- TLA Inference/equivalence rules

1. $Inv \wedge Next \Rightarrow Inv'$ (Next: Action predicate)

$Inv \wedge \Box Next \Rightarrow \Box INV$

Inv: State predicate; $\Box Next$: box action predicate; $\Box INV$: Invariant

All are temporal predicates.

- 2. $\Box F \Rightarrow F$

$\forall F(s_i) \Rightarrow F(s_1)$

$\forall F(s_i, s_{i+1}) \Rightarrow F(s_1, s_2)$

holds both when F is state predicate or action predicate.

- 3. F provable by proposition logic

$\Box F$

Examples:

True, $p \Rightarrow p \vee q$, $x + x' = x' + x$

- 4 $\dfrac{F \Rightarrow G}{\Box F \Rightarrow \Box G}$

$S_1 \to S_2 \to S_3 \to S_4 \to \ldots$
F F F F ...
G G G G

$\forall F(S_i) \Rightarrow \forall G(S_i)$ state predicate

$\forall F(S_i, S_{i+1}) \Rightarrow \forall G(S_i, S_{i+1})$ action predicate

- 5. $\Box(F \wedge G) \equiv \Box F \wedge \Box G$

$S_1 \to S_2 \to S_3 \to S_4 \to S_5 \to \ldots$
F F F F F
G G G G G

Both F and G hold for every state/action

- 6. $\Box(F \vee G) \not\equiv \Box F \vee \Box G$

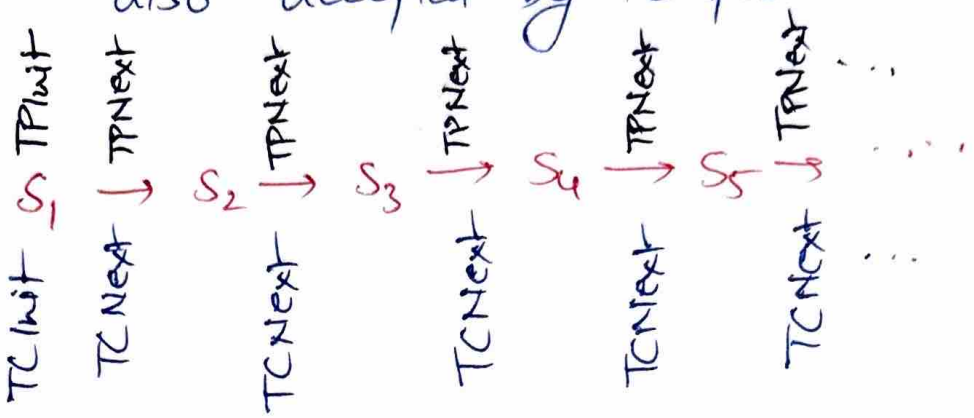
$S_1 \to S_2 \to S_3 \to S_4 \to \ldots$
F G F F

$\Box(F \vee G)$ holds. But $\Box F \vee \Box G$ does not!

$\Box F \Rightarrow \Box F \vee G$ since $F \Rightarrow F \vee G$ and rule 4

- To prove TPSpec ⇒ TCSpec.

