.sigma[v_U[p]] = v_U[p]$
61	$InvU7All(p, t) \triangleq$	$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
62		$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
63		$\wedge t.ret[p] = ACK \Rightarrow SameRoot(t, u_U[p], v_U[p])$
65	$InvU8All(p, t) \triangleq$	$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
66		$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
67		$\wedge t.ret[p] = ACK \Rightarrow SameRoot(t, u_U[p], v_U[p])$
69	$InvDecide \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$
70		$\wedge pc[p] = "0" \Rightarrow \wedge t.ret[p] = BOT$
71		$\wedge t.op[p] = BOT$
72		$\wedge t.arg[p] = BOT$
73	$InvF1 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$
74		$\wedge pc[p] = "F1" \Rightarrow \wedge t.ret[p] = BOT$
75		$\wedge t.op[p] = "F"$
76		$\wedge t.arg[p] \in NodeSet$
77		$\wedge SameRoot(t, c[p], t.arg[p])$
78		$\wedge pc[p] = "F1U1" \Rightarrow \wedge t.ret[p] = BOT$
79		$\wedge t.op[p] = "U"$
80		$\wedge t.arg[p] \in NodeSet \times NodeSet$
81		$\wedge SameRoot(t, c[p], u_U[p])$
82		$\wedge pc[p] = "F1U2" \Rightarrow \wedge t.ret[p] = BOT$
83		$\wedge t.op[p] = "U"$
84		$\wedge t.arg[p] \in NodeSet \times NodeSet$
85		$\wedge InvU2All(p, t)$
86		$\wedge SameRoot(t, c[p], v_U[p])$
87		$\wedge pc[p] = "F1U7" \Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
88		$\wedge t.op[p] = "U"$
89		$\wedge t.arg[p] \in NodeSet \times NodeSet$
90		$\wedge InvU7All(p, t)$
91		$\wedge SameRoot(t, c[p], u_U[p])$
92		$\wedge pc[p] = "F1U8" \Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
93		$\wedge t.op[p] = "U"$
94		$\wedge t.arg[p] \in NodeSet \times NodeSet$
95		$\wedge InvU8All(p, t)$

96			$\wedge \text{SameRoot}(t, c[p], v_U[p])$
97	$\text{InvF2} \triangleq$	$\forall p \in \text{PROCESSES} : \forall t \in M :$	
98		$\wedge pc[p] = \text{"F2"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
99			$\wedge t.\text{op}[p] = \text{"F"}$
100			$\wedge t.\text{arg}[p] \in \text{NodeSet}$
101			$\wedge \text{SameRoot}(t, c[p], t.\text{arg}[p])$
102			$\wedge \text{InvF2All}(p, t)$
103		$\wedge pc[p] = \text{"F2U1"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
104			$\wedge t.\text{op}[p] = \text{"U"}$
105			$\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
106			$\wedge \text{SameRoot}(t, c[p], u_U[p])$
107			$\wedge \text{InvF2All}(p, t)$
108		$\wedge pc[p] = \text{"F2U2"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
109			$\wedge t.\text{op}[p] = \text{"U"}$
110			$\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
111			$\wedge \text{InvU2All}(p, t)$
112			$\wedge \text{SameRoot}(t, c[p], v_U[p])$
113			$\wedge \text{InvF2All}(p, t)$
114		$\wedge pc[p] = \text{"F2U7"} \Rightarrow$	$\wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$
115			$\wedge t.\text{op}[p] = \text{"U"}$
116			$\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
117			$\wedge \text{InvU7All}(p, t)$
118			$\wedge \text{SameRoot}(t, c[p], u_U[p])$
119			$\wedge \text{InvF2All}(p, t)$
120		$\wedge pc[p] = \text{"F2U8"} \Rightarrow$	$\wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$
121			$\wedge t.\text{op}[p] = \text{"U"}$
122			$\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
123			$\wedge \text{InvU8All}(p, t)$
124			$\wedge \text{SameRoot}(t, c[p], v_U[p])$
125			$\wedge \text{InvF2All}(p, t)$
128	$\text{InvF3} \triangleq$	$\forall p \in \text{PROCESSES} : \forall t \in M :$	
129		$\wedge pc[p] = \text{"F3"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
130			$\wedge t.\text{op}[p] = \text{"F"}$
131			$\wedge t.\text{arg}[p] \in \text{NodeSet}$
132			$\wedge \text{SameRoot}(t, c[p], t.\text{arg}[p])$
133			$\wedge \text{InvF3All}(p, t)$
134		$\wedge pc[p] = \text{"F3U1"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
135			$\wedge t.\text{op}[p] = \text{"U"}$
136			$\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
137			$\wedge \text{SameRoot}(t, c[p], u_U[p])$
138			$\wedge \text{InvF3All}(p, t)$
139		$\wedge pc[p] = \text{"F3U2"} \Rightarrow$	$\wedge t.\text{ret}[p] = \text{BOT}$
140			$\wedge t.\text{op}[p] = \text{"U"}$

