15-414 Bug Catching:

Model Checking

Soonho Kong
soonhok@cs.cmu.edu

10 Oct 2011

Model Checking

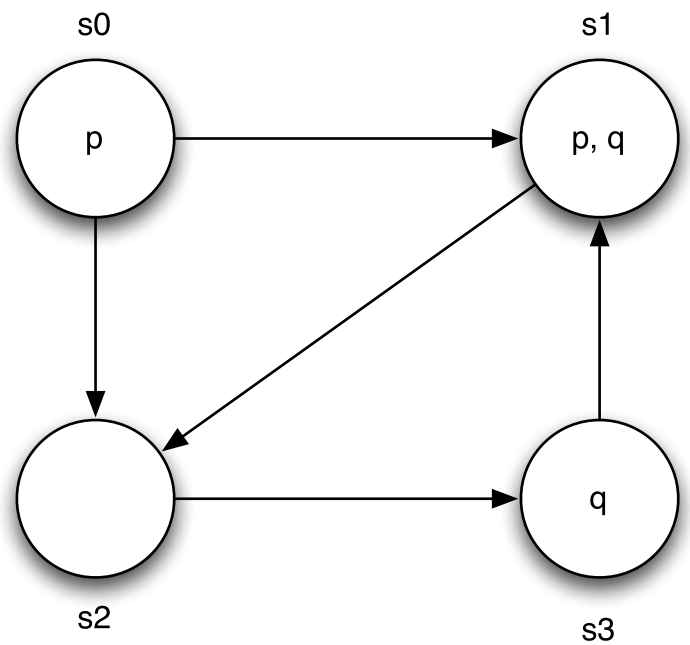
Model Checking

What is “Model”?

Model Checking

Kripke Structure is a triple $\langle S, R, L \rangle$, where

- S is the set of states
- $R \subseteq S \times S$ is the transition relation (left-total), and
- $L : S \to \mathcal{P}(AP)$ gives the set of atomic propositions ***true*** in each state



Model Checking

What to Check?

Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s*.**

$$M, s \models f$$

Kripke Structure

state

Property
(Temporal Logic Formula)

Model Checking Problem

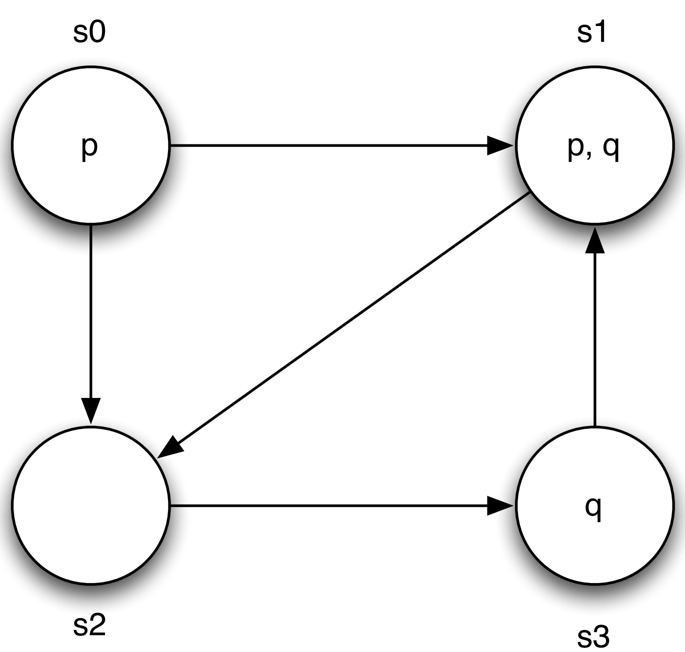
Find all states ***s*** such that ***M*** has property ***f*** at state ***s*.**

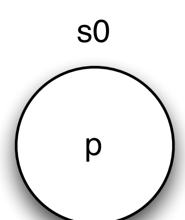
$$M, s \models f$$

Kripke Structure

state

Property
(Temporal Logic Formula)





?

