MODULE *Inv*

EXTENDS *Implementation*, *TypeSafety*

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

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

$$SharedRespectsSigma \triangleq \quad \forall\, t \in M : \forall\, i \in NodeSet : \quad \wedge\, t.sigma[i] = i \quad \Rightarrow F[i].bit = 1$$

$$\begin{array}{ll} InvF2All(p,\, t) \triangleq & \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \end{array}$$

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

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

$$\begin{array}{ll} InvF5All(p,\, t) \triangleq & \wedge\, F[u\_F[p]].bit = 0 \\ & \wedge\, a\_F[p].bit = 0 \\ & \wedge\, SameRoot(t,\, c[p],\, a\_F[p].parent) \\ & \wedge\, SameRoot(t,\, c[p],\, u\_F[p]) \\ & \wedge\, b\_F[p].bit = 0 \Rightarrow SameRoot(t,\, a\_F[p].parent,\, b\_F[p].parent) \\ & \wedge\, b\_F[p].bit = 1 \Rightarrow t.sigma[a\_F[p].parent] = a\_F[p].parent \end{array}$$

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

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

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

$$\begin{array}{ll} InvU5All(p,\, t) \triangleq & \wedge\, SameRoot(t,\, t.arg[p][1],\, u\_U[p]) \\ & \wedge\, SameRoot(t,\, t.arg[p][2],\, v\_U[p]) \\ & \wedge\, u\_U[p] \neq v\_U[p] \end{array}$$

$$
\begin{array}{l}
\qquad\qquad \land\ a\_U[p].bit = 0 \Rightarrow SameRoot(t,\ a\_U[p].parent,\ u\_U[p]) \\
\qquad\qquad \land\ a\_U[p].bit = 1 \Rightarrow t.sigma[u\_U[p]] = u\_U[p] \\
\\
InvU6All(p,\ t) \triangleq \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
\qquad\qquad \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
\qquad\qquad \land\ u\_U[p] \neq v\_U[p] \\
\qquad\qquad \land\ a\_U[p].bit = 0 \Rightarrow SameRoot(t,\ a\_U[p].parent,\ u\_U[p]) \\
\qquad\qquad \land\ a\_U[p].bit = 1 \Rightarrow t.sigma[u\_U[p]] = u\_U[p] \\
\qquad\qquad \land\ b\_U[p].bit = 0 \Rightarrow SameRoot(t,\ b\_U[p].parent,\ v\_U[p]) \\
\qquad\qquad \land\ b\_U[p].bit = 1 \Rightarrow t.sigma[v\_U[p]] = v\_U[p] \\
\\
InvU7All(p,\ t) \triangleq \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
\qquad\qquad \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
\qquad\qquad \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
\\
InvU8All(p,\ t) \triangleq \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
\qquad\qquad \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
\qquad\qquad \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
\\
InvDecide \triangleq \forall\, p \in PROCESSES : \forall\, t \in M : \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“0”} \quad \Rightarrow\ \land\ t.ret[p] = BOT \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = BOT \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] = BOT \\
InvF1 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M : \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“F1”} \quad \Rightarrow\ \land\ t.ret[p] = BOT \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = \text{“F”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] \in NodeSet \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ SameRoot(t,\ c[p],\ t.arg[p]) \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“F1U1”} \ \Rightarrow\ \land\ t.ret[p] = BOT \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = \text{“U”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] \in NodeSet \times NodeSet \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“F1U2”} \ \Rightarrow\ \land\ t.ret[p] = BOT \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = \text{“U”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] \in NodeSet \times NodeSet \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ InvU2All(p,\ t) \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ SameRoot(t,\ c[p],\ v\_U[p]) \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“F1U7”} \ \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = \text{“U”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] \in NodeSet \times NodeSet \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ InvU7All(p,\ t) \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ SameRoot(t,\ c[p],\ u\_U[p]) \\
\qquad\qquad\qquad\qquad \land\ pc[p] = \text{“F1U8”} \ \Rightarrow\ \land\ t.ret[p] \in \{BOT,\ ACK\} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.op[p] = \text{“U”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ t.arg[p] \in NodeSet \times NodeSet \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \land\ InvU8All(p,\ t)
\end{array}
$$

