MODULE *Inv*

EXTENDS *Implementation*, *TypeSafety*

$$SameRoot(t,\, i,\, j) \triangleq \quad t.sigma[i] = t.sigma[j]$$

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

$$InvF2All(p,\, t) \triangleq \quad \wedge\, SameRoot(t,\, c[p],\, u\_F[p])$$

$$InvF3All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, F[u\_F[p]].bit = 0 \\ \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \end{array}$$

$$InvF4All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, F[u\_F[p]].bit = 0 \\ \wedge\, a\_F[p].bit = 0 \\ \wedge\, SameRoot(t,\, c[p],\, a\_F[p].parent) \\ \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \end{array}$$

$$InvF5All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, F[u\_F[p]].bit = 0 \\ \wedge\, a\_F[p].bit = 0 \\ \wedge\, SameRoot(t,\, c[p],\, a\_F[p].parent) \\ \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \\ \wedge\, b\_F[p].bit = 0 \Rightarrow \wedge\, SameRoot(t,\, a\_F[p].parent,\, b\_F[p].parent) \\ \qquad\qquad\qquad\qquad\qquad\quad \wedge\, F[a\_F[p].parent].bit = 0 \end{array}$$

$$InvF6All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, F[u\_F[p]].bit = 0 \\ \wedge\, a\_F[p].bit = 0 \\ \wedge\, F[a\_F[p].parent].bit = 0 \\ \wedge\, b\_F[p].bit = 0 \\ \wedge\, SameRoot(t,\, c[p],\, a\_F[p].parent) \\ \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \\ \wedge\, SameRoot(t,\, a\_F[p].parent,\, b\_F[p].parent) \end{array}$$

$$InvF7All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, F[u\_F[p]].bit = 0 \\ \wedge\, a\_F[p].bit = 0 \\ \wedge\, SameRoot(t,\, c[p],\, a\_F[p].parent) \\ \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \end{array}$$

$$InvU2All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, SameRoot(t,\, t.arg[p][1],\, u\_U[p]) \\ \wedge\, SameRoot(t,\, t.arg[p][2],\, v\_U[p]) \end{array}$$

$$InvU5All(p,\, t) \triangleq \quad \begin{array}{l} \wedge\, SameRoot(t,\, t.arg[p][1],\, u\_U[p]) \\ \wedge\, SameRoot(t,\, t.arg[p][2],\, v\_U[p]) \\ \wedge\, u\_U[p] \neq v\_U[p] \\ \wedge\, a\_U[p].bit = 0 \;\Rightarrow SameRoot(t,\, a\_U[p].parent,\, u\_U[p]) \\ \wedge\, t.ret[p] = ACK \Rightarrow SameRoot(t,\, u\_U[p],\, v\_U[p]) \end{array}$$

$$
\begin{array}{lll}
50 & InvU6All(p,\ t) \triangleq & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
51 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
52 & & \land\ u\_U[p] \neq v\_U[p] \\
53 & & \land\ a\_U[p].bit = 0\ \Rightarrow SameRoot(t,\ a\_U[p].parent,\ u\_U[p]) \\
54 & & \land\ b\_U[p].bit = 0\ \Rightarrow SameRoot(t,\ b\_U[p].parent,\ v\_U[p]) \\
55 & & \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
\\
57 & InvU7All(p,\ t) \triangleq & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
58 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
59 & & \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
\\
61 & InvU8All(p,\ t) \triangleq & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
62 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
63 & & \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
\\
65 & InvDecide \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : \\
66 & & \qquad \land\ pc[p] = \text{“0”} \quad \Rightarrow\ \land\ t.ret[p] = BOT \\
67 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = BOT \\
68 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] = BOT \\
69 & InvF1 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : \\
70 & & \qquad \land\ pc[p] = \text{“F1”} \quad \Rightarrow\ \land\ t.ret[p] = BOT \\
71 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“F”} \\
72 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] \in NodeSet \\
73 & & \qquad\qquad\qquad\qquad\ \ \land\ SameRoot(t,\ c[p],\ t.arg[p]) \\
74 & & \qquad \land\ pc[p] = \text{“F1U1”} \ \Rightarrow\ \land\ t.ret[p] = BOT \\
75 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“U”} \\
76 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] \in NodeSet \times NodeSet \\
77 & & \qquad\qquad\qquad\qquad\ \ \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
78 & & \qquad \land\ pc[p] = \text{“F1U2”} \ \Rightarrow\ \land\ t.ret[p] = BOT \\
79 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“U”} \\
80 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] \in NodeSet \times NodeSet \\
81 & & \qquad\qquad\qquad\qquad\ \ \land\ InvU2All(p,\ t) \\
82 & & \qquad\qquad\qquad\qquad\ \ \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
83 & & \qquad \land\ pc[p] = \text{“F1U7”} \ \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
84 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“U”} \\
85 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] \in NodeSet \times NodeSet \\
86 & & \qquad\qquad\qquad\qquad\ \ \land\ InvU7All(p,\ t) \\
87 & & \qquad\qquad\qquad\qquad\ \ \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
88 & & \qquad \land\ pc[p] = \text{“F1U8”} \ \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
89 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“U”} \\
90 & & \qquad\qquad\qquad\qquad\ \ \land\ t.arg[p] \in NodeSet \times NodeSet \\
91 & & \qquad\qquad\qquad\qquad\ \ \land\ InvU8All(p,\ t) \\
92 & & \qquad\qquad\qquad\qquad\ \ \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
93 & InvF2 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : \\
94 & & \qquad \land\ pc[p] = \text{“F2”} \quad \Rightarrow\ \land\ t.ret[p] = BOT \\
95 & & \qquad\qquad\qquad\qquad\ \ \land\ t.op[p] = \text{“F”}
\end{array}
$$