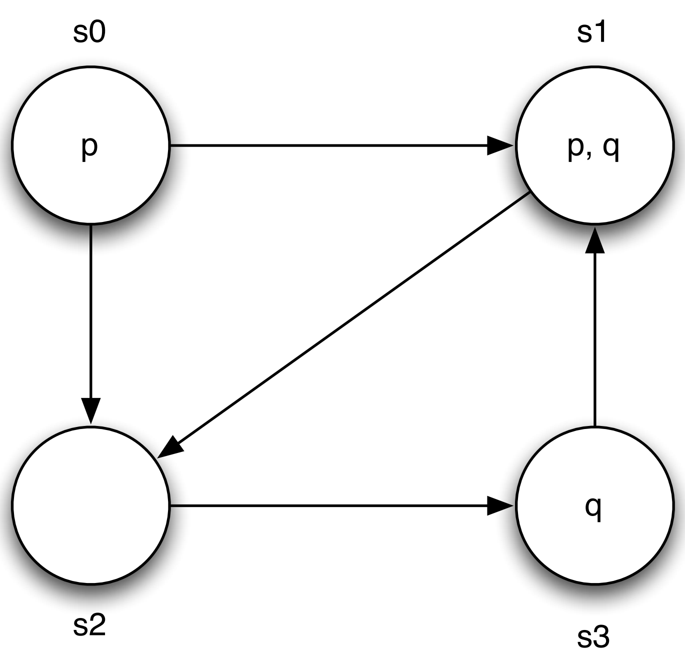
$$\mathbf{EX}\ q$$

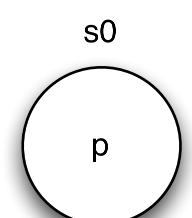
Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s***.

$$M, s \models f$$

Kripke Structure   state   Property (Temporal Logic Formula)





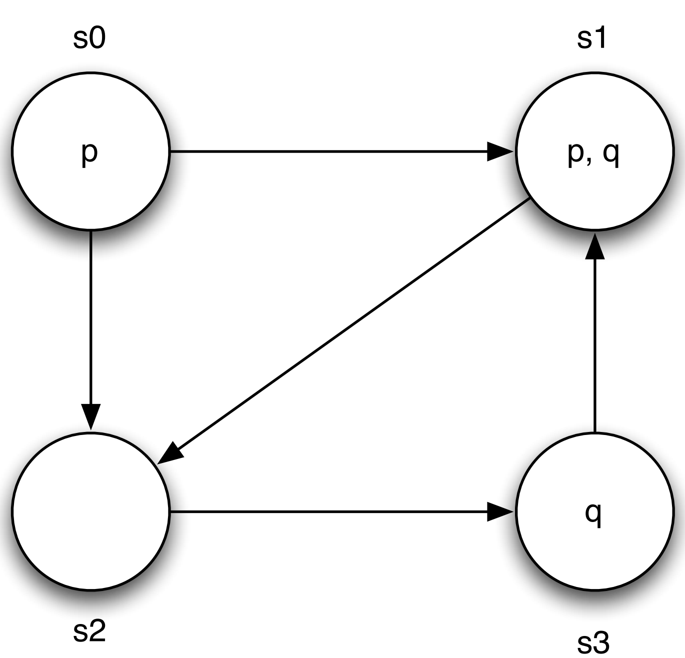
$$\models \mathbf{EX}\ q$$

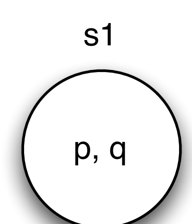
Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s.***

$$M, s \models f$$

Kripke Structure   state   Property (Temporal Logic Formula)





?

$\mathbf{EX}\ q$

Model Checking Problem

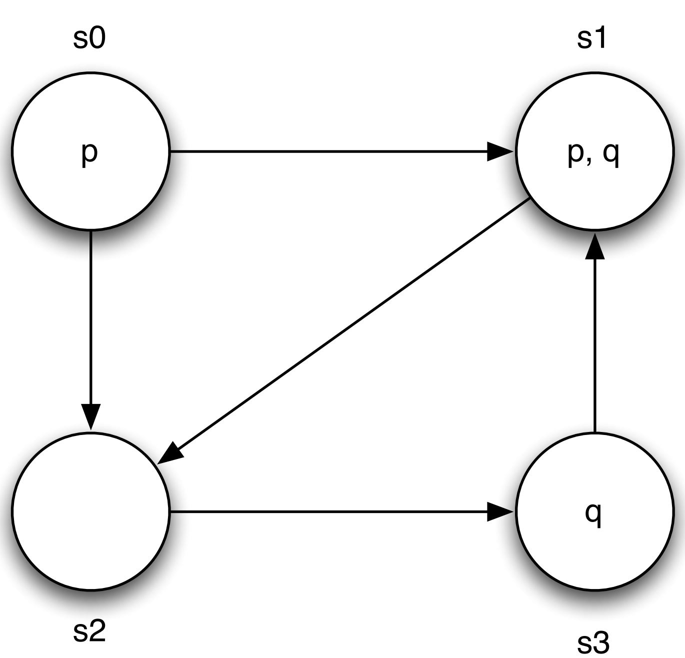
Find all states ***s*** such that ***M*** has property ***f*** at state ***s*.**

