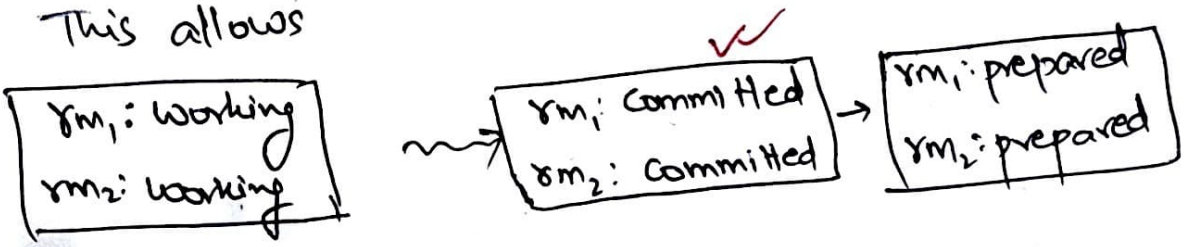
- Liveness properties

Transaction should commit or abort eventually.

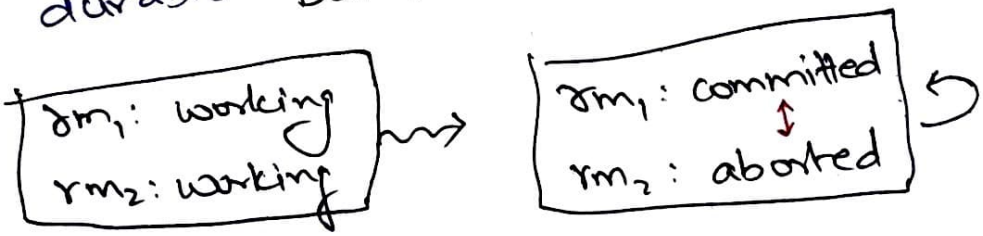
$\Diamond (\forall rm : RM : rmState[rm] \in \{committed, aborted\})$

This allows



- $\Diamond \Box \forall rm : RM : rmState[rm] = \{committed, aborted\}$

Once everyone is committed / aborted, they should stay committed / aborted, ie, transactions are durable. But this allows:

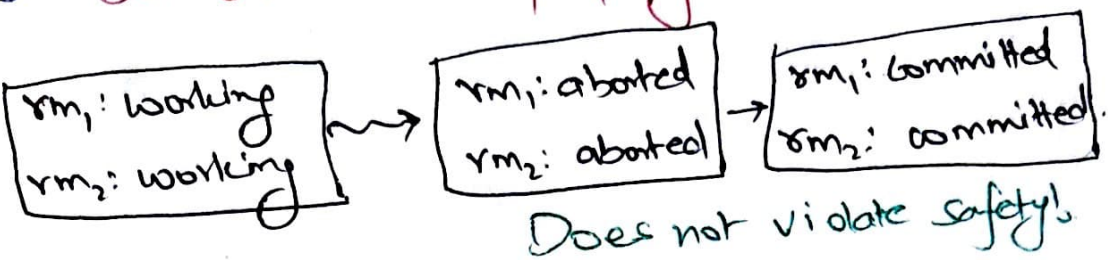


- We have already checked that this is not possible with our SAFETY property (Atomicity)

$\Box \forall rm_1, rm_2 \in RM : \neg(rmState[rm_1] = committed \wedge rmState[rm_2] = aborted)$

Is this enough?

- But our liveness property allows



Does not violate safety.

Liveness

$$\Diamond((\Box \forall rm \in RM : rmState[rm] = aborted) \vee (\Box \forall rm \in RM : rmState[rm] = committed))$$

- Try TCSpec $\Rightarrow$ Eventually Decided. using TLC

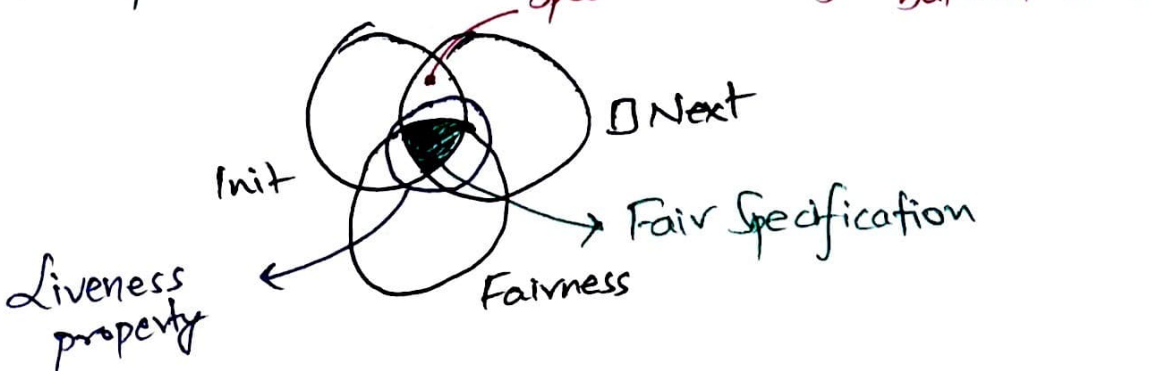
rm_1: working
rm_2: working
$\rightsquigarrow$ Stutters forever.

