Lecture 13 - March 14

Model Checking

Model Satisfaction: Nested LTL Operators
$GF\,\phi$, $GF\,\phi \Rightarrow GF\,\phi$
LTL Operators: Until, Weak Until, Release

Announcements

- ProgTest1 result to be released by Friday
- Lab3 to be released by the end of Thursday

mutual
exclusion

textual

G
T
F.

Nesting "Global" and "Future" in LTL Formulas

$s \models GF\,\phi$

infinitely often

$\pi: \bigcirc \to \bigcirc \to \bigcirc \to \cdots \bigcirc \to \cdots$

(1) ϕ should "almost" always true
(2) relative to any state, can't wait indefinitely for ϕ to be true again

Each path starting with s is s.t. continuously, ϕ eventually holds.

Q. **Formulate** the above nested pattern of LTL operator.

$* \forall \pi \cdot \pi = s \to \cdots \Rightarrow ($ $***$

$** \forall i \cdot i \geq 1 \Rightarrow (\exists j \cdot j \geq i \wedge \pi^{j} \models \phi)$

$)$

Q. How to **prove** the above nested pattern of LTL operators?

(1) consider path patterns (2) argue for each state on the path p.
(3) for each state, where's the future state that satisfies ϕ.

Q. How to **disprove** the above nested pattern of LTL operators?

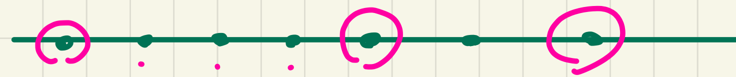
* Give a witness path π

** Give a witness state on π, say s'

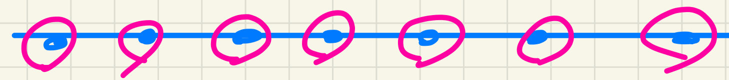
$G \neg \phi$

$\boxed{*** \text{ relative to } s' \text{ on } \pi, \ \phi \text{ is never true.}}$

(1) $GF\phi$

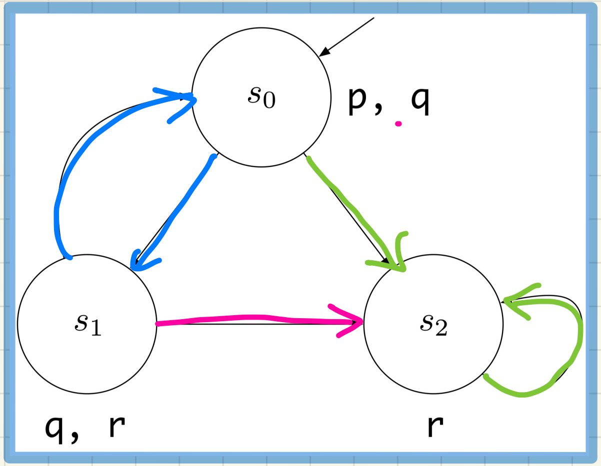


(2) $G\phi$



$$\boxed{\begin{array}{c} (2) \Rightarrow (1) \\ (1) \not\Rightarrow (2) \end{array}}$$

Model Satisfaction: Exercises (6.1)



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

$s_0 \models \mathbf{GF}\ p$ $\boxed{\text{false}}$

$\boxed{s_0} \rightarrow \boxed{s_2} \rightarrow \boxed{s_2} \rightarrow \cdots$

p $\quad \neg p$

$s_0 \models \mathbf{GF}\ (p \vee q)$ $\boxed{\text{false}}$

$\boxed{s_0} \rightarrow s_2 \rightarrow s_2 \rightarrow \cdots$

$p \vee q$ $\quad \neg(p \vee q)$

$\because s_0 \models G(p \vee r)$

$\Rightarrow s_0 \models GF(p \vee r)$

$s_0 \models GF(p \vee r)$

$\boxed{\text{True}}$

$\hookrightarrow \because$ all states satisfy $p \vee r$

Path Patterns

(1) $s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_1 \rightarrow \cdots$