$$\wedge\ SameRoot(t,\ c[p],\ v\_U[p])$$

$$InvF2 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$$
$$\wedge\ pc[p] = \text{“F2”} \Rightarrow \wedge\ t.ret[p] = BOT$$
$$\wedge\ t.op[p] = \text{“F”}$$
$$\wedge\ t.arg[p] \in NodeSet$$
$$\wedge\ SameRoot(t,\ c[p],\ t.arg[p])$$
$$\wedge\ InvF2All(p,\ t)$$
$$\wedge\ pc[p] = \text{“F2U1”} \Rightarrow \wedge\ t.ret[p] = BOT$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ SameRoot(t,\ c[p],\ u\_U[p])$$
$$\wedge\ InvF2All(p,\ t)$$
$$\wedge\ pc[p] = \text{“F2U2”} \Rightarrow \wedge\ t.ret[p] = BOT$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU2All(p,\ t)$$
$$\wedge\ SameRoot(t,\ c[p],\ v\_U[p])$$
$$\wedge\ InvF2All(p,\ t)$$
$$\wedge\ pc[p] = \text{“F2U7”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU7All(p,\ t)$$
$$\wedge\ SameRoot(t,\ c[p],\ u\_U[p])$$
$$\wedge\ InvF2All(p,\ t)$$
$$\wedge\ pc[p] = \text{“F2U8”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$$
$$\wedge\ t.op[p] = \text{“U”}$$
$$\wedge\ t.arg[p] \in NodeSet \times NodeSet$$
$$\wedge\ InvU8All(p,\ t)$$
$$\wedge\ SameRoot(t,\ c[p],\ v\_U[p])$$
$$\wedge\ InvF2All(p,\ t)$$

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

$\wedge\ t.arg[p] \in NodeSet \times NodeSet$
$\wedge\ InvU2All(p,\ t)$
$\wedge\ SameRoot(t,\ c[p],\ v\_U[p])$
$\wedge\ InvF3All(p,\ t)$
$\wedge\ pc[p] = \text{“F3U7”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p] = \text{“U”}$
$\wedge\ t.arg[p] \in NodeSet \times NodeSet$
$\wedge\ InvU7All(p,\ t)$
$\wedge\ SameRoot(t,\ c[p],\ u\_U[p])$
$\wedge\ InvF3All(p,\ t)$
$\wedge\ pc[p] = \text{“F3U8”} \Rightarrow \wedge\ t.ret[p] \in \{BOT,\ ACK\}$
$\wedge\ t.op[p] = \text{“U”}$
$\wedge\ t.arg[p] \in NodeSet \times NodeSet$
$\wedge\ InvU8All(p,\ t)$
$\wedge\ SameRoot(t,\ c[p],\ v\_U[p])$
$\wedge\ InvF3All(p,\ t)$

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

$\land\ InvF4All(p,\ t)$

$InvF5 \triangleq \quad \forall\, p \in PROCESSES : \forall\, t \in M :$

$\land\ pc[p] = \text{“F5”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“F”}$
$\land\ t.arg[p] \in NodeSet$
$\land\ SameRoot(t,\ c[p],\ t.arg[p])$
$\land\ InvF5All(p,\ t)$

$\land\ pc[p] = \text{“F5U1”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ SameRoot(t,\ c[p],\ u\_U[p])$
$\land\ InvF5All(p,\ t)$

$\land\ pc[p] = \text{“F5U2”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ InvU2All(p,\ t)$
$\land\ SameRoot(t,\ c[p],\ v\_U[p])$
$\land\ InvF5All(p,\ t)$

$\land\ pc[p] = \text{“F5U7”} \quad \Rightarrow \quad \land\ t.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ InvU7All(p,\ t)$
$\land\ SameRoot(t,\ c[p],\ u\_U[p])$
$\land\ InvF5All(p,\ t)$

$\land\ pc[p] = \text{“F5U8”} \quad \Rightarrow \quad \land\ t.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ InvU8All(p,\ t)$
$\land\ SameRoot(t,\ c[p],\ v\_U[p])$
$\land\ InvF5All(p,\ t)$

