A Formal Proof of Deadlock Freedom

Lemma $Spec \Rightarrow \Box LInv$

Theorem $Spec \Rightarrow DeadlockFree$

DEFINE
$$\begin{aligned} T0 &\triangleq Trying(0) \\ T1 &\triangleq Trying(1) \\ Success &\triangleq InCS(0) \lor InCS(1) \\ Fairness &\triangleq \forall i \in \{0, 1\} : \mathrm{WF}_{vars}((pc[i] \neq \text{“ncs”}) \land P(i)) \end{aligned}$$

1 $\langle 1 \rangle 1$. SUFFICES ASSUME: $\Box LInv \land \Box[Next]_{vars} \land Fairness \land \Box\neg Success$
PROVE: $T0 \lor T1 \leadsto \text{FALSE}$

1.1 $\langle 2 \rangle 1$. SUFFICES: $\Box LInv \land \Box[Next]_{vars} \land Fairness \Rightarrow DeadlockFree$

PROOF: By the lemma and the definition of *Spec*.

1.2 $\langle 2 \rangle 2$. $DeadlockFree \equiv ((\Box\neg Success) \land (T0 \lor T1) \leadsto \text{FALSE})$

PROOF: By definition of *DeadlockFree* and the tautology $(F \leadsto G) \equiv ((\Box\neg G) \land F \leadsto \text{FALSE}$.

1.3 $\langle 2 \rangle 3$. Q.E.D.

PROOF: By $\langle 2 \rangle 1$, $\langle 2 \rangle 2$, and the proof rule
$(\Box F \land \Box G \vdash H \leadsto K) \vdash (\Box F \Rightarrow (\Box G \land H \leadsto K))$
since $Fairness \equiv \Box Fairness$.

2 $\langle 1 \rangle 2$. CASE: $T0 \leadsto \text{FALSE}$.

2.1 $\langle 2 \rangle 1$. $T0 \leadsto \Box(pc[0] = \text{“e2”})$

PROOF: *LInv* implies that process 0 is never at $e3$ or $e4$, and $\Box\neg Success$ (from the step $\langle 1 \rangle 1$ assumption) implies $\Box\neg InCS(0)$. Therefore, *Fairness* implies $T0 \leadsto (pc[0] = \text{“e2”})$, and $\Box LInv \land \Box[Next]_{vars}$ implies $(pc[0] = \text{“e2”}) \Rightarrow \Box(pc[0] = \text{“e2”})$.

2.2 $\langle 2 \rangle 2$. $\Box(pc[0] = \text{“e2”}) \leadsto \Box((pc[0] = \text{“e2”}) \land \neg x[1])$

2.2.1 $\langle 3 \rangle 1$. SUFFICES ASSUME: $\Box(pc[0] = \text{“e2”})$
PROVE: $\text{TRUE} \leadsto \Box\neg x[1]$

PROOF: By proof rule $(\Box F \vdash G \leadsto H) \vdash (\Box F \land G \leadsto \Box F \land H)$.

2.2.2 $\langle 3 \rangle 2$. $\text{TRUE} \leadsto (\Box(pc[1] = \text{“ncs”}) \lor \Box T1)$

PROOF: By $\Box\neg Success$ (from the step $\langle 1 \rangle 1$ assumption), process 1 never reaches *cs*. The code and fairness therefore imply that process 1 must eventually either reach and remain forever at *ncs*, or $T1$ must become true and remain true forever.

2.2.3 $\langle 3 \rangle 3$. $(\Box(pc[1] = \text{“ncs”}) \Rightarrow \Box\neg x[1]$

PROOF: *LInv* implies that $x[1]$ equals FALSE when process 1 is at *ncs*.

