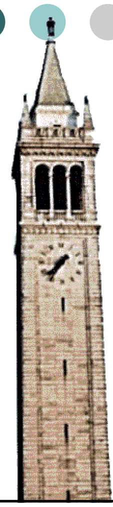