141		$\wedge t.arg[p] \in NodeSet \times NodeSet$
142		$\wedge InvU2All(p, t)$
143		$\wedge SameRoot(t, c[p], v_U[p])$
144		$\wedge InvF3All(p, t)$
145	$\wedge pc[p] = \text{"F3U7"} \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
146		$\wedge t.op[p] = \text{"U"}$
147		$\wedge t.arg[p] \in NodeSet \times NodeSet$
148		$\wedge InvU7All(p, t)$
149		$\wedge SameRoot(t, c[p], u_U[p])$
150		$\wedge InvF3All(p, t)$
151	$\wedge pc[p] = \text{"F3U8"} \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
152		$\wedge t.op[p] = \text{"U"}$
153		$\wedge t.arg[p] \in NodeSet \times NodeSet$
154		$\wedge InvU8All(p, t)$
155		$\wedge SameRoot(t, c[p], v_U[p])$
156		$\wedge InvF3All(p, t)$
158	$InvF4 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$
159		$\wedge pc[p] = \text{"F4"} \Rightarrow$
160		$\wedge t.ret[p] = BOT$
161		$\wedge t.op[p] = \text{"F"}$
162		$\wedge t.arg[p] \in NodeSet$
163		$\wedge SameRoot(t, c[p], t.arg[p])$
164		$\wedge InvF4All(p, t)$
165	$\wedge pc[p] = \text{"F4U1"} \Rightarrow$	$\wedge t.ret[p] = BOT$
166		$\wedge t.op[p] = \text{"U"}$
167		$\wedge t.arg[p] \in NodeSet \times NodeSet$
168		$\wedge SameRoot(t, c[p], u_U[p])$
169		$\wedge InvF4All(p, t)$
170	$\wedge pc[p] = \text{"F4U2"} \Rightarrow$	$\wedge t.ret[p] = BOT$
171		$\wedge t.op[p] = \text{"U"}$
172		$\wedge t.arg[p] \in NodeSet \times NodeSet$
173		$\wedge InvU2All(p, t)$
174		$\wedge SameRoot(t, c[p], v_U[p])$
175		$\wedge InvF4All(p, t)$
176	$\wedge pc[p] = \text{"F4U7"} \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
177		$\wedge t.op[p] = \text{"U"}$
178		$\wedge t.arg[p] \in NodeSet \times NodeSet$
179		$\wedge InvU7All(p, t)$
180		$\wedge SameRoot(t, c[p], u_U[p])$
181		$\wedge InvF4All(p, t)$
182	$\wedge pc[p] = \text{"F4U8"} \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
183		$\wedge t.op[p] = \text{"U"}$
184		$\wedge t.arg[p] \in NodeSet \times NodeSet$
185		$\wedge InvU8All(p, t)$
		$\wedge SameRoot(t, c[p], v_U[p])$

186

 $\wedge \text{InvF4All}(p, t)$ 189 $\text{InvF5} \triangleq$ $\forall p \in \text{PROCESSES} : \forall t \in M :$