Liveness checking makes no sense if we don't constrain spec to make "progress"

- Constraints of progress $\equiv$ fairness property.

Resources will eventually be given
eg. to TM and RMs.

Fair Spec $\equiv$ Init $\wedge \Box$ Next $\wedge$ Fairness



- Weak fairness: either take the action or disable the action

  ¬enable

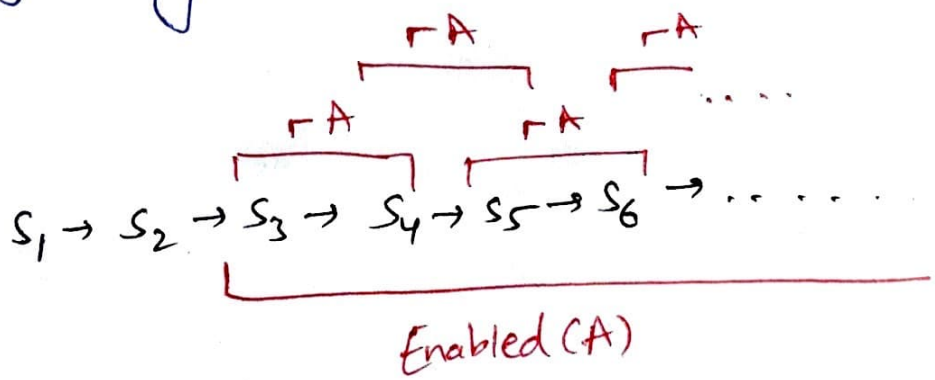
  action predicate

  Enabled(A) ≡ ∃ t: A(s,t)

  State predicate that is True iff the action can be taken.

- Weak fairness WF(A)

  following behavior is not allowed!.



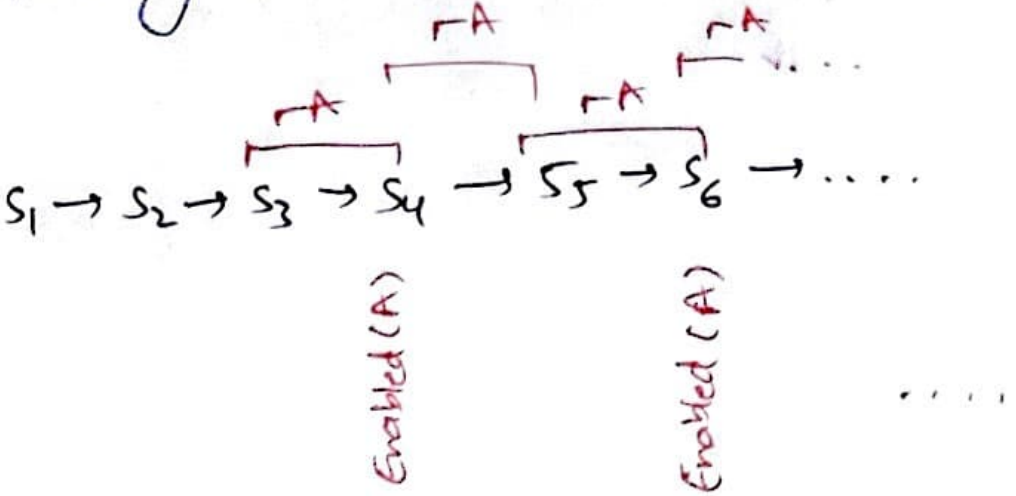
- $WF(A) \equiv \neg(\Diamond\Box \text{Enabled}(A) \wedge \Diamond\Box \neg A)$

  It should not be the case that action A is enabled forever, but action A is never taken

  $\equiv \Box\Diamond \neg \text{Enabled}(A) \vee \Box\Diamond A$

- Strong Fairness SF(A)

Following behavior is not allowed



- $SF(A) \equiv \neg(\Box\Diamond Enabled(A) \wedge \Diamond\Box \neg A)$

If should not be the case that action A gets enabled infinitely often, but action A is never taken.

$$\equiv \Diamond\Box \neg Enabled(A) \vee \Box\Diamond A$$

- what does weak and strong mean?

Nothing really.

$$SF(A) \Rightarrow WF(A)$$

Stronger condition.

$\Diamond\Box \neg Enabled(A) \vee \Box\Diamond A$ ↓ never happens

$\Rightarrow \Box\Diamond Enabled(A) \vee \Box\Diamond A$ ↓ does not happen infinitely often

Try TCSpec ^ WF(∃ rm ∈ RM : Prepare(RM))
⇒ Eventually Decided

No! stutters forever after prepare is disabled.

TCSpec ^ WF(TCNext) ⇒ Eventually Decided ✓