(2) $s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow \cdots$

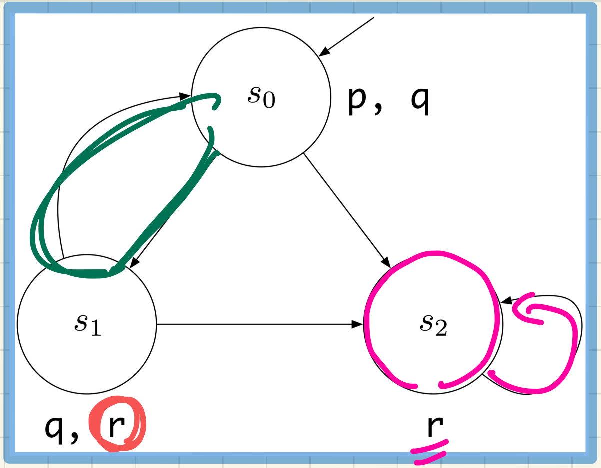
(3) $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \cdots$

(4) $s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_1 \cdots \rightarrow s_1 \rightarrow s_2 \rightarrow s_2 \rightarrow \cdots$

(5) $s_0 \rightarrow s_1 \rightarrow s_0 \rightarrow s_2 \rightarrow \cdots$

Exercise: What if we change the LHS to s_2?

Model Satisfaction: Exercises (6.2)



$S_0 \models GF\,p \Rightarrow G\,r$ $\boxed{\text{false}}$

Just. For $S_0 \to S_1 \to \cdots$, r is not continuously true.

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

$\boxed{s_0 \models GF\,p \Rightarrow GF\,r}$ $\boxed{\text{true}}$.

$\forall \pi \cdot \pi = S \to \cdots \Rightarrow ($

$(\forall i \cdots \Rightarrow$

$\exists j \cdots \wedge \pi^j \models p)$

$\Rightarrow (\forall i \cdot \cdots \Rightarrow (\exists j \cdot \cdots \wedge \pi^j \models r))$

$)$

(1) assume GF p: only path to consider is $S_0 \to S_1 \to S_0 \to \cdots$

(2) In that path: GF r true.

$s0 \models GF\,r \Rightarrow GF\,p$ $\boxed{\text{false}}$.

Witness

$S_0 \to S_2 \to S_2 \to \cdots$

GF r is True

but GF p is false

$T \Rightarrow F = F$.

Exercise: What if we change the LHS to s_2?

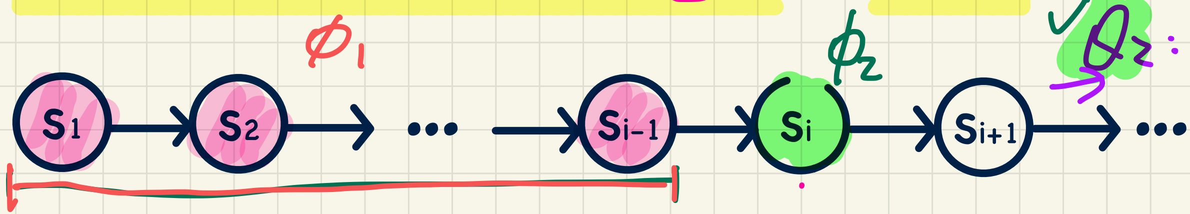
Path Satisfaction: Temporal Operations (4)

$\pi \models \phi 1 \; U \; \phi 2$ until

There is some future state satisfies $\phi 2$, and **until then**, all states satisfy $\phi 1$.

Q_1: Is it ok that $G\,\phi_1$ but $G\,\neg\phi_2$? ✗

Q_2: Is it ok that $G\,\phi_1$ and $F\,\phi_2$? ✓



Formulation (over a path)

$$\pi \models \phi_1 \,\mathcal{U}\, \phi_2 \iff \left(\exists i \cdot i \geq 1 \wedge \left(\begin{array}{l} \pi^{i} \models \phi_2 \\ \wedge \\ (\forall j \cdot 1 \leq j \leq i-1 \Rightarrow \pi^{j} \models \phi_1) \end{array} \right) \right)$$

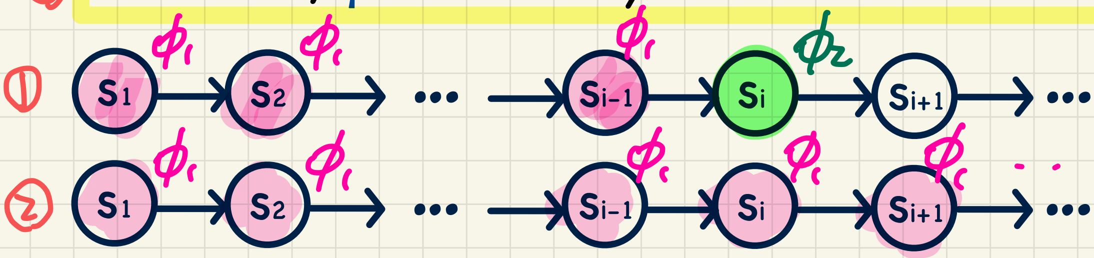
Path Satisfaction: Temporal Operations (5)

weak until

$\pi \models \phi_1 \, W \, \phi_2$

① If there is ever a future state that satisfies ϕ_2, then until then, all states satisfy ϕ_1.

