MODULE *petersons_algo_modified*

EXTENDS *Integers*

VARIABLES $pc0$, $pc1$, $turn$, $intr0$, $intr1$

$TypeOK \triangleq$
$\land\ pc0 \in 0\,..\,7$
$\land\ pc1 \in 0\,..\,7$
$\land\ turn \in \{0, 1\}$
$\land\ intr0 \in \{0, 1\}$
$\land\ intr1 \in \{0, 1\}$

a) adding weak fairness constraints on steps where applicable and b) check
i) whether all runs satisfy starvation freeness *i.e* a process requesting to enter *CS* at any instant will be allowed to enter *CS* at a future instant ii) whether all runs mandate strict sequencing between process 1 and process 2 in critical section
show a trace where strict sequencing need not hold

Ref pg 36 of handbook of model checking

asynchronous system

for $i = 0, 1$

the algorithm is

0 : *while*(*True*){
1 : *//non critical section*
2 : $intr[i] = True$
3 : $turn = 1 - i$
4 : *while*($turn \triangleq 1$ *and* $intr[1 - i] \triangleq 1$)*//wait*
5 : *//critical section*
6 : $intr[i] = 0$
7 : }

weak fairness :

$Init0 \triangleq$
$\land\ turn = 0$
$\land\ intr0 = 0$
$\land\ pc0 = 0$

$Init1 \triangleq$
$\land\ turn = 0$
$\land\ intr1 = 0$
$\land\ pc1 = 0$

$Init \triangleq Init0 \land Init1$

$L01 \triangleq$
$\land\ pc0 = 0$

$\land\ pc0' = 1$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$L12\ \triangleq$
$\land\ pc0 = 1$
$\land\ pc0' = 2$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$L23\ \triangleq$
$\land\ pc0 = 2$
$\land\ pc0' = 3$
$\land\ intr0' = 1$
$\land$ UNCHANGED $\langle intr1,\ turn\rangle$

$L34\ \triangleq$
$\land\ pc0 = 3$
$\land\ pc0' = 4$
$\land\ turn' = 1$
$\land$ UNCHANGED $\langle intr0,\ intr1\rangle$

$L44\ \triangleq$
$\land\ pc0 = 4$
$\land\ pc0' = 4$
$\land\ turn = 1$
$\land\ intr1 = 1$
$\land$ UNCHANGED $\langle intr0,\ intr1,\ turn\rangle$

$L45\ \triangleq$
$\land\ pc0 = 4$
$\land\ pc0' = 5$
$\land\ (turn = 0 \lor intr1 = 0)$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$L56\ \triangleq$
$\land\ pc0 = 5$
$\land\ pc0' = 6$
$\land$ UNCHANGED $\langle intr0,\ intr1,\ turn\rangle$

$L67\ \triangleq$
$\land\ pc0 = 6$
$\land\ pc0' = 7$
$\land\ intr0' = 0$
$\land$ UNCHANGED $\langle intr1,\ turn\rangle$

$L70\ \triangleq$
$\land\ pc0 = 7$
$\land\ pc0' = 0$

$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$SLOGP \triangleq$ UNCHANGED $\langle pc0,\ intr0,\ intr1,\ turn\rangle$

for the second system

$M01 \triangleq$
$\land\ pc1 = 0$
$\land\ pc1' = 1$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$M12 \triangleq$
$\land\ pc1 = 1$
$\land\ pc1' = 2$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$M23 \triangleq$
$\land\ pc1 = 2$
$\land\ pc1' = 3$
$\land\ intr1' = 1$
$\land$ UNCHANGED $\langle intr0,\ turn\rangle$

$M34 \triangleq$
$\land\ pc1 = 3$
$\land\ pc1' = 4$
$\land\ turn' = 0$
$\land$ UNCHANGED $\langle intr0,\ intr1\rangle$

$M44 \triangleq$
$\land\ pc1 = 4$
$\land\ pc1' = 4$
$\land\ turn = 0$
$\land\ intr0 = 1$
$\land$ UNCHANGED $\langle intr0,\ intr1,\ turn\rangle$

$M45 \triangleq$
$\land\ pc1 = 4$
$\land\ pc1' = 5$
$\land\ (turn = 1 \lor intr0 = 0)$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$M56 \triangleq$
$\land\ pc1 = 5$
$\land\ pc1' = 6$
$\land$ UNCHANGED $\langle intr0,\ intr1,\ turn\rangle$