$$
\begin{array}{lll}
 & & \wedge\ t.arg[p] \in NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \wedge\ InvF2All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F2U1”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF2All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F2U2”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF2All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F2U7”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU7All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF2All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F2U8”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU8All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF2All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
InvF3 \ \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & \wedge\ pc[p] = \text{“F3”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“F”} \\
 & & \wedge\ t.arg[p] \in NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \wedge\ InvF3All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F3U1”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF3All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F3U2”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF3All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
 & \land\ pc[p] = \text{“F3U7”} & \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU7All(p,\ t) \\
 & & \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \land\ InvF3All(p,\ t) \\
 & \land\ pc[p] = \text{“F3U8”} & \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU8All(p,\ t) \\
 & & \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \land\ InvF3All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
InvF4 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & \land\ pc[p] = \text{“F4”} & \Rightarrow\ \land\ t.ret[p] = BOT \\
 & & \land\ t.op[p] = \text{“F”} \\
 & & \land\ t.arg[p] \in NodeSet \\
 & & \land\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \land\ InvF4All(p,\ t) \\
 & \land\ pc[p] = \text{“F4U1”} & \Rightarrow\ \land\ t.ret[p] = BOT \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \land\ InvF4All(p,\ t) \\
 & \land\ pc[p] = \text{“F4U2”} & \Rightarrow\ \land\ t.ret[p] = BOT \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU2All(p,\ t) \\
 & & \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \land\ InvF4All(p,\ t) \\
 & \land\ pc[p] = \text{“F4U7”} & \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU7All(p,\ t) \\
 & & \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \land\ InvF4All(p,\ t) \\
 & \land\ pc[p] = \text{“F4U8”} & \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU8All(p,\ t) \\
 & & \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \land\ InvF4All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
InvF5 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & \land\ pc[p] = \text{“F5”} & \Rightarrow\ \land\ t.ret[p] \in \{BOT\} \cup NodeSet
\end{array}
$$

$$
\begin{array}{lll}
 & & \wedge\ t.op[p] = \text{“F”} \\
 & & \wedge\ t.arg[p] \in NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \wedge\ InvF5All(p,\ t) \\
 & & \wedge\ b\_F[p].bit = 0 \Rightarrow t.ret[p] = BOT \\
 & & \wedge\ b\_F[p].bit = 1 \Rightarrow t.ret[p] = a\_F[p].pa \\
 & \wedge\ pc[p] = \text{“F5U1”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF5All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F5U2”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF5All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F5U7”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU7All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF5All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F5U8”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU8All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF5All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
InvF6 \ \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & \wedge\ pc[p] = \text{“F6”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“F”} \\
 & & \wedge\ t.arg[p] \in NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U1”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U2”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U7”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU7All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U8”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU8All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
InvF7 \ \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & \wedge\ pc[p] = \text{“F7”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“F”} \\
 & & \wedge\ t.arg[p] \in NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ t.arg[p]) \\
 & & \wedge\ InvF7All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F7U1”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF7All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F7U2”} \ \Rightarrow & \wedge\ t.ret[p] = BOT \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF7All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F7U7”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU7All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF7All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F7U8”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU8All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF7All(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
\mathit{InvFR} \triangleq & \forall\, p \in \mathit{PROCESSES} : \forall\, t \in M : & \\
& \quad \wedge\ \mathit{pc}[p] = \text{“FR”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] = u\_F[p] \\
& & \wedge\ t.\mathit{op}[p] = \text{“F”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \\
& & \wedge\ \mathit{SameRoot}(t,\ t.\mathit{arg}[p],\ u\_F[p]) \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ u\_F[p]) \\
& \quad \wedge\ \mathit{pc}[p] = \text{“FRU1”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] = \mathit{BOT} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ u\_U[p]) \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ u\_F[p]) \\
& \quad \wedge\ \mathit{pc}[p] = \text{“FRU2”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] = \mathit{BOT} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{InvU2All}(p,\ t) \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ v\_U[p]) \\
& \quad \wedge\ \mathit{pc}[p] = \text{“FRU7”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] \in \{\mathit{BOT},\ \mathit{ACK}\} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{InvU7All}(p,\ t) \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ u\_U[p]) \\
& \quad \wedge\ \mathit{pc}[p] = \text{“FRU8”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] \in \{\mathit{BOT},\ \mathit{ACK}\} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{InvU8All}(p,\ t) \\
& & \wedge\ \mathit{SameRoot}(t,\ c[p],\ v\_U[p])
\end{array}
$$

