Deadlock Free and FCFS Implies Starvation Free

We first formally define *FCFS*.

$$InNCS(p) \quad \triangleq \quad pc[p] = \text{“}\mathsf{ncs}\text{”}$$

$$Waiting(p) \quad \triangleq \quad pc[p] = \text{“}\mathsf{waiting}\text{”}$$

$$\begin{array}{l} FCFS \;\triangleq \\ \quad \forall\, p,\, q \in Procs : \\ \qquad \Box(\, Waiting(p) \;\wedge\; InNCS(q) \;\wedge\; \Box\neg InCS(p) \;\Rightarrow\; \Box\neg InCS(q)) \end{array}$$

We now state and prove the theorem.

Theorem $DeadlockFree \wedge FCFS \;\Rightarrow\; StarvationFree$

1. SUFFICES ASSUME: $p \in Procs$, $FCFS$, $DeadlockFree$
   PROVE: $Trying(p) \wedge \Box\neg InCS(p) \leadsto$ FALSE

   PROOF: By definition of *StarvationFree* and simple temporal logic.

2. $Trying(p) \wedge \Box\neg InCS(p) \;\leadsto\; Waiting(p) \wedge \Box\neg InCS(p)$

   PROOF: By fairness for process p.

3. $Waiting(p) \wedge \Box\neg InCS(p) \;\leadsto\; \Box(\, Waiting(p) \wedge \neg InCS(p))$

   PROOF: The algorithm implies that $Waiting(p)$ can become false only by making $InCS(p)$ true.

4. $\forall q \in Procs \setminus \{p\} \,:\, \Box(\, Waiting(p) \wedge \neg InCS(p)) \leadsto \Box\neg InCS(q)$

   4.1. SUFFICES ASSUME: $q \in Procs$, $q \neq p$, $\Box(\, Waiting(p) \wedge \neg InCS(p))$
   PROVE: TRUE $\leadsto \Box\neg InCS(q)$

   PROOF: By simple temporal reasoning.

   4.2. TRUE $\leadsto (\Box\Diamond InCS(q)) \vee (\Box\neg InCS(q))$

   PROOF: By the temporal logic tautology $\Box\Diamond F \vee \Diamond\Box(\neg F)$.

   4.3. $\Box\Diamond InCS(q) \leadsto InNCS(q)$

   PROOF: The algorithm's code and fairness assumption imply $InCS(q) \leadsto InNCS(q)$.

   4.4. $InNCS(q) \Rightarrow \Box\neg InCS(q)$

   PROOF: By the step 4.1 assumption, which implies $Waiting(p) \wedge \Box\neg InCS(p)$ and $FCFS$.

   4.5. Q.E.D.

   PROOF: By 4.2–4.4 and the Leads-To Induction Rule.

5. $Waiting(p) \leadsto \exists q \in Procs \,:\, InCS(q)$

   PROOF: By *DeadlockFree* (assumed in 1).

6. Q.E.D.

PROOF: Steps 2–5 and temporal logic yield:

$$Trying(p) \land \Box\neg InCS(p) \leadsto \begin{array}{l} \land\ \Box\neg InCS(p) \\ \land\ \forall q \in Procs \setminus \{p\} : \Box\neg InCS(q) \\ \land\ \exists q \in Procs : InCS(q) \end{array}$$

and the conjunction to the right of the $\leadsto$ equals FALSE.

CLOSE