2.2.4 $\langle 3\rangle 4.$ $\Box T1 \leadsto \Box\neg x[1]$

PROOF: $\Box \mathit{LInv} \land \Box(pc[0] = \text{“e2”})$ imply $\Box x[0]$. Thus, $\Box T1$ (the case assumption), $\Box\neg \mathit{InCS}(1)$ (by the step $\langle 1\rangle 1$ assumption $\Box\neg \mathit{Success}$), the code, and fairness imply that process 1 must eventually reach and remain forever at $e4$ with $x[1]$ equal to FALSE.

2.2.5 $\langle 3\rangle 5.$ Q.E.D.

PROOF: By $\langle 3\rangle 2$–$\langle 3\rangle 4$ and Leads-To Induction.

2.3 $\langle 2\rangle 3.$ Q.E.D.

2.3.1 $\langle 3\rangle 1.$ $\Box((pc[0] = \text{“e2”}) \land \neg x[1]) \leadsto \mathit{InCS}(0)$

2.3.2 $\langle 3\rangle 2.$ Q.E.D.

PROOF: $\langle 2\rangle 1$, $\langle 2\rangle 2$, and $\langle 3\rangle 1$ imply $T0 \leadsto \mathit{InCS}(0)$, and $\mathit{InCS}(0) \land \Box\neg \mathit{Success}$ implies FALSE.

3 $\langle 1\rangle 3.$ CASE: $T1 \leadsto$ FALSE.

3.1 $\langle 2\rangle 1.$ $\Box T1$ is true time t_1.

PROOF: By the step $\langle 1\rangle 1$ assumption, $\Box\neg \mathit{InCS}(1)$ (which is implied by $\Box\neg \mathit{Success}$) is true at time t_1. From the code and the step $\langle 1\rangle 3$ case assumption, this implies that $\Box T1$ is true at time t_1.

3.2 $\langle 2\rangle 2.$ Either $\Box\neg T0$ is true a time t_1, or $T0$ is true at some time $t_2 \geq t_1$.

PROOF: Obviously, $\Box\neg T0$ is false at time t_1 iff $T0$ is true at some time $t_2 \geq t_1$.

3.3 $\langle 2\rangle 3.$ CASE: $\Box\neg T0$ is true at time t_1

3.3.1 $\langle 3\rangle 1.$ There is some $t_3 \geq t_1$ such that $\Box\neg x[0]$ is true at time t_3.

PROOF: By the code and fairness, $\neg T0$ true at time t_1 implies that process 0 is at ncs at some time $t_3 \geq t_1$. The code and $\neg T0$ true at all times $t \geq t_1$ and the code imply that process 0 is at ncs with $\neg x[0]$ true for all $t \geq t_3$.

3.3.2 $\langle 3\rangle 2.$ $\Box(T_1 \land \neg x[0])$ is true at time t_3

PROOF: By $\langle 3\rangle 1$ and $\langle 2\rangle 1$.

3.3.3 $\langle 3\rangle 3.$ Q.E.D.

PROOF: Step $\langle 3\rangle 2$, the code, and fairness imply that process 1 reaches $e2$ at some time $t_4 \geq t_3$. Step $\langle 3\rangle 2$ implies $\Box\neg x[0]$ is true at time t_4, which by fairness implies that process 1 reaches its critical section at some time $t_5 > t_4$. Since $t_5 \geq t_1$, this contradicts the assumption from step $\langle 1\rangle 1$ that $\Box\neg \mathit{Success}$ is true at time t_1.

3.4 $\langle 2\rangle 4.$ CASE: $T0$ is true at time $t_2 \geq t_1$

PROOF: By $\langle 1\rangle 2$.

3.5 $\langle 2\rangle 5.$ Q.E.D.

PROOF: By $\langle 2\rangle 2$, $\langle 2\rangle 3$, and $\langle 2\rangle 4$.

4 $\langle 1\rangle 4$. Q.E.D.

PROOF: By the step $\langle 1\rangle 1$ assumption, $\langle 1\rangle 2$ (letting t_2 equal t_1), and $\langle 1\rangle 3$.

CLOSE