$M67 \triangleq$

$\land\ pc1 = 6$
$\land\ pc1' = 7$
$\land\ intr1' = 0$
$\land$ UNCHANGED $\langle intr0,\ turn\rangle$

$M70\ \triangleq$
$\land\ pc1 = 7$
$\land\ pc1' = 0$
$\land$ UNCHANGED $\langle turn,\ intr0,\ intr1\rangle$

$SLOGQ\ \triangleq$ UNCHANGED $\langle pc1,\ intr0,\ intr1,\ turn\rangle$

$Next\_First\ \triangleq$
$\lor\ L01$
$\lor\ L12$
$\lor\ L23$
$\lor\ L34$
$\lor\ L45$
$\lor\ L56$
$\lor\ L67$
$\lor\ L70$
$\lor\ SLOGP$

$Next\_Second\ \triangleq$
$\lor\ M01$
$\lor\ M12$
$\lor\ M23$
$\lor\ M34$
$\lor\ M45$
$\lor\ M56$
$\lor\ M67$
$\lor\ M70$
$\lor\ SLOGQ$

$Next\ \triangleq\ (Next\_First \land$ UNCHANGED $pc1) \lor (Next\_Second \land$ UNCHANGED $pc0)$

$Mutual\_Exclusion\ \triangleq\ (pc0 \neq 5) \lor (pc1 \neq 5)$

we need justice conditions, because here in this example, it can happen that
the scheduler never schedules one process
we want to avoid such runs ?????

justice conditions

$J00\ \triangleq\ pc0 \neq 0$
$J02\ \triangleq\ pc0 \neq 2$
$J03\ \triangleq\ pc0 \neq 3$

we cannot write $pc0 \neq 4$, because that's not a requirement, it should be proven

$J04 \triangleq \neg((pc0 = 4) \land ((turn = 0) \lor (intr1 = 0)))$
$J05 \triangleq pc0 \neq 5$
$J06 \triangleq pc0 \neq 6$
$J07 \triangleq pc0 \neq 7$

for the process 1

$J10 \triangleq pc1 \neq 0$
$J12 \triangleq pc1 \neq 2$
$J13 \triangleq pc1 \neq 3$

$J14 \triangleq \neg((pc1 = 4) \land ((turn = 0) \lor (intr0 = 0)))$
$J15 \triangleq pc1 \neq 5$
$J16 \triangleq pc1 \neq 6$
$J17 \triangleq pc1 \neq 7$

the below justice conditions are to ensure that the scheduler is fair

$J \triangleq$
$\land J00$
$\land J02$
$\land J03$
$\land J04$
$\land J05$
$\land J06$
$\land J07$
$\land J10$
$\land J12$
$\land J13$
$\land J14$
$\land J15$
$\land J16$
$\land J17$

$Fairness \triangleq$
$\land \mathrm{WF}_{pc0}(L01)$
$\land \mathrm{WF}_{pc0}(L12)$
$\land \mathrm{WF}_{pc0}(L23)$
$\land \mathrm{WF}_{pc0}(L34)$
$\land \mathrm{WF}_{pc0}(L56)$
$\land \mathrm{WF}_{pc0}(L67)$
$\land \mathrm{WF}_{pc0}(L70)$
$\land \mathrm{WF}_{pc1}(M01)$
$\land \mathrm{WF}_{pc1}(M12)$
$\land \mathrm{WF}_{pc1}(M23)$
$\land \mathrm{WF}_{pc1}(M34)$

$\land \mathrm{WF}_{pc1}(M56)$
$\land \mathrm{WF}_{pc1}(M67)$
$\land \mathrm{WF}_{pc1}(M70)$

$vars \triangleq \langle pc0,\ pc1,\ turn,\ intr0,\ intr1 \rangle$
$FairSpec \triangleq$
$\land\ Init$
$\land \Box[Next]_{vars}$
$\land\ Fairness$

$MUTUAL\_EXCLUSION \triangleq \Box\neg((pc0 = 5) \land (pc1 = 5))$

$NOSTARVE\_1 \triangleq \Box((pc0 = 4) \Rightarrow \Diamond(pc0 = 5))$
$NOSTARVE\_2 \triangleq \Box((pc1 = 4) \Rightarrow \Diamond(pc1 = 5))$

---

* Modification History
* Last modified *Tue Mar* 05 17:28:48 *IST* 2024 by *neeraj*
* Created *Tue Mar* 05 17:17:01 *IST* 2024 by *neeraj*