Lecture 15 - March 5

Model Checking

Model Satisfaction
Path vs. Model Satisfactions: X,G, F

Announcements/Reminders

- **ProgTest1** results to be released (by end of Friday)
- **WrittenTest1** guide & examples released
- **Review Q&A** materials posted
- **Lab3** to be released after WrittenTest1
- Office Hours: 3pm to 4pm, Mon/Tue/Wed/Thu
- TA contact information (on-demand for labs) on eClass

Model Satisfaction

Given:

- Model $M = (S, \longrightarrow, L)$
- State $s \in S$
- LTL Formula ϕ

$\forall$

$M, s \models \phi$ **iff** for $\boxed{\text{every path } \pi}$ of M starting at s, $\pi \models \phi$.

Formulation (over all paths)

model sat (where M is clear in the context)

$\pi = s \to \cdots$

path sat.

$$s \models \phi \iff \forall \pi \cdot \boxed{\pi \text{ starts with } s \land s \in S} \Rightarrow \pi \models \phi$$

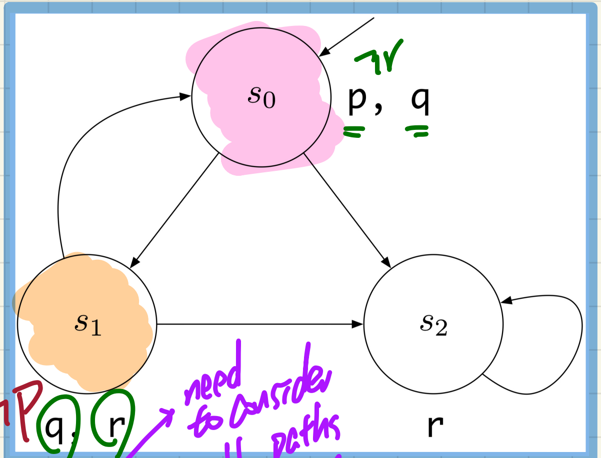
$\pi \not\models \phi$

How to prove vs. disprove $M, s \models \phi$?

(1) To prove $s \models \phi$, need to show that every path (pattern) π, $\pi \models \phi$

(2) To disprove $s \models \phi$, provide a witness path π, $\boxed{\neg(\pi \models \phi)}$

Model vs. Path Satisfaction: Exercises (1.2)



$s \models p \Leftrightarrow$ all π starting at s, $\pi \models p$

$s_0 \in S$ model sat. (all paths starting s_0)

all such path π has $\pi^1 = s_0 \to \dots$

only need to consider s_0 to evaluate props. formula.

s_0	$\models$	$\top$	T
s_0	$\not\models$	$\bot$	T
s_0	$\models$	$p \land q$	T
s_0	$\models$	$p \lor q$	T
s_0	$\models$	$p \Rightarrow q$	T
s_0	$\models$	r	F
s_0	$\models$	$\boxed{r \Rightarrow p \land q \land r}$	T

$\pi = s_0 \to s_1 \to \dots$

need to consider all paths starting s_1

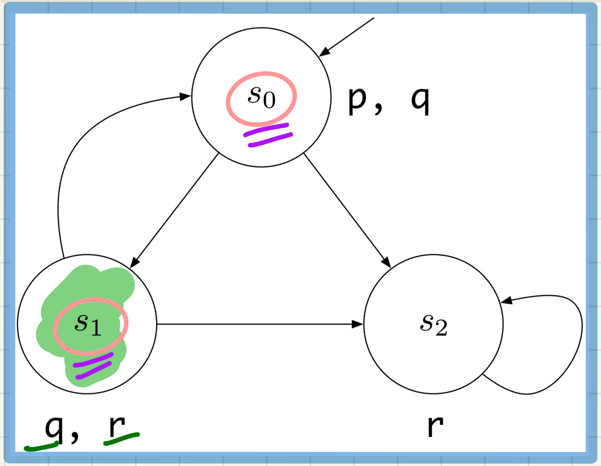
s_1	$\models$	$\top$	
s_1	$\not\models$	$\bot$	
s_1	$\models$	$p \land q$	F
s_1	$\models$	$p \lor q$	T
s_1	$\models$	$p \Rightarrow q$	T
s_1	$\models$	$r \Rightarrow p \land q \land r$	F

when eval. prop. $s_1 \models p$ vs. $\pi_1 \models p$

as $\#$: $s_0 \models p$

Exercise: What if we change the LHS to s_1?