② ~~Otherwise~~ Or, ϕ_1 must always be the case.



Q1. Is it ok that $G\,\phi_1$ but $\boxed{G\,\neg\phi_2}$. ok

Q2. Is it ok that $G\,\phi_1$ and $F\,\phi_2$? ✓

Formulation (over a path)

$$\phi_1 \,\mathcal{W}\, \phi_2 \iff \phi_1 \,\mathcal{U}\, \phi_2 \lor (\forall k \cdot k \geq 1 \Rightarrow \pi^k \models \phi_1)$$

$$\phi_1 \,\mathcal{W}\, \phi_2 \iff \phi_1 \,\mathcal{U}\, \phi_2 \lor \underline{G\,\phi_1}$$

P

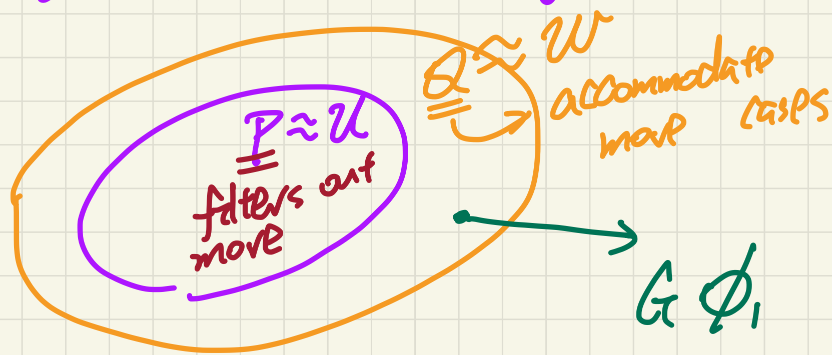
q

$P \Rightarrow q$

stronger — weaker

satisfying values

$\{x \mid P(x)\} \subseteq \{x \mid q(x)\}$



Path Satisfaction: Temporal Operations (6)

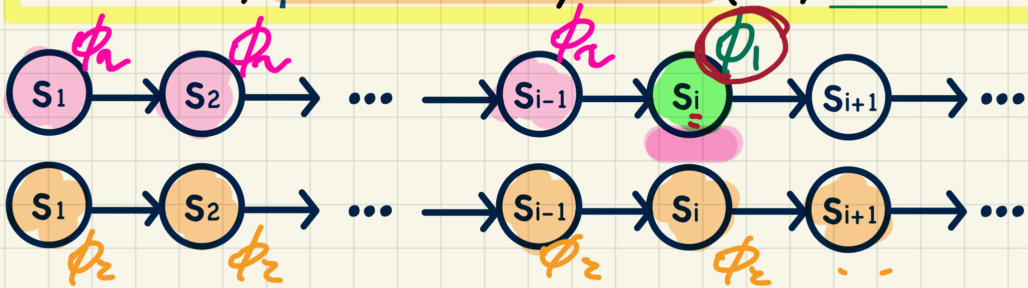
release

$\pi \models \phi 1 \; R \; \phi 2$ → "ϕ_2 has been holding, ϕ_1 releases it"

If there is ever a future state that satisfies $\phi 1$, then until then, all states satisfy $\phi 2$.

OV

~~Otherwise~~, $\phi 2$ must always hold (i.e., never released).



Formulation (over a path)

$$\pi \models \phi_1 R \phi_2 \iff \left(\left(\exists i \cdot i \geq 1 \wedge \left(\pi^i \models \phi_1 \wedge \left(\forall j \cdot j \leq i \cdot \pi^j \models \phi_2 \right) \right) \right) \vee \underbrace{\left(\forall k \cdot k \geq 1 \Rightarrow \pi^k \models \phi_2 \right)}_{G \phi_2} \right)$$

this disjunct put constraints on ϕ_1 being satisfied