$$
\begin{array}{lll}
\mathit{InvU1} \triangleq & \forall\, p \in \mathit{PROCESSES} : \forall\, t \in M : & \\
& \quad \mathit{pc}[p] = \text{“U1”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] = \mathit{BOT} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet}
\end{array}
$$

$$
\begin{array}{lll}
\mathit{InvU2} \triangleq & \forall\, p \in \mathit{PROCESSES} : \forall\, t \in M : & \\
& \quad \mathit{pc}[p] = \text{“U2”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] = \mathit{BOT} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{InvU2All}(p,\ t)
\end{array}
$$

$$
\begin{array}{lll}
\mathit{InvU3} \triangleq & \forall\, p \in \mathit{PROCESSES} : \forall\, t \in M : & \\
& \quad \mathit{pc}[p] = \text{“U3”} \quad \Rightarrow & \wedge\ t.\mathit{ret}[p] \in \{\mathit{BOT},\ \mathit{ACK}\} \\
& & \wedge\ t.\mathit{op}[p] = \text{“U”} \\
& & \wedge\ t.\mathit{arg}[p] \in \mathit{NodeSet} \times \mathit{NodeSet} \\
& & \wedge\ \mathit{SameRoot}(t,\ t.\mathit{arg}[p][1],\ u\_U[p]) \\
& & \wedge\ \mathit{SameRoot}(t,\ t.\mathit{arg}[p][2],\ v\_U[p])
\end{array}
$$

$$\wedge\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],$$

$$InvU4 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“U4”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ SameRoot(t,\ t.arg[p][1],\ u\_U[p])$$
$$\wedge\ SameRoot(t,\ t.arg[p][2],\ v\_U[p])$$
$$\wedge\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],$$
$$\wedge\ u\_U[p] \neq v\_U[p]$$

$$InvU5 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“U5”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU5All(p,\ t)$$

$$InvU6 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“U6”} \Rightarrow$$
$$\wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU6All(p,\ t)$$

$$InvU7 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“U7”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU7All(p,\ t)$$

$$InvU8 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“U8”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU8All(p,\ t)$$

$$InvUR \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$pc[p] = \text{“UR”} \Rightarrow \wedge\ t.ret[p] = ACK$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ SameRoot(t,\ t.arg[p][1],\ u\_U[p])$$
$$\wedge\ SameRoot(t,\ t.arg[p][2],\ v\_U[p])$$
$$\wedge\ SameRoot(t,\ u\_U[p],\ v\_U[p])$$

$$Linearizable \triangleq M \neq \{\}$$

$$Inv \triangleq \wedge\ TypeOK$$
$$\wedge\ InvDecide$$
$$\wedge\ InvF1$$

$\land \mathit{InvF2}$
$\land \mathit{InvF3}$
$\land \mathit{InvF4}$
$\land \mathit{InvF5}$
$\land \mathit{InvF6}$
$\land \mathit{InvF7}$
$\land \mathit{InvFR}$
$\land \mathit{InvU1}$
$\land \mathit{InvU2}$
$\land \mathit{InvU3}$
$\land \mathit{InvU4}$
$\land \mathit{InvU5}$
$\land \mathit{InvU6}$
$\land \mathit{InvU7}$
$\land \mathit{InvU8}$
$\land \mathit{InvUR}$
$\land \mathit{SigmaRespectsShared}$
$\land \mathit{Linearizable}$

* Modification History
* Last modified *Fri* May 02 00:44:09 *EDT* 2025 by *karunram*
* Created *Thu Apr* 03 22:44:42 *EDT* 2025 by *karunram*