190

 $\wedge pc[p] = \text{"F5"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

191

 $\wedge t.\text{op}[p] = \text{"F"}$

192

 $\wedge t.\text{arg}[p] \in \text{NodeSet}$

193

 $\wedge \text{SameRoot}(t, c[p], t.\text{arg}[p])$

194

 $\wedge \text{InvF5All}(p, t)$

195

 $\wedge pc[p] = \text{"F5U1"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

196

 $\wedge t.\text{op}[p] = \text{"U"}$

197

 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

198

 $\wedge \text{SameRoot}(t, c[p], u_U[p])$

199

 $\wedge \text{InvF5All}(p, t)$

200

 $\wedge pc[p] = \text{"F5U2"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

201

 $\wedge t.\text{op}[p] = \text{"U"}$

202

 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

203

 $\wedge \text{InvU2All}(p, t)$

204

 $\wedge \text{SameRoot}(t, c[p], v_U[p])$

205

 $\wedge \text{InvF5All}(p, t)$

206

 $\wedge pc[p] = \text{"F5U7"} \Rightarrow \wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$

207

 $\wedge t.\text{op}[p] = \text{"U"}$

208

 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

209

 $\wedge \text{InvU7All}(p, t)$

210

 $\wedge \text{SameRoot}(t, c[p], u_U[p])$

211

 $\wedge \text{InvF5All}(p, t)$

212

 $\wedge pc[p] = \text{"F5U8"} \Rightarrow \wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$

213

 $\wedge t.\text{op}[p] = \text{"U"}$

214

 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

215

 $\wedge \text{InvU8All}(p, t)$

216

 $\wedge \text{SameRoot}(t, c[p], v_U[p])$

217

 $\wedge \text{InvF5All}(p, t)$ 219 $\text{InvF6} \triangleq$ $\forall p \in \text{PROCESSES} : \forall t \in M :$

220

 $\wedge pc[p] = \text{"F6"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

221

 $\wedge t.\text{op}[p] = \text{"F"}$

222

 $\wedge t.\text{arg}[p] \in \text{NodeSet}$

223

 $\wedge \text{SameRoot}(t, c[p], t.\text{arg}[p])$

224

 $\wedge \text{InvF6All}(p, t)$

225

 $\wedge pc[p] = \text{"F6U1"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

226

 $\wedge t.\text{op}[p] = \text{"U"}$

227

 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

228

 $\wedge \text{SameRoot}(t, c[p], u_U[p])$

229

 $\wedge \text{InvF6All}(p, t)$

230

 $\wedge pc[p] = \text{"F6U2"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$

