A Better Informal Proof of Deadlock Freedom

Theorem The 2-process 1-bit algorithm satisfies *DeadlockFree*

DEFINE $T0 \triangleq \mathit{Trying}(0)$
$T1 \triangleq \mathit{Trying}(1)$
$\mathit{Success} \triangleq \mathit{InCS}(0) \lor \mathit{InCS}(1)$

1 $\langle 1 \rangle 1$. It suffices to assume $(T0 \lor T1) \land \Box\neg \mathit{Success}$ is true at some time t_1 and obtain a contradiction.

PROOF: By definition of deadlock freedom.

2 $\langle 1 \rangle 2$. CASE: There is a time $t_2 \geq t_1$ at which $T0$ is true.

2.1 $\langle 2 \rangle 1$. $\Box(pc[0] = \text{“e2”})$ is true at some time $t_3 \geq t_2$.

PROOF: Process 0 is never at $e3$ or $e4$, and $\Box\neg \mathit{Success}$ (from the step $\langle 1 \rangle 1$ assumption) implies that $\Box\neg \mathit{InCS}(0)$ is true at time t_2. Therefore, $T0$ true at time t_2, the code, and fairness imply that process 0 eventually reaches $e2$ at some time $t_3 \geq t_2$ and stays there forever.

2.2 $\langle 2 \rangle 2$. $\Box\neg x[1]$ is true at some time $t_4 \geq t_3$.

2.2.1 $\langle 3 \rangle 1$. $(\Box(pc[1] = \text{“ncs”}) \lor \Box T1)$ is true at some time $t_5 \geq t_3$.

PROOF: By $\Box\neg \mathit{Success}$ (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.

2.2.2 $\langle 3 \rangle 2$. CASE: $\Box(pc[1] = \text{“ncs”})$ is true at time t_5.

PROOF: Since $x[1]$ equals FALSE when process 1 is at *ncs*, the case assumption implies that $\Box\neg x[1]$ is true at time t_5. This proves $\langle 2 \rangle 2$ for t_4 equal to t_5.

2.2.3 $\langle 3 \rangle 3$. CASE: $\Box T1$ is true at time t_5.

PROOF: Since $x[0]$ is true when process 0 is at $e2$, $\langle 2 \rangle 1$ and $t_5 \geq t_3$ implies $\Box x[0]$ is true at time t_5. 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 at some time $t_4 \geq t_5$ reach and remain forever at $e4$ with $x[1]$ equal to FALSE, proving $\langle 2 \rangle 2$.

2.2.4 $\langle 3 \rangle 4$. Q.E.D.

PROOF: By $\langle 3 \rangle 1$–$\langle 3 \rangle 3$.

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

PROOF: $\langle 2 \rangle 1$ and $\langle 2 \rangle 2$ imply that $(pc[0] = \text{“e2”})$ and $\Box\neg x[1]$ are true at time t_4. The code and fairness then imply that process 0 reaches *cs* at some time $t_6 \geq t_4$. Since $t_4 \geq t_1$ by $\langle 2 \rangle 2$, $\langle 2 \rangle 1$, and the $\langle 1 \rangle 2$ case assumption, this contradicts the assumption $\Box\neg Success$ of step $\langle 1\rangle 1$.

3 $\langle 1\rangle 3$. CASE: $T1$ is true at time t_1.

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

PROOF: By the step $\langle 1\rangle 1$ assumption, $\Box\neg InCS(1)$ (which is implied by $\Box\neg Success$) 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 $\langle 3\rangle 2$. $\Box(T_1 \wedge \neg x[0])$ 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 $\Box\neg Success$ 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