

# The Bakery Algorithm Invariant

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

$$\begin{aligned} TypeOK \triangleq & \wedge num \in [Procs \rightarrow Nat] \\ & \wedge flag \in [Procs \rightarrow BOOLEAN] \\ & \wedge unchecked \in [Procs \rightarrow SUBSET Procs] \\ & \wedge max \in [Procs \rightarrow Nat] \\ & \wedge nxt \in [Procs \rightarrow Procs] \\ & \wedge pc \in [Procs \rightarrow \{ "ncs", "e1", "e2", "e3", \\ & \quad "e4", "w1", "w2", "cs", "exit" \}] \end{aligned}$$

$$\begin{aligned} Before(i, j) \triangleq & \wedge num[i] > 0 \\ & \wedge \vee pc[j] \in \{ "ncs", "e1" \} \\ & \quad \vee \wedge pc[j] = "e2" \\ & \quad \quad \wedge \vee i \in unchecked[j] \\ & \quad \quad \quad \vee max[j] \geq num[i] \\ & \vee \wedge pc[j] = "e3" \\ & \quad \wedge max[j] \geq num[i] \\ & \vee \wedge pc[j] \in \{ "e4", "w1", "w2" \} \\ & \quad \wedge \langle num[i], i \rangle < \langle num[j], j \rangle \\ & \quad \wedge (pc[j] \in \{ "w1", "w2" \}) \Rightarrow (i \in unchecked[j]) \end{aligned}$$

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