231

 $\wedge t.\text{op}[p] = \text{"U"}$

232		$\wedge t.arg[p] \in NodeSet \times NodeSet$
233		$\wedge InvU2All(p, t)$
234		$\wedge SameRoot(t, c[p], v_U[p])$
235		$\wedge InvF6All(p, t)$
236	$\wedge pc[p] = "F6U7" \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
237		$\wedge t.op[p] = "U"$
238		$\wedge t.arg[p] \in NodeSet \times NodeSet$
239		$\wedge InvU7All(p, t)$
240		$\wedge SameRoot(t, c[p], u_U[p])$
241		$\wedge InvF6All(p, t)$
242	$\wedge pc[p] = "F6U8" \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
243		$\wedge t.op[p] = "U"$
244		$\wedge t.arg[p] \in NodeSet \times NodeSet$
245		$\wedge InvU8All(p, t)$
246		$\wedge SameRoot(t, c[p], v_U[p])$
247		$\wedge InvF6All(p, t)$
250	$InvF7 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$
251		$\wedge pc[p] = "F7" \Rightarrow \wedge t.ret[p] = BOT$
252		$\wedge t.op[p] = "F"$
253		$\wedge t.arg[p] \in NodeSet$
254		$\wedge SameRoot(t, c[p], t.arg[p])$
255		$\wedge InvF7All(p, t)$
256	$\wedge pc[p] = "F7U1" \Rightarrow$	$\wedge t.ret[p] = BOT$
257		$\wedge t.op[p] = "U"$
258		$\wedge t.arg[p] \in NodeSet \times NodeSet$
259		$\wedge SameRoot(t, c[p], u_U[p])$
260		$\wedge InvF7All(p, t)$
261	$\wedge pc[p] = "F7U2" \Rightarrow$	$\wedge t.ret[p] = BOT$
262		$\wedge t.op[p] = "U"$
263		$\wedge t.arg[p] \in NodeSet \times NodeSet$
264		$\wedge InvU2All(p, t)$
265		$\wedge SameRoot(t, c[p], v_U[p])$
266		$\wedge InvF7All(p, t)$
267	$\wedge pc[p] = "F7U7" \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
268		$\wedge t.op[p] = "U"$
269		$\wedge t.arg[p] \in NodeSet \times NodeSet$
270		$\wedge InvU7All(p, t)$
271		$\wedge SameRoot(t, c[p], u_U[p])$
272		$\wedge InvF7All(p, t)$
273	$\wedge pc[p] = "F7U8" \Rightarrow$	$\wedge t.ret[p] \in \{BOT, ACK\}$
274		$\wedge t.op[p] = "U"$
275		$\wedge t.arg[p] \in NodeSet \times NodeSet$
276		$\wedge InvU8All(p, t)$

277 $\wedge \text{SameRoot}(t, c[p], v_U[p])$
 278 $\wedge \text{InvF7All}(p, t)$

281 $\text{InvFR} \triangleq \forall p \in \text{PROCESSES} : \forall t \in M :$
 282 $\wedge pc[p] = \text{"FR"} \Rightarrow \wedge t.\text{ret}[p] = u_F[p]$
 283 $\wedge t.\text{op}[p] = \text{"F"}$
 284 $\wedge t.\text{arg}[p] \in \text{NodeSet}$
 285 $\wedge \text{SameRoot}(t, t.\text{arg}[p], u_F[p])$
 286 $\wedge \text{SameRoot}(t, c[p], u_F[p])$
 287 $\wedge pc[p] = \text{"FRU1"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$
 288 $\wedge t.\text{op}[p] = \text{"U"}$
 289 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
 290 $\wedge \text{SameRoot}(t, c[p], u_U[p])$
 291 $\wedge \text{SameRoot}(t, c[p], u_F[p])$
 292 $\wedge pc[p] = \text{"FRU2"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$
 293 $\wedge t.\text{op}[p] = \text{"U"}$
 294 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
 295 $\wedge \text{InvU2All}(p, t)$
 296 $\wedge \text{SameRoot}(t, c[p], v_U[p])$

298 $\wedge pc[p] = \text{"FRU7"} \Rightarrow \wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$
 299 $\wedge t.\text{op}[p] = \text{"U"}$
 300 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
 301 $\wedge \text{InvU7All}(p, t)$
 302 $\wedge \text{SameRoot}(t, c[p], u_U[p])$
 303 $\wedge pc[p] = \text{"FRU8"} \Rightarrow \wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$
 304 $\wedge t.\text{op}[p] = \text{"U"}$
 305 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
 306 $\wedge \text{InvU8All}(p, t)$
 307 $\wedge \text{SameRoot}(t, c[p], v_U[p])$

309 $\text{InvU1} \triangleq \forall p \in \text{PROCESSES} : \forall t \in M :$
 310 $pc[p] = \text{"U1"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$
 311 $\wedge t.\text{op}[p] = \text{"U"}$
 312 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$

315 $\text{InvU2} \triangleq \forall p \in \text{PROCESSES} : \forall t \in M :$
 316 $pc[p] = \text{"U2"} \Rightarrow \wedge t.\text{ret}[p] = \text{BOT}$
 317 $\wedge t.\text{op}[p] = \text{"U"}$
 318 $\wedge t.\text{arg}[p] \in \text{NodeSet} \times \text{NodeSet}$
 319 $\wedge \text{InvU2All}(p, t)$