$InvF6 \triangleq \quad \forall\, p \in PROCESSES : \forall\, t \in M :$

$\land\ pc[p] = \text{“F6”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“F”}$
$\land\ t.arg[p] \in NodeSet$
$\land\ SameRoot(t,\ c[p],\ t.arg[p])$
$\land\ InvF6All(p,\ t)$

$\land\ pc[p] = \text{“F6U1”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ SameRoot(t,\ c[p],\ u\_U[p])$
$\land\ InvF6All(p,\ t)$

$\land\ pc[p] = \text{“F6U2”} \quad \Rightarrow \quad \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$

$$
\begin{array}{lll}
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU2All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U7”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU7All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ u\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t) \\
 & \wedge\ pc[p] = \text{“F6U8”} \ \Rightarrow & \wedge\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \wedge\ t.op[p] = \text{“U”} \\
 & & \wedge\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \wedge\ InvU8All(p,\ t) \\
 & & \wedge\ SameRoot(t,\ c[p],\ v\_U[p]) \\
 & & \wedge\ InvF6All(p,\ t)
\end{array}
$$

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

$\land\ SameRoot(t,\ c[p],\ v\_U[p])$
$\land\ InvF7All(p,\ t)$

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

$InvU1 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$
$pc[p] = \text{“U1”} \Rightarrow \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$

$InvU2 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$
$pc[p] = \text{“U2”} \Rightarrow \land\ t.ret[p] = BOT$
$\land\ t.op[p] = \text{“U”}$
$\land\ t.arg[p] \in NodeSet \times NodeSet$
$\land\ InvU2All(p,\ t)$

$InvU3 \triangleq \forall\, p \in PROCESSES : \forall\, t \in M :$
$pc[p] = \text{“U3”} \Rightarrow \land\ t.ret[p] \in \{BOT,\ ACK\}$
$\land\ t.op[p] = \text{“U”}$

$$
\begin{array}{lll}
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
 & & \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ \\
InvU4 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“U4”} \quad \Rightarrow & \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
 & & \land\ t.ret[p] = ACK \Rightarrow SameRoot(t,\ u\_U[p],\ \\
 & & \land\ u\_U[p] \neq v\_U[p] \\
InvU5 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“U5”} \quad \Rightarrow & \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU5All(p,\ t) \\
InvU6 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“U6”} \quad \Rightarrow & \\
 & & \land\ t.ret[p] \in \{BOT,\ ACK\} \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ InvU6All(p,\ t) \\
InvU7 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“U7”} \quad \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) \\
InvU8 \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“U8”} \quad \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) \\
InvUR \triangleq & \forall\, p \in PROCESSES : \forall\, t \in M : & \\
 & pc[p] = \text{“UR”} \quad \Rightarrow & \land\ t.ret[p] = ACK \\
 & & \land\ t.op[p] = \text{“U”} \\
 & & \land\ t.arg[p] \in NodeSet \times NodeSet \\
 & & \land\ SameRoot(t,\ t.arg[p][1],\ u\_U[p]) \\
 & & \land\ SameRoot(t,\ t.arg[p][2],\ v\_U[p]) \\
 & & \land\ SameRoot(t,\ u\_U[p],\ v\_U[p]) \\
Linearizable \triangleq & M \neq \{\} &
\end{array}
$$

$$
\begin{aligned}
Inv \triangleq\ & \land\ TypeOK \\
& \land\ InvDecide \\
& \land\ InvF1 \\
& \land\ InvF2 \\
& \land\ InvF3 \\
& \land\ InvF4 \\
& \land\ InvF5 \\
& \land\ InvF6 \\
& \land\ InvF7 \\
& \land\ InvFR \\
& \land\ InvU1 \\
& \land\ InvU2 \\
& \land\ InvU3 \\
& \land\ InvU4 \\
& \land\ InvU5 \\
& \land\ InvU6 \\
& \land\ InvU7 \\
& \land\ InvU8 \\
& \land\ InvUR \\
& \land\ SigmaRespectsShared \\
& \land\ SharedRespectsSigma \\
& \land\ Linearizable
\end{aligned}
$$

* 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*