The Bakery Algorithm Invariant

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

```
TupeOK \stackrel{\Delta}{=} \land num \in [Procs \rightarrow Nat]
                      \land flaa \in [Procs \rightarrow BOOLEAN]
                      \land unchecked \in [Procs \rightarrow SUBSET\ Procs]
                      \land max \in [Procs \rightarrow Nat]
                      \land nxt \in [Procs \rightarrow Procs]
                      \land pc \in [Procs \rightarrow \{\text{"ncs"}, \text{"e1"}, \text{"e2"}, \text{"e3"},
                                                      "e4", "w1", "w2", "cs", "exit"}]
Before(i, j) \stackrel{\Delta}{=} \wedge num[i] > 0
                            \land \lor pc[j] \in \{\text{"ncs", "e1"}\}
                                \lor \land pc[j] = \text{``e2''}
                                    \land \lor i \in unchecked[j]
                                         \vee max[j] \geq num[i]
                                \lor \land pc[j] = \text{``e3''}
                                    \land max[j] \ge num[i]
                                \lor \land pc[j] \in \{\text{"e4"}, \text{"w1"}, \text{"w2"}\}\
                                    \land \langle num[i], i \rangle \prec \langle num[j], j \rangle
                                    \land (pc[j] \in \{\text{"w1"}, \text{"w2"}\}) \Rightarrow (i \in unchecked[j])
Inv \triangleq \land TypeOK
              \land \forall i \in Procs:
                     \land (num[i] = 0) \equiv (pc[i] \in \{\text{"ncs"}, \text{"e1"}, \text{"e2"}, \text{"e3"}\})
                     \land flag[i] \equiv (pc[i] \in \{\text{"e2", "e3", "e4"}\})
                     \land (pc[i] = \text{``w2''}) \Rightarrow (nxt[i] \neq i)
                     \land pc[i] \in \{\text{"e2"}, \text{"w1"}, \text{"w2"}\} \Rightarrow i \notin unchecked[i]
                     \land (pc[i] \in \{\text{"w1"}, \text{"w2"}\}) \Rightarrow
                             \forall i \in (Procs \setminus unchecked[i]) \setminus \{i\} : Before(i, j)
                     \wedge \wedge (pc[i] = \text{``w2''})
                         \land \lor (pc[nxt[i]] = \text{``e2''}) \land (i \notin unchecked[nxt[i]])
                               \vee pc[nxt[i]] = \text{"e3"}
                          \Rightarrow max[nxt[i]] \geq num[i]
                     \land (pc[i] \in \{\text{"cs"}, \text{"exit"}\}) \Rightarrow \forall j \in Procs \setminus \{i\} : Before(i, j)
```