321 $\text{InvU3} \triangleq \forall p \in \text{PROCESSES} : \forall t \in M :$
 322 $pc[p] = \text{"U3"} \Rightarrow \wedge t.\text{ret}[p] \in \{\text{BOT}, \text{ACK}\}$
 323 $\wedge t.\text{op}[p] = \text{"U"}$

324			$\wedge t.arg[p] \in NodeSet \times NodeSet$
325			$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
326			$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
327			$\wedge t.ret[p] = ACK \Rightarrow SameRoot(t, u_U[p], v_U[p])$
328	$InvU4 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
329		$pc[p] = \text{"U4"}$	$\Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
330			$\wedge t.op[p] = \text{"U"}$
331			$\wedge t.arg[p] \in NodeSet \times NodeSet$
332			$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
333			$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
334			$\wedge t.ret[p] = ACK \Rightarrow SameRoot(t, u_U[p], v_U[p])$
335			$\wedge u_U[p] \neq v_U[p]$
337	$InvU5 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
338		$pc[p] = \text{"U5"}$	$\Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
339			$\wedge t.op[p] = \text{"U"}$
340			$\wedge t.arg[p] \in NodeSet \times NodeSet$
341			$\wedge InvU5All(p, t)$
342	$InvU6 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
343		$pc[p] = \text{"U6"}$	\Rightarrow
344			$\wedge t.ret[p] \in \{BOT, ACK\}$
345			$\wedge t.op[p] = \text{"U"}$
346			$\wedge t.arg[p] \in NodeSet \times NodeSet$
347			$\wedge InvU6All(p, t)$
349	$InvU7 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
350		$pc[p] = \text{"U7"}$	$\Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
351			$\wedge t.op[p] = \text{"U"}$
352			$\wedge t.arg[p] \in NodeSet \times NodeSet$
353			$\wedge InvU7All(p, t)$
355	$InvU8 \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
356		$pc[p] = \text{"U8"}$	$\Rightarrow \wedge t.ret[p] \in \{BOT, ACK\}$
357			$\wedge t.op[p] = \text{"U"}$
358			$\wedge t.arg[p] \in NodeSet \times NodeSet$
359			$\wedge InvU8All(p, t)$
361	$InvUR \triangleq$	$\forall p \in PROCESSES : \forall t \in M :$	
362		$pc[p] = \text{"UR"}$	$\Rightarrow \wedge t.ret[p] = ACK$
363			$\wedge t.op[p] = \text{"U"}$
364			$\wedge t.arg[p] \in NodeSet \times NodeSet$
365			$\wedge SameRoot(t, t.arg[p][1], u_U[p])$
366			$\wedge SameRoot(t, t.arg[p][2], v_U[p])$
367			$\wedge SameRoot(t, u_U[p], v_U[p])$
369	$Linearizable \triangleq$	$M \neq \{\}$	


```

371  $Inv \triangleq$   $\wedge TypeOK$ 
372            $\wedge InvDecide$ 
373            $\wedge InvF1$ 
374            $\wedge InvF2$ 
375            $\wedge InvF3$ 
376            $\wedge InvF4$ 
377            $\wedge InvF5$ 
378            $\wedge InvF6$ 
379            $\wedge InvF7$ 
380            $\wedge InvFR$ 
381            $\wedge InvU1$ 
382            $\wedge InvU2$ 
383            $\wedge InvU3$ 
384            $\wedge InvU4$ 
385            $\wedge InvU5$ 
386            $\wedge InvU6$ 
387            $\wedge InvU7$ 
388            $\wedge InvU8$ 
389            $\wedge InvUR$ 
390            $\wedge SigmaRespectsShared$ 
391            $\wedge SharedRespectsSigma$ 
392            $\wedge Linearizable$ 

```

```

394 |-----|
    \ * Modification History
    \ * Last modified Thu Apr 17 20:52:02 EDT 2025 by karunram
    \ * Created Thu Apr 03 22:44:42 EDT 2025 by karunram

```