Lecture 17 - March 17

Model Checking

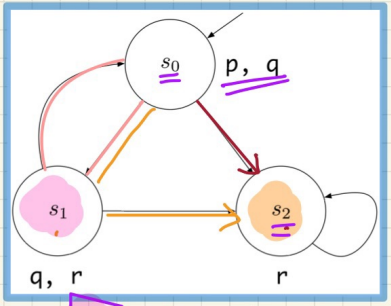
Parsing Property
Exercise: Fϕ ⇒ FGϕ
Nesting Temporal Operators: GFϕ

Announcements/Reminders

- **ProgTest2** guide & example questions released
- **WrittenTest2** potential shift of date?
- **ProgTest1** results & feedback released
  + Submit a regrading request if necessary.
- **WT1** results & feedback released
- **Lab3** due today
- Office Hours: 3pm to 4pm, Mon/Tue/Wed/Thu
- TA contact information (on-demand for labs) on eClass

Correction: Exercise 2.2 from March 5

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)

$s_0 \models X\ \top$ ⊤ satisfied by s_1 and s_2?

$s_0 \not\models X\ \bot$ ⊤

$s_0 \models X\ (q \wedge r)$ F witness: $s_0 \to s_2 \to s_2 \to \ldots$ only satisfies r.

$s_0 \models X\ q \wedge r$ F witness: $s_0 \to s_2 \to \ldots$ not sat. q; $s_0 \to s_2 \to$ not sat. r.

$s_0 \models X\ (q \Rightarrow r)$ ⊤

$s_0 \models X\ q \Rightarrow r$ ⊤ only need to consider s_1 and s_2

F witness: $s_0 \to s_2 \to s_2 \to \ldots$ not sat. q

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

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

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

next states of paths starting from s_0

Exercise: What if we change the LHS to s_1?

false.

what about $s_0 \to s_1 \to \ldots$?

s_0: r?

s_1: q?

YES

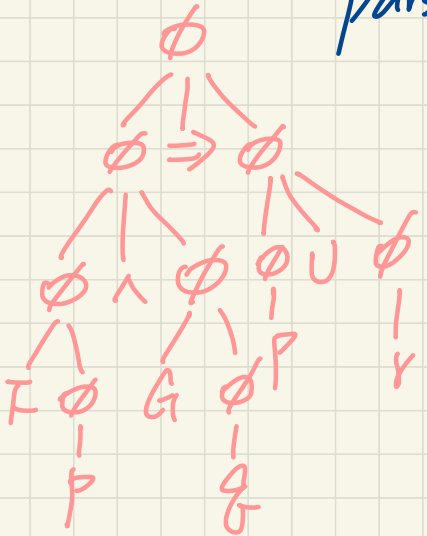
$T \Rightarrow F$

F!

Given two LTL formula strings f_1 and f_2

$Fp \wedge Gq \Rightarrow p \,U\, r$ $(Fp) \wedge (Gq) \Rightarrow (p \,U\, r)$

(1) If $f_1 \neq f_2$ (different spellings), but f_1 and f_2 have the same parse tree, f_1 and f_2 are considered as semantically equivalent.

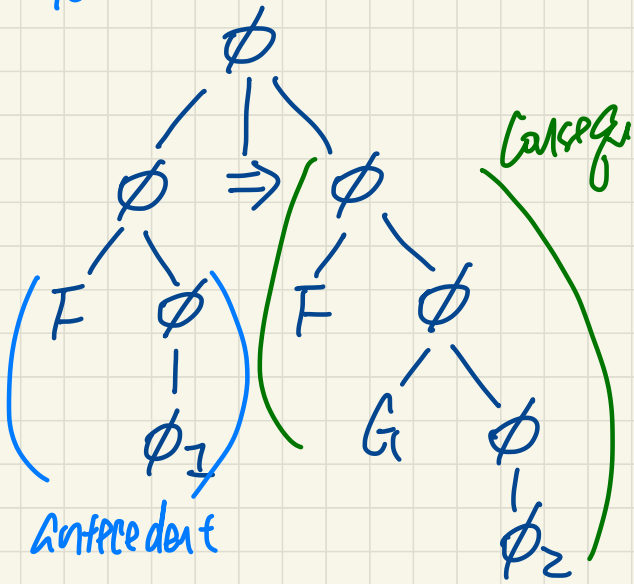


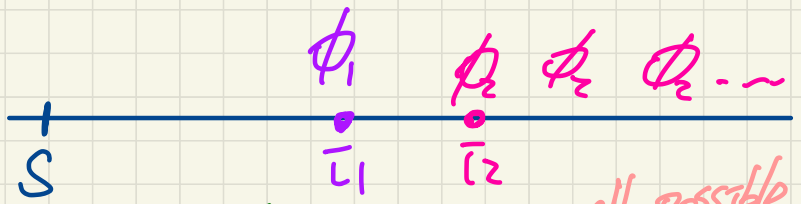
(2) If $f_1 = f_2$, but f_1 and f_2 have distinct PTs, this means the grammar is ambiguous. (e.g., "dangling else").

$S \models F\phi_1 \Rightarrow FG\phi_2$

Consider all paths $\pi = s \to \cdots$

If at some future point $\bar{i}_1$, ϕ_1 is true,
then at some future point $\bar{i}_2$ $G\phi_2$ is true.





all possible.