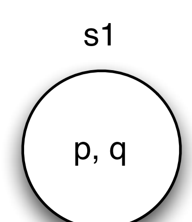
$$M, s \models f$$

Kripke Structure

state

Property
(Temporal Logic Formula)





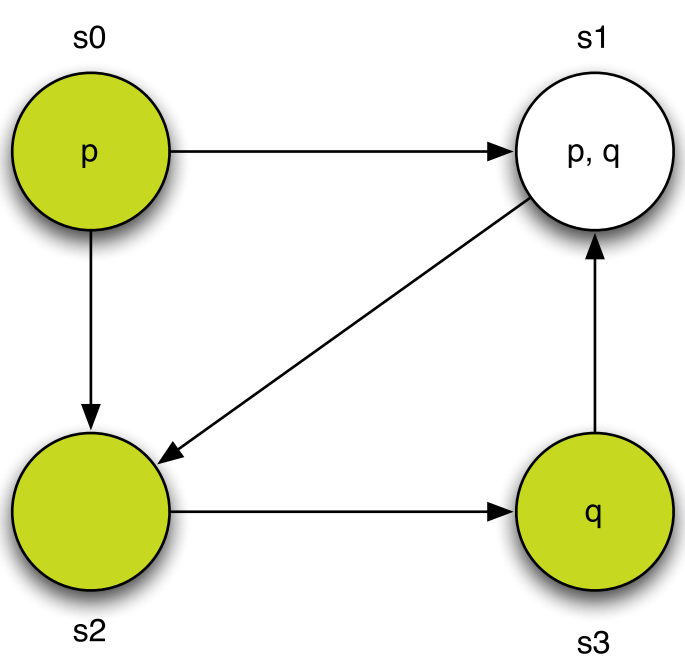
$$\not\models \mathbf{EX}\ q$$

Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s***.

$$M, s \models f$$

Kripke Structure — state — Property (Temporal Logic Formula)



$$\mathbf{EX}\ q$$

Model Checking

What's Temporal Logic (esp, CTL*)?

The Logic CTL*

The computation tree logic CTL* combines both branching-time and linear-time operators.

In this logic a *path quantifier* can prefix an assertion composed of arbitrary combinations of the usual linear-time operators.

1. Path quantifier:
   A - "for every path"
   E - "there exists a path"

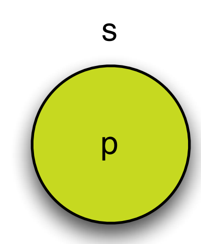
2. Linear-time operators:
   X p - p holds next time
   F p - p holds sometime in the future
   G p - p holds globally in the future
   p **U** q - p holds until q holds

Semantics of State Formulas

For a state formula f, the notation

$$M, s \models f$$

means that f holds at state s in the Kripke structure M.
It's inductively defined as follows:



$$M, s \models p \quad \Leftrightarrow \quad p \in L(s)$$

$$M, s \models \neg f \quad \Leftrightarrow \quad M, s \not\models f$$

$$M, s \models f_1 \vee f_2 \quad \Leftrightarrow \quad M, s \models f_1 \text{ or } M, s \models f_2$$