Model vs. Path Satisfaction: Exercises (2.1)



Recall: $\pi \models \mathbf{X}\,\phi \iff \pi^2 \models \phi$

Say: $\pi = s_0 \rightarrow \overbrace{s_1 \rightarrow s_2 \rightarrow s_2 \rightarrow \dots}^{\pi^2}$

path sat.

$\pi \models \mathbf{X}\,\top \iff \pi^2 \models \top$ T

$\pi \not\models \mathbf{X}\,\bot$ T

$\pi \models \mathbf{X}\,(q \wedge r)$ T

$\pi \models \boxed{\mathbf{X}\,q \wedge r}$ F $\iff \boxed{\pi \models \mathbf{X}\,q} \wedge \boxed{\pi \models r}$

$\pi^2 \models q$ T F

$\pi \models \mathbf{X}\,(q \Rightarrow r)$ T

$\pi \models \boxed{\mathbf{X}\,q \Rightarrow r} \iff \boxed{\pi \models \mathbf{X}\,q} \Rightarrow \boxed{\pi \models r}$

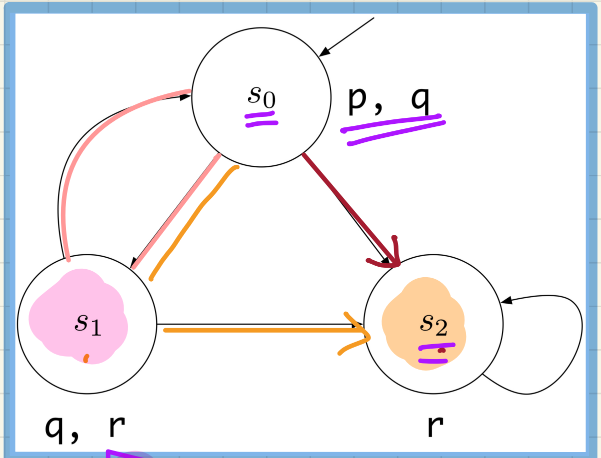
T T F

F.

$\pi^2 \models q$

Exercise: What if we change the LHS to π^2? Exercise

Model vs. Path Satisfaction: Exercises (2.2)



$s \models \phi \Leftrightarrow$ all π starting at s, $\pi \models \phi$

model sat. (consider all paths starting from s_0)

satisfied by s_1 and s_2?

$s_0 \models X\ \top$ (T)

$s_0 \not\models X\ \bot$ (T)

$s_0 \models X\ (q \land r)$ (F) witness: $s_0 \to \boxed{s_2} \to s_2 \to \dots$ — only satisfies r.

$s_0 \models X\ q \land r$ (F) ① witness: $s_0 \to \boxed{s_2^*} \to \dots$ — not sat. q ② $\boxed{s_0^*} \to s_2 \to$ — not sat. r.

$s_0 \models X\ (q \Rightarrow r)$ (T)

$s_0 \models \boxed{X\ q \Rightarrow \boxed{r}}$ (T) F (F) witness: $s_0 \to s_2^* \to s_2 \to \dots$ — not sat. q

→ - - only need to consider s_1 and s_2

(1) $s_0 \to s_1 \to s_0 \to s_1 \to \dots$

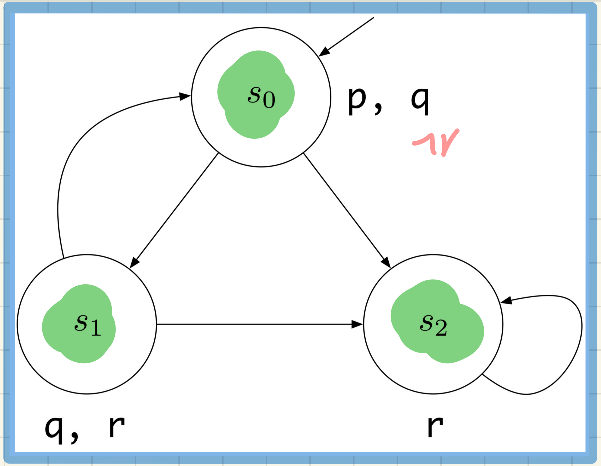
(2) $s_0 \to s_2 \to s_2 \to \dots$

(3) $s_0 \to s_1 \to s_0 \to \dots \to s_1 \to s_2 \to s_2$

next states of paths starting from s_0

Exercise: What if we change the LHS to s_1?