① $\bar{i}_1 < \bar{i}_2$
② $\bar{i}_1 > \bar{i}_2$
③ $\bar{i}_1 = \bar{i}_2$

Nesting "Global" and "Future" in LTL Formulas

$s \models F\phi_1 \Rightarrow FG\phi_2$

Each path π starting with s is s.t. if eventually $\phi 1$ holds on π, then $\phi 2$ eventually holds on π continuously.

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

$$\forall \pi \cdot \pi = s \rightarrow \cdots \Rightarrow \Big((\exists i_1 \cdot i_1 \geq 1 \wedge \pi^{i_1} \models \phi_1) \Rightarrow (\exists i_2 \cdot i_2 \geq 1 \wedge (\forall j \cdot j \geq i_2 \Rightarrow \pi^j \models \phi_2)) \Big)$$

c. $\_ \Rightarrow T$

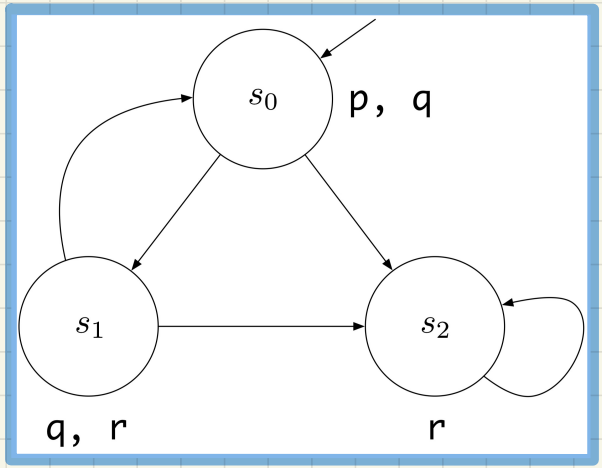
Q. How to **prove** the above nested pattern of LTL operators?

① Consider all path patterns starting with s ② for each path a. $T \Rightarrow T$ b. $F \Rightarrow \_$

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

① Show a witness path π ② for π, show: $T \Rightarrow F$

Model Satisfaction: Exercises (5.2)



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

$s_0 \models F(\neg q \wedge r) \Rightarrow FG\ r$ (T)

① $s_0 \to s_1 \to s_0 \to s_2 \to \cdots$
↳ reachable states: s_0 and s_1 (¬q)
↳ $F(\neg q \wedge r)$ is false
↳ false $\Rightarrow$ _ ≡ True

$s_0 \models F(\neg q \vee r) \Rightarrow FG\ r$ (F.)

② $s_0 \to s_2 \to s_2 \to \cdots$
↳ s_2 satisfies r, and the remaining path all reach s_2
↳ FG r is True
↳ _ ⇒ True ≡ True.

Witness: $s_0 \to s_1 \to s_0 \to s_2 \to \cdots$
$F(\neg q \vee r)$: established by s_1
FG r: always violated by s_0
↳ T ⇒ F ≡ F.

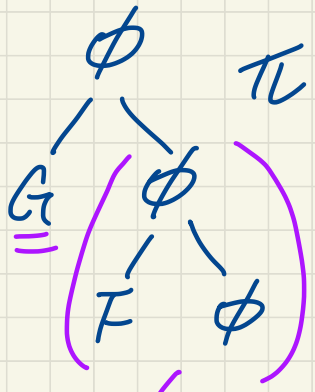
③ $s_0 \to s_1 \to s_0 \to \cdots \to s_2 \to s_2$

④ $s_0 \to s_2 \to \cdots \to s_0 \to s_2$

Exercise: What if we change the LHS to s_2?

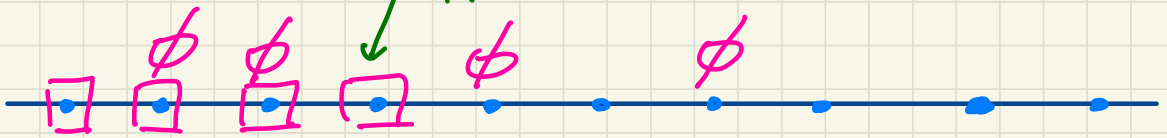
Exercise: compare $G\phi$ vs. $GF\phi$

$S \models GF\phi$



this property is globally true

↳ for each state, it's always possible to find a future point that satisfies ϕ.



↳ $GF\phi$ is false if there is a state s_i from which no future point can be found that satisfies ϕ

$G\neg\phi$

Nesting "Global" and "Future" in LTL Formulas

$s \overset{*}{\models} \mathbf{GF}\ \phi$ → infinitely often, ϕ is true.

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

Q. Formulate the above nested pattern of LTL operator.

$* \ \forall \pi \cdot \pi = s \rightarrow \cdots \Rightarrow$

$\left(\forall i \cdot i \geq 1 \Rightarrow \left(\exists j \cdot j \geq i \wedge \pi^j \models \phi \right) \right)$

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

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

Exercice 1

(1) $GF\phi \Rightarrow G\phi$

(2) $G\phi \Rightarrow GF\phi$

(3) $GF\phi \Leftrightarrow G\phi$

Exercise 2

(1) $FG\phi \Rightarrow GF\phi$

(2) $GF\phi \Rightarrow FG\phi$

(3) $FG\phi \Leftrightarrow GF\phi$