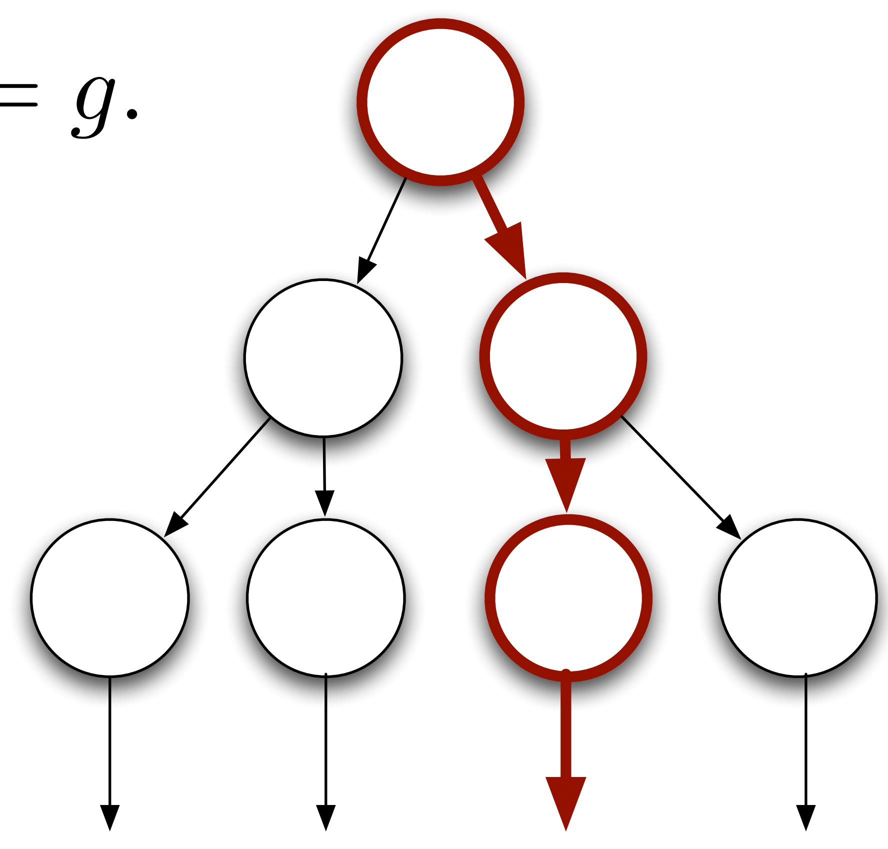
Semantics of State Formulas

For a state formula f, the notation

$$M, s \models f$$

means that f holds at state s in the Kripke structure M.
It's inductively defined as follows:

$$s \models \mathbf{E}(g) \quad \Leftrightarrow \quad \text{there exists a path } \pi \text{ starting with } s \text{ such that } \pi \models g.$$