Model vs. Path Satisfaction: Exercises (3.1)



$$\pi \models G\ \phi \Leftrightarrow \forall i \bullet i \geq 1 \Rightarrow \pi^i \models \phi$$

Say: $\pi = s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow s_2 \longrightarrow \dots$

↳ reachable = $\{s_0, s_1, s_2\}$

$\pi \models G\ \top$ T

$\pi \not\models G\ \bot$ T

$\neg p \vee \neg r$

$\pi \models G\ \boxed{\neg(p \wedge r)}$ T

e.g. in s_0, $\neg r$ is true.

$\pi \models G\ r$ F → witness: $\overset{\pi^1}{s_0}$, $\neg r$

$\pi^2 \models G\ r$

reachable = $\{s_1, s_2\}$

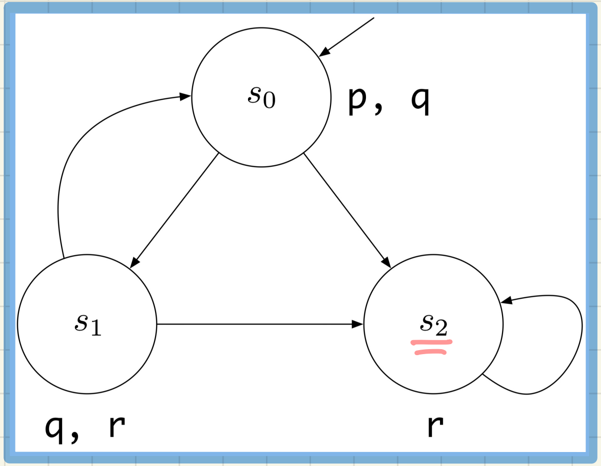
check these on reachable states of paths.

Exercise: What if we change the LHS to π^2?

Model vs. Path Satisfaction: Exercises (3.2)

$s_1 \models G\, r$ F. Witness: $s_1 \to s_0 \to s_1$ ($\neg r$ at s_0)

reachable = $\{s_0, s_1, s_2\}$



$s \models \phi \Leftrightarrow$ all π starting at s, $\pi \models \phi$

model sat. (all paths starting from s_0)

$s_0 \models G\, \top$ T

$s_0 \not\models G\, \bot$ T

$s_0 \models G\, \neg(p \land r)$ T ∵ $\neg p \lor \neg r$ sat. in all states.

($\neg(p \land r)$: $\neg p \lor \neg r$)

$s_0 \models G\, r$ F Witness: $s_0 \to s_1 \to s_0 \to$ (r not sat. at s_0)

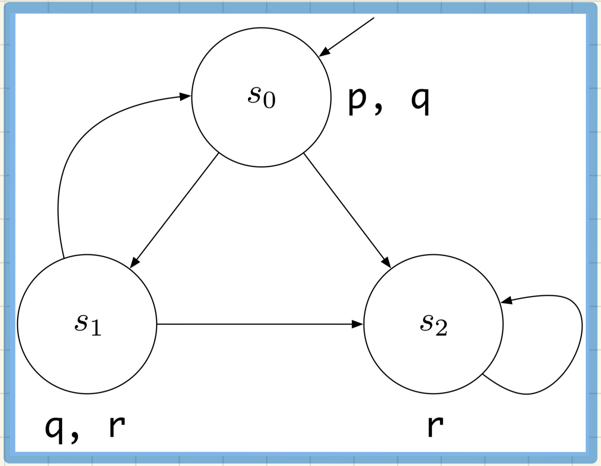
$s_2 \models G\, r$ T

s_2 is the only reachable state for all paths starting at s_2

Reachable states from paths starting at s_0 = $\{s_0, s_1, s_2\}$

Exercise: What if we change the LHS to s_1?

Model vs. Path Satisfaction: Exercises (4.1)



$\pi \models \mathbf{F}\,\phi \iff \exists i \bullet i \geq 1 \land \pi^i \models \phi$

Say: $\pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_2 \rightarrow \ldots$

↳ reaches $\{s_0, s_1, s_2\}$

$\pi \models \mathbf{F}\ \top$ — T

$\pi \not\models \mathbf{F}\ \bot$ — T

$\neg p \lor \neg r$

$\pi \models \mathbf{F}\ \boxed{\neg(p \land r)}$ — T witness state: s_0

$\pi \models \mathbf{F}\ r$ — T witness: s_2

$\pi \models \mathbf{F}\ (q \land r)$ — T witness: s_1

Exercise: What if we change the LHS to π^2?