Lecture 11 - February 28

Model Checking

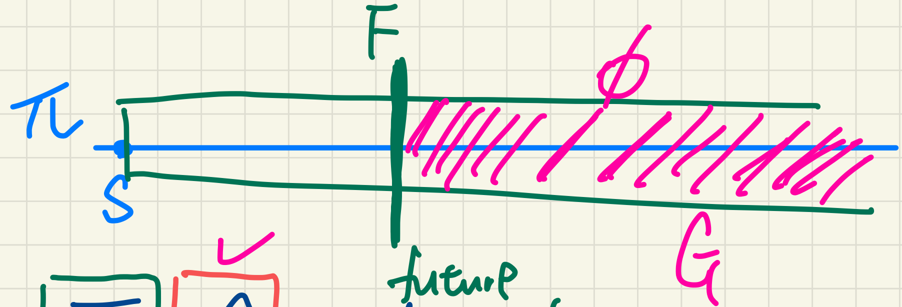
Path Satisfaction: Nested LTL Operators
FG vs. F => FG

Announcements

progtest1

- Released: WrittenTest1, $\boxed{\text{Lab2}}$ solution
- To be released:
  + ProgTest1 Guide (by the end of Wednesday)
  + ProgTest1 practice questions (by Thursday class)

- 1 ~ 2 algorithms
- conditionals, loops, tuples
- assertions (postcondition)



future point

$$s \models FG\phi$$

some state

model satisfaction
(consider all paths starting with s).

arbitrary LTL formula

$\forall x \cdot P(x)$

disprove:

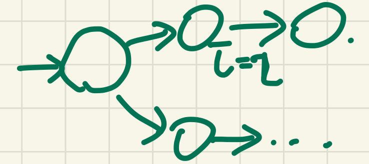
- find an x s.t. $\neg P(x)$

$\exists x \cdot P(x)$

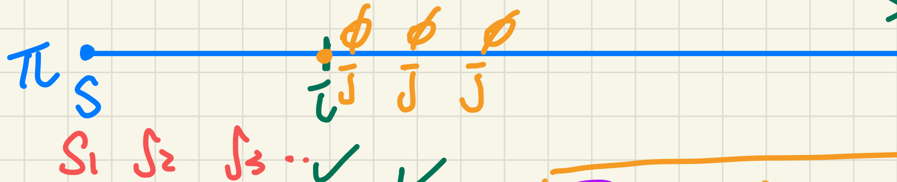
disprove:

- find all possible x s.t. $\neg P(x)$

Nesting "Global" and "Future" in LTL Formulas



$$s \models \mathbf{FG}\ \phi$$



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

Q. Formulate the above nested pattern of LTL operator.

specific to the π being considered

$$* \forall \pi \bullet \pi = s \rightarrow \cdots \Rightarrow ^{***}$$
$$^{**}(\exists i \bullet i \geq 1 \land (\forall j \bullet j \geq i \Rightarrow (\pi^{j} \models \phi)))$$

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

* ① consider all path patterns starting from s

** ② find such i *** ③ each state subsequent to ith state (including ith state) satisfies ϕ

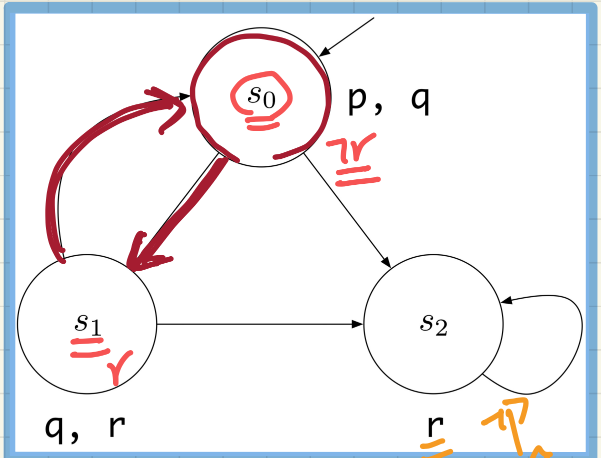
Q. How to disprove the above nested pattern of LTL operators?

* ① Find a witness $\pi = s \rightarrow \cdots$

** ② Show that for each state in π.

*** ③ there's one subsequent state that violates ϕ.

Path Satisfaction: Exercises (5.1)



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

$s_0 \models$ FG r false

Witness: $s_0 \to s_1 \to s_0 \to s_1 \to \cdots$

violates r, cannot be ignored in path

$s_0 \models$ FG (p $\vee$ q) false

Witness: $s_0 \to s_2 \to s_2 \to \cdots$

get stuck here, and both p and q are violated

$s_0 \models$ FG (p $\vee$ r) True

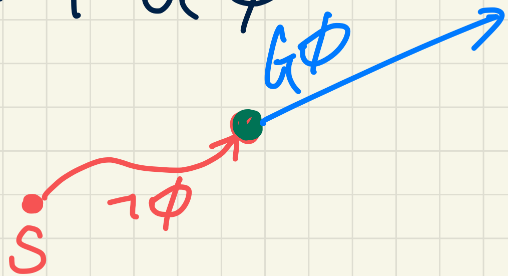
states involved in all possible paths satisfy p∨q.

① $s_0 \to s_2 \to s_2 \to \cdots$
② $s_0 \to s_1 \to s_2 \to s_2 \to \cdots$
③ $s_0 \to s_1 \to s_0 \to s_1 \to \cdots$

Exercise: What if we change the LHS to s_2?

$$S \models G\phi$$

$$S \models FG\phi$$

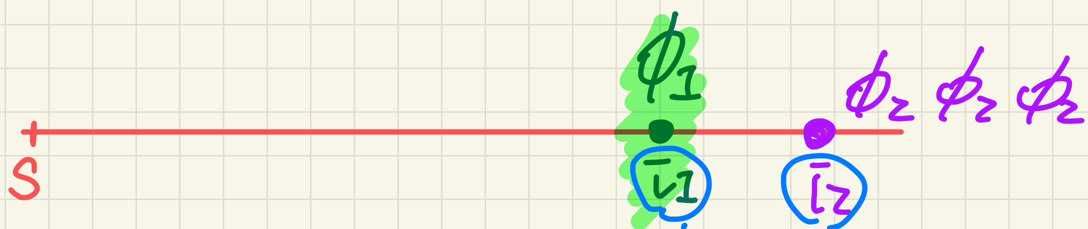


for each π.

$$S \models \boxed{F\phi_1} \Rightarrow \boxed{\underline{E}G\phi_2}$$

Consider all paths

$\pi = S \rightarrow \cdots$



may or may not be the same

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

Nesting "Global" and "Future" in LTL Formulas

$$s \models \boxed{F\phi 1} \Rightarrow \boxed{FG\phi_2}$$

Each path π starting with s is s.t. if eventually ϕ1 holds on π, then ϕ2 eventually holds on π continuously.

Q. Formulate the above nested pattern of LTL operators.

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

$i_1 \quad i_1 \quad i_1 \quad i_2 \quad i_2 \quad i_2$

dummies at different scopes

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

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