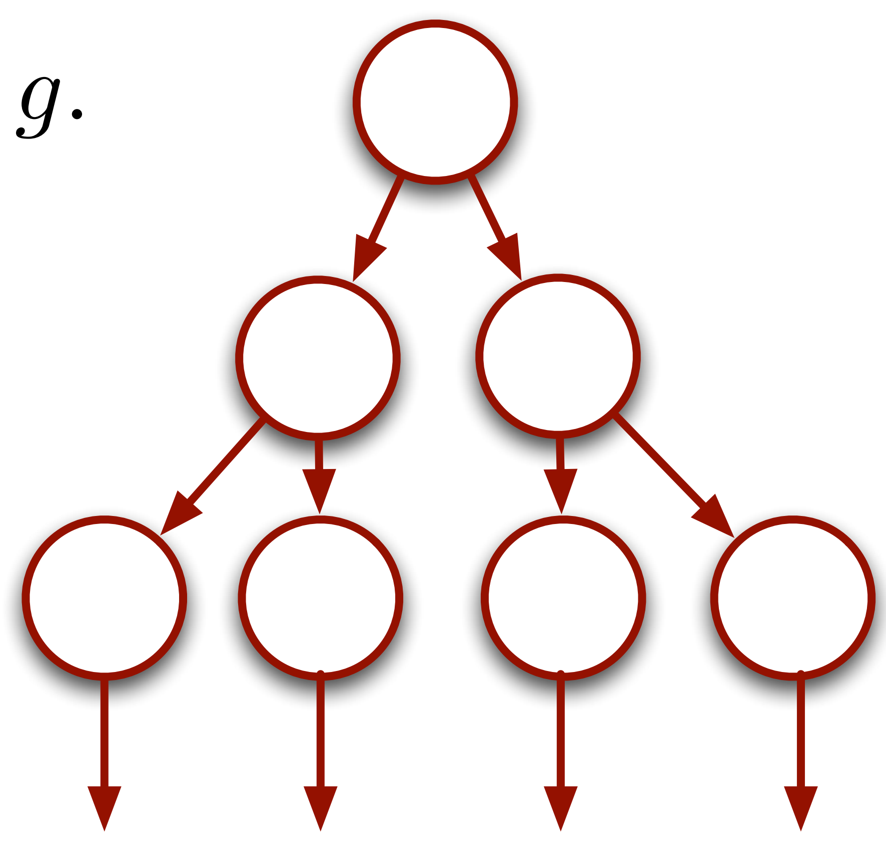
Semantics of State Formulas

For a state formula f, the notation

$$M, s \models f$$

means that f holds at state s in the Kripke structure M. It's inductively defined as follows:

$$s \models \mathbf{A}(g) \quad \Leftrightarrow \quad \text{For all path } \pi \text{ starting with } s, \text{ we have } \pi \models g.$$



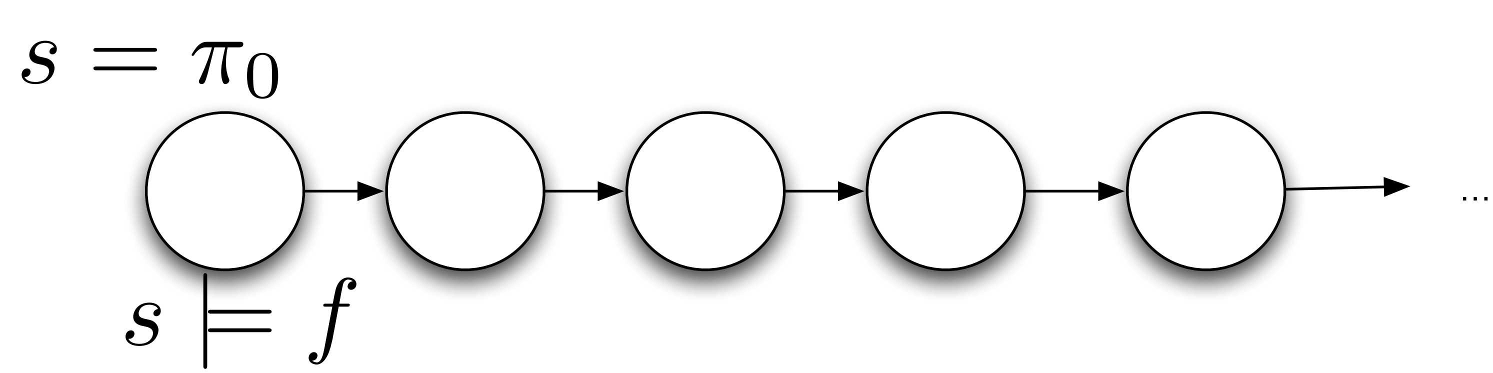
Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models f \quad \Leftrightarrow \quad s \text{ is the first state of } \pi \text{ and } s \models f.$$



Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{X} f \quad \Leftrightarrow \quad M, \pi^1 \models f$$

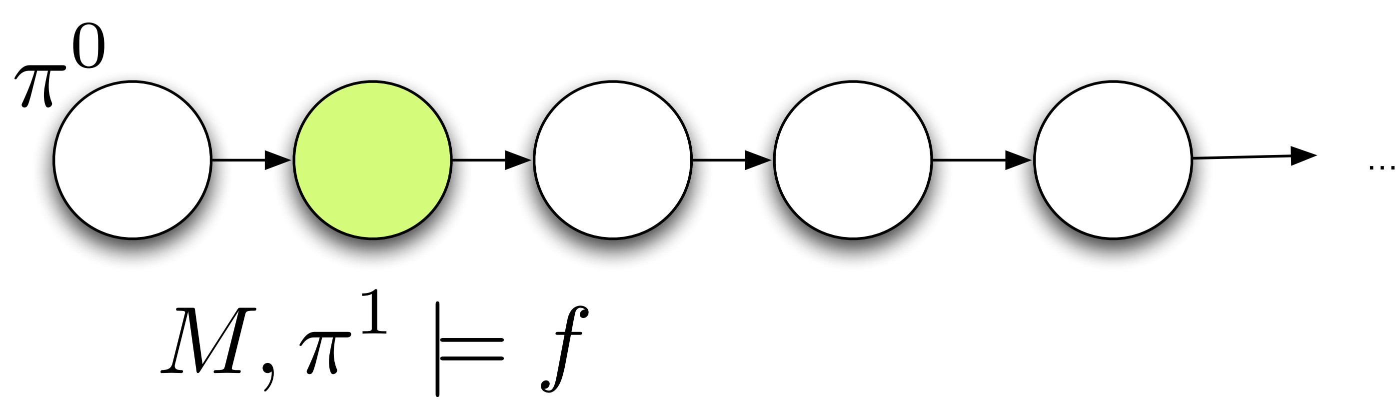
Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{X} f \quad \Leftrightarrow \quad M, \pi^1 \models f$$



Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{G} f \quad \Leftrightarrow \quad \text{for all } i \geq 0, \pi^i \models f$$

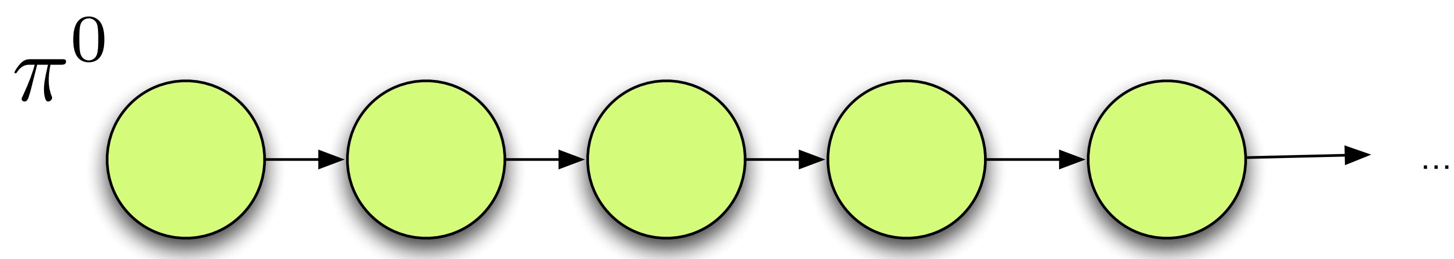
Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{G} f \quad \Leftrightarrow \quad \text{for all } i \geq 0, \pi^i \models f$$



Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{F} f \quad \Leftrightarrow \quad \text{there exists } i \geq 0, \pi^i \models f$$

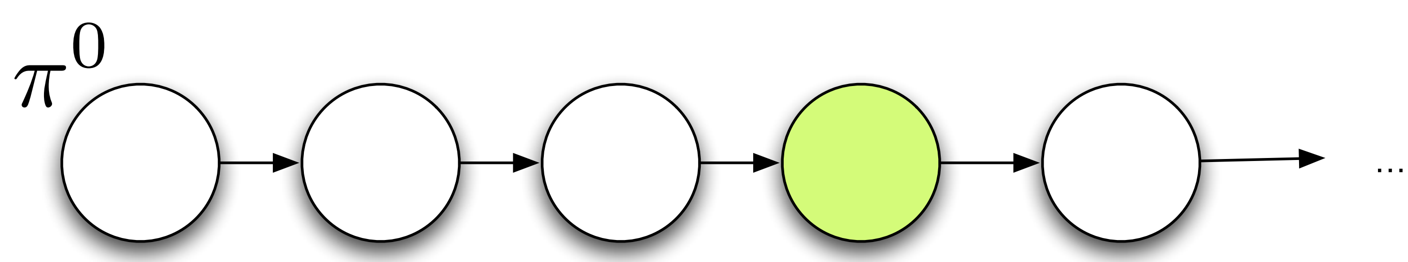
Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models \mathbf{F} f \quad \Leftrightarrow \quad \text{there exists } i \geq 0, \pi^i \models f$$



Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$\begin{aligned} M, \pi \models f_1 \mathbf{U} f_2 \quad \Leftrightarrow \quad & \text{there exists } k \geq 0 \text{ such that } M, \pi^k \models f_2 \\ & \text{and for all } 0 \leq j < k,\ M, \pi^j \models f_1 \end{aligned}$$

