The Bakery Algorithm is FCFS

Theorem $Spec \Rightarrow FCFS$

1. SUFFICES ASSUME: $\Box Inv \wedge \Box[Next]_{vars}$, $p \in Procs$, $q \in Procs$
   PROVE: $Waiting(p) \wedge InNCS(q) \wedge \Box\neg InCS(p) \Rightarrow \Box\neg InCS(q)$

   PROOF: By definition of $Spec$ and $FCFS$, the invariance of Inv (the theorem $Spec \Rightarrow \Box Inv$), and temporal logic. We are using the proof rule $(F \Rightarrow G) \vdash (\Box F \Rightarrow \Box G)$, together with the observation that $\Box Inv \wedge \Box[Next]_{vars}$ is equivalent to $\Box(\Box Inv \wedge \Box[Next]_{vars})$.

DEFINE: $WInv \triangleq Waiting(p) \wedge Before(p, q)$

We prove that $\Box Inv \wedge \Box\neg InCS(p)$ implies

$$Waiting(p) \wedge InNCS \wedge \Box[Next]_{vars} \Rightarrow \Box\neg InCS(q)$$

by proving that $\neg InCS(q)$ is an invariant of the specification

$$(Waiting(p) \wedge InNCS) \wedge \Box[Next]_{vars}$$

using the inductive invariant $WInv$. This is an ordinary invariance proof, except that because we are assuming $\Box Inv \wedge \Box\neg InCS(p)$, we can assume $Inv \wedge Inv' \wedge \neg InCS(p) \wedge \neg InCS(p)'$ in our action reasoning.

2. $Inv \wedge Waiting(p) \wedge InNCS(q) \Rightarrow WInv$

   PROOF: By definition of $WInv$, since $Inv \wedge Waiting(p) \wedge InNCS(q)$ implies $(num[p] > 0) \wedge (num[q] = 0)$, which implies $Before(p, q)$.

3. $Inv \wedge \neg InCS(p)' \wedge WInv \wedge [Next]_{vars} \Rightarrow WInv'$

   PROOF: $\neg InCS(p)'$ implies that p can't enter its critical section, so $[Next]_{vars} \wedge Waiting(p)$ implies $Waiting(p)'$. Since $Inv \wedge Waiting(p)$ imply $num[p] \neq 0$, a $Next$ step can make $Before(p, q)$ false only by making $\langle num'[q], q\rangle \prec \langle num[p], p\rangle$ true, which is impossible because an $enter(q)$ step sets $num'[q] > num[p]$.

4. $Inv \wedge WInv \Rightarrow \neg InCS(q)$

   PROOF: $Inv \wedge InCS(q)$ implies $(num[q] \neq 0) \wedge Before(q, p)$, which implies $\neg Before(p, q)$.

5. Q.E.D.

   PROOF: Step 3 implies

   $$\Box Inv \wedge \Box\neg InCS(p) \Rightarrow (WInv \wedge \Box[Next]_{vars} \Rightarrow \Box WInv)$$

   which by steps 2 and 4 and the step 1 assumptions proves

   $$Waiting(p) \wedge InNCS(q) \wedge \Box\neg InCS(p); \Rightarrow \Box\neg InCS(q)$$

CLOSE