Behaviors accepted by TPSpec are also accepted by TCSpec



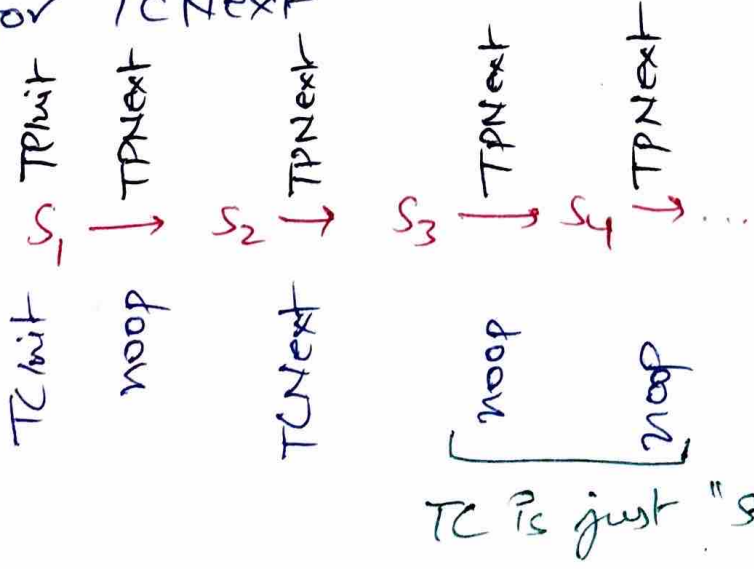
- If suffices to show

TPInit ⇒ TCInit

TPNext ⇒ TCNext

However, TCNext does not have actions for TM that TPNext has

- Such TPNext actions are a no-op for TCNext



- Hence, show

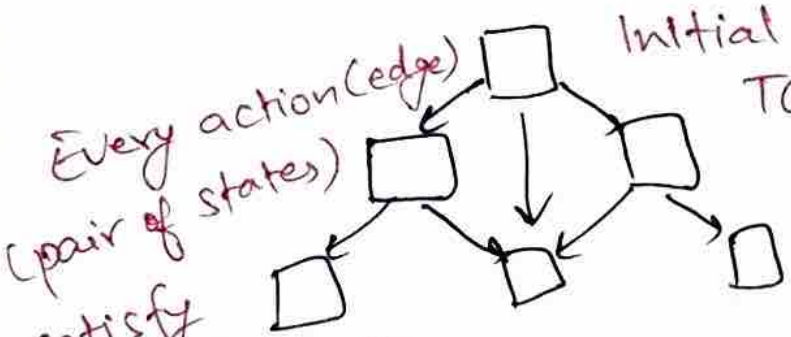
  $TPInit \Rightarrow TCInit$

  $TPNext \Rightarrow TCNext \vee \underbrace{rmState = rmState'}_{\text{noop / stuttering}}$

  $\Rightarrow [TCNext]_{rmState}$.

Demo: manual proof / TCSpec is checked as property by TLC.

- How does TLC check $TPSpec \Rightarrow TCSpec$?



- what's next?

Safety properties $\Box$ (always) $\neg$ Bad things

Bad things never happen i.e, ($\neg$ Bad things) always happens

Liveness properties

Good things eventually happen

eventually $\Diamond$ Good thing

- ◇ is dual of □

$\neg \Box p \equiv \Diamond \neg p$

$s_1 \to s_2 \to s_3 \to s_4 \to \ldots$

$\neg p$

Some place where $\neg p$ holds.

$$\neg \forall_i p(s_i) \equiv \exists_i \neg p(s_i)$$

- Similarly, $\neg \Diamond p$ says there is no state where p holds.

$\equiv \Box \neg p$

$s_1 \to s_2 \to s_3 \to \ldots$

$\neg p \quad \neg p \quad \neg p \quad \neg p \ldots$

$$\neg \exists_i p(s_i) \equiv \forall_i \neg p(s_i)$$

- Therefore ⇒ Safety = $\neg \Diamond$ Bad thing

It is not the case that bad thing eventually happens

Similarly, Liveness = $\neg \Box \neg$ Good thing

It is not the case that good thing never happens

- Practice: Say
Process X can be in ready queue r
or performing some IO operation io
CPU can be busy with some proc. b
or empty $\neg b$

- If CPU is empty and X is not ready, then X is doing IO.

$$\Box(\neg b \wedge \neg r \Rightarrow io)$$

- Process X does not suffer starvation. When it is in ready queue, it will eventually leave it

$$\Box(r \Rightarrow \Diamond \neg r)$$

$$r \rightsquigarrow \neg r$$

↑ leads to

- Process X does not get permanently blocked doing IO.

$\neg \Diamond \Box io \equiv \Box \Diamond \neg io$

It is not the case that process eventually gets permanently stuck with IO

It is always the case that the process is eventually not doing IO.

- $\Diamond \Box p$

eventually always p

$s_1 \to s_2 \to s_3 \to s_4 \to \ldots$

p

$\Diamond \Box (F \wedge G) \equiv \Diamond \Box F \wedge \Diamond \Box G$

G

$s_1 \to s_2 \to s_3 \to s_4 \to \ldots$

F

$F \wedge G$

- $\Diamond \Box F \vee G \not\equiv \Diamond \Box F \vee \Diamond \Box G$

$s_1 \to s_2 \to s_3 \to s_4 \to s_5 \to$

F G F F ...

$F \vee G$ holds

of course,

$\Diamond \Box F \Rightarrow \Diamond \Box (F \vee G)$ since $F \Rightarrow F \vee G$

- $\Box\Diamond p$ Always eventually p

$$s_1 \to s_2 \to s_3 \to s_4 \to \dots$$
$$p \qquad p \qquad p \qquad \dots$$

p happens Infinity often.

$\Box\Diamond(F \wedge G) \not\equiv \Box\Diamond F \wedge \Box\Diamond G$

$$s_1 \to s_2 \to s_3 \to s_4 \to \dots$$
G and $\qquad F \qquad G \qquad F \qquad G$

F happens Infinitely often. But F^G does not!

- $\Box\Diamond \quad (F \vee G) \equiv \Box\Diamond F \vee \Box\Diamond G$

$$s_1 \to s_2 \to s_3 \to s_4 \to s_5 \to \dots$$
$$F \vee G \qquad F \vee G \quad F \vee G$$

If $F \vee G$ is happening Infinitely often. either

F " " " " or

G " " " " or both

- $\ulcorner \Box\Diamond (F \vee G) \equiv \ulcorner(\Box\Diamond F \vee \Box\Diamond G)$

$\Diamond \ulcorner \Diamond (F \vee G) \equiv \ulcorner \Box\Diamond F \wedge \ulcorner \Box\Diamond G$

$\Diamond\Box \ulcorner (F \vee G) \equiv \Diamond \ulcorner \Diamond F \wedge \Diamond \ulcorner \Diamond G$

$\Diamond\Box(\ulcorner F \wedge \ulcorner G) \equiv \Diamond\Box \ulcorner F \wedge \Diamond\Box \ulcorner G$