The Bakery Algorithm Invariant

Here is the inductive invariant I found that is implied by *Init* and implies *MutualExclusion*.

$$
\begin{aligned}
\mathit{TypeOK} \triangleq\ & \land\ num \in [\mathit{Procs} \to \mathit{Nat}] \\
& \land\ \mathit{flag} \in [\mathit{Procs} \to \text{BOOLEAN }] \\
& \land\ \mathit{unchecked} \in [\mathit{Procs} \to \text{SUBSET } \mathit{Procs}] \\
& \land\ \mathit{max} \in [\mathit{Procs} \to \mathit{Nat}] \\
& \land\ \mathit{nxt}\ \in [\mathit{Procs} \to \mathit{Procs}] \\
& \land\ \mathit{pc} \in [\mathit{Procs} \to \{\text{“ncs”},\ \text{“e1”},\ \text{“e2”},\ \text{“e3”}, \\
& \qquad\qquad \text{“e4”},\ \text{“w1”},\ \text{“w2”},\ \text{“cs”},\ \text{“exit”}\}]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Before}(i, j) \triangleq\ & \land\ num[i] > 0 \\
& \land\ \lor\ \mathit{pc}[j] \in \{\text{“ncs”},\ \text{“e1”}\} \\
& \quad \lor\ \land\ \mathit{pc}[j] = \text{“e2”} \\
& \qquad \land\ \lor\ i \in \mathit{unchecked}[j] \\
& \qquad\quad \lor\ \mathit{max}[j] \geq num[i] \\
& \quad \lor\ \land\ \mathit{pc}[j] = \text{“e3”} \\
& \qquad \land\ \mathit{max}[j] \geq num[i] \\
& \quad \lor\ \land\ \mathit{pc}[j] \in \{\text{“e4”},\ \text{“w1”},\ \text{“w2”}\} \\
& \qquad \land\ \langle num[i],\ i\rangle \prec \langle num[j],\ j\rangle \\
& \qquad \land\ (\mathit{pc}[j] \in \{\text{“w1”},\ \text{“w2”}\}) \Rightarrow (i \in \mathit{unchecked}[j])
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Inv} \triangleq\ & \land\ \mathit{TypeOK} \\
& \land\ \forall\, i \in \mathit{Procs} : \\
& \qquad \land\ (num[i] = 0) \equiv (\mathit{pc}[i] \in \{\text{“ncs”},\ \text{“e1”},\ \text{“e2”},\ \text{“e3”}\}) \\
& \qquad \land\ \mathit{flag}[i] \equiv (\mathit{pc}[i] \in \{\text{“e2”},\ \text{“e3”},\ \text{“e4”}\}) \\
& \qquad \land\ (\mathit{pc}[i] = \text{“w2”}) \Rightarrow (\mathit{nxt}[i] \neq i) \\
& \qquad \land\ \mathit{pc}[i] \in \{\text{“e2”},\ \text{“w1”},\ \text{“w2”}\} \Rightarrow i \notin \mathit{unchecked}[i] \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{“w1”},\ \text{“w2”}\}) \Rightarrow \\
& \qquad\quad \forall\, j \in (\mathit{Procs} \setminus \mathit{unchecked}[i]) \setminus \{i\} : \mathit{Before}(i, j) \\
& \qquad \land\ \land\ (\mathit{pc}[i] = \text{“w2”}) \\
& \qquad\quad \land\ \lor\ (\mathit{pc}[\mathit{nxt}[i]] = \text{“e2”}) \land (i \notin \mathit{unchecked}[\mathit{nxt}[i]]) \\
& \qquad\qquad \lor\ \mathit{pc}[\mathit{nxt}[i]] = \text{“e3”} \\
& \qquad\quad \Rightarrow \mathit{max}[\mathit{nxt}[i]] \geq num[i] \\
& \qquad \land\ (\mathit{pc}[i] \in \{\text{“cs”},\ \text{“exit”}\}) \Rightarrow \forall\, j \in \mathit{Procs} \setminus \{i\} : \mathit{Before}(i, j)
\end{aligned}
$$

CLOSE