- Practice on TP Spec

1. $\Diamond\Box$ type = Abort $\in$ msgs? No
2. $\Diamond\Box$(type = Abort $\vee$ type = commit) $\in$ msgs?
   Yes. But allows switch from abort to commit.
3. $\Diamond$[($\Box$ type = Abort $\in$ msgs) $\vee$ ($\Box$ type = Commit $\in$ msgs)] Yes.

- 4. $\forall rm \in Rm$:
   rmState[rm] = working $\leadsto$ rmState[rm] = prepared.
   No! RMs can abort directly!

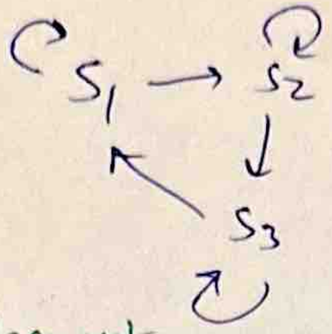
5. $\forall rm \in Rm$:
   (type = Abort) $\in$ msgs $\leadsto$ rmState[rm] = abort Yes.
   Does not need WF on TPNext. WF(RMRecv Abort) suffices. If TM has sent abort, RM must recieve it!

- How to Check liveness?

  $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$

When model checking specs with infinite traces, Cannot say $\Diamond p$ is violated if we donot see p in a finite trace prefix

- TLC approach



Check

$\boxed{\text{Fairness} \Rightarrow \text{Liveness}}$

in all cycles. Cycles give infinite traces.

If p does not hold in S_1, S_2, S_3 then $\Diamond p$ will not hold for $S_1 \to S_2 \to S_3 \to S_1 \to S_2 \to \dots$

How to prove liveness?

- $TPInit \wedge \Box TPNext \wedge WF(RmRecvAbort) \Rightarrow$

$\Box \forall rm \in RM: (type = abort \in msgs \Rightarrow$

$\Diamond rmstate[rm] = aborted)$

Say $N = TPNext / RmRecvAbort(rm)$ all other actions

$P = abort \in msgs \wedge rmState[rm] \neq aborted$

$Q = rmState[rm] = aborted$

$A = RMRecvAbort(rm)$

- $P \Rightarrow Enabled(\overset{A}{RMRecvAbort(rm)})$

(1) P keeps action enabled

$P \wedge N \Rightarrow P' \vee Q'$ all OTHER actions keep P or Q true in next state

(2) RMChooseToABort(rm)

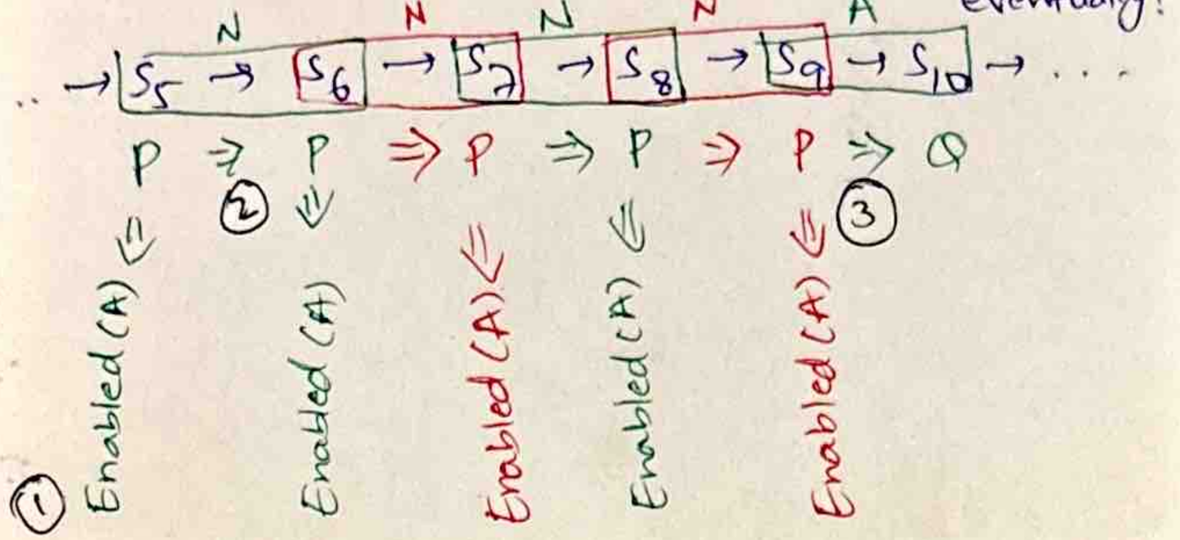
(3) $P \wedge \overset{A}{RMRecvAbort(rm)} \Rightarrow Q'$ Taking that action makes Q true

---

$\Box[N \vee A] \wedge WF(A) \Rightarrow P \rightsquigarrow Q$

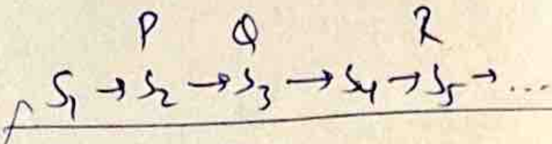
$P \leadsto Q$

Due to WF(A), A action must happen eventually!

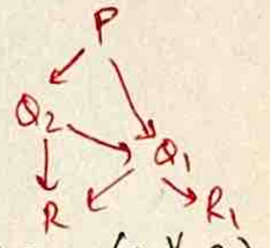


Inference rules

$$\frac{P \leadsto Q \wedge Q \leadsto R}{P \leadsto R}$$



Proof lattice



more generally

$$\frac{P \leadsto (Q_1 \vee Q_2) \wedge Q_1 \leadsto (R \vee R_1) \wedge Q_2 \leadsto (Q_1 \vee R)}{P \leadsto (R \vee R_1)}$$

Proof lattice for eventualy decided.