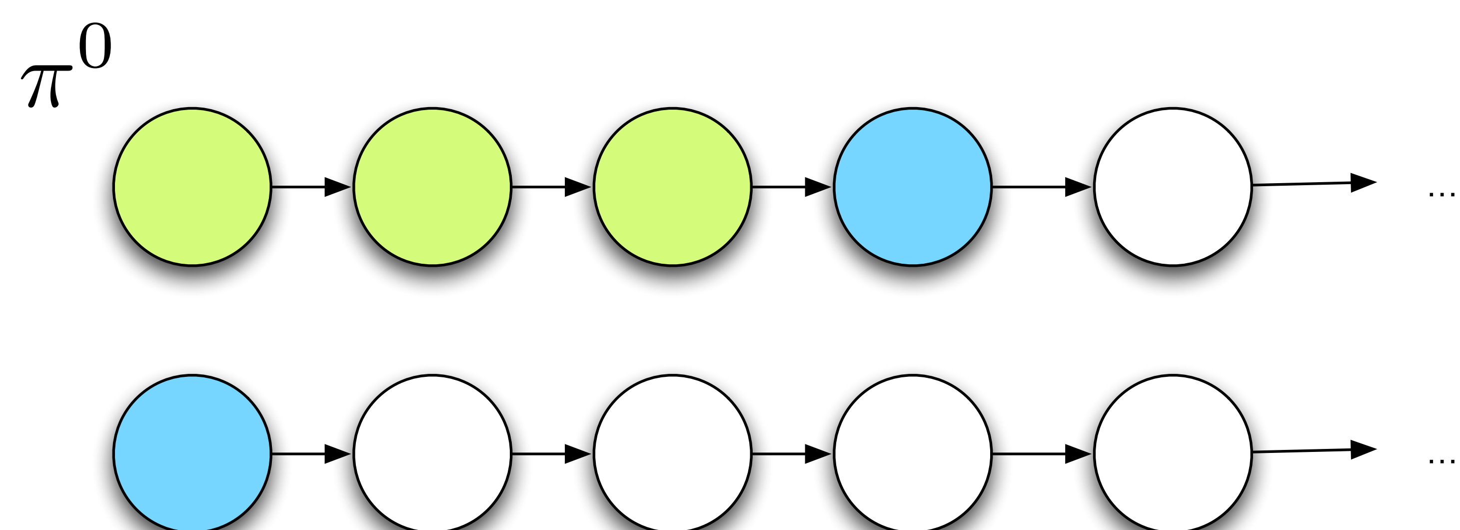
Semantics of Path Formulas

For a path formula f, the notation

$$M, \pi \models f$$

means that f holds along path π in the Kripke structure M. It's inductively defined as follows:

$$M, \pi \models f_1 \mathbf{U} f_2 \quad \Leftrightarrow \quad \text{there exists } k \geq 0 \text{ such that } M, \pi^k \models f_2$$
$$\text{and for all } 0 \leq j < k,\ M, \pi^j \models f_1$$



Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s*****.**

$$M, s \models f$$

Kripke Structure

state

Property
(Temporal Logic Formula)

How to Solve it?

Model Checking Problem

Find all states ***s*** such that ***M*** has property ***f*** at state ***s*.**

$$M, s \models f$$

Kripke Structure

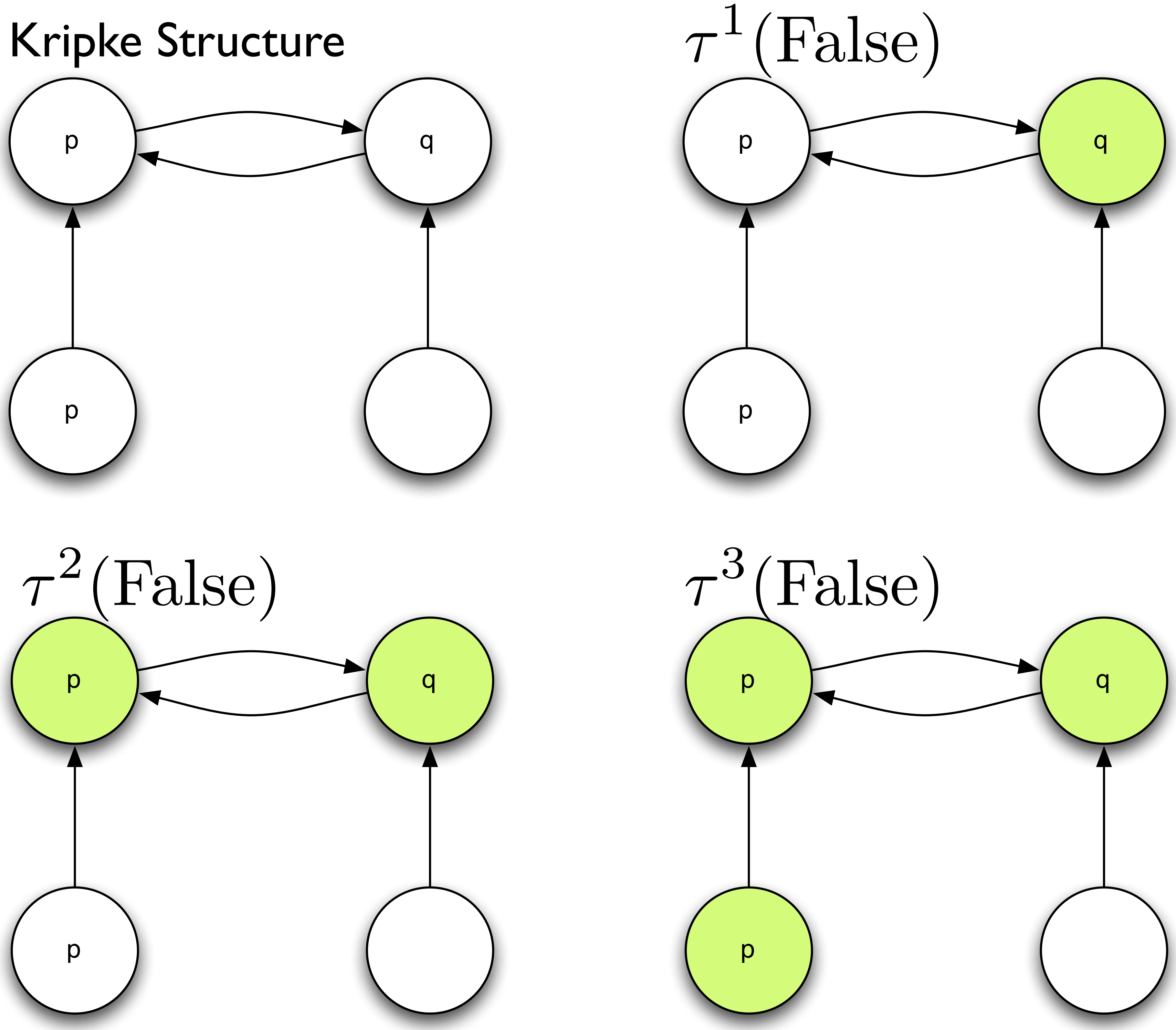
state

Property
(Temporal Logic Formula)

Fixed-Point Computation, using the following Identity!

$$\mathbf{AF}\ f_1 = \mathbf{lfp} Z. f_1 \vee \mathbf{AX}\ Z$$
$$\mathbf{EF}\ f_1 = \mathbf{lfp} Z. f_1 \vee \mathbf{EX}\ Z$$
$$\mathbf{AG}\ f_1 = \mathbf{gfp} Z. f_1 \wedge \mathbf{AX}\ Z$$
$$\mathbf{EG}\ f_1 = \mathbf{gfp} Z. f_1 \wedge \mathbf{EX}\ Z$$
$$\mathbf{A}[f_1 \mathbf{U} f_2] = \mathbf{lfp} Z. f_2 \vee (f_1 \wedge \mathbf{AX}\ Z)$$
$$\mathbf{E}[f_1 \mathbf{U} f_2] = \mathbf{lfp} Z. f_2 \vee (f_1 \wedge \mathbf{EX}\ Z)$$

This examples is from the textbook (page 65)



$$\mathbf{E}[p\mathbf{U}q] = \mathbf{lfp}Z.q \vee (p \wedge \mathbf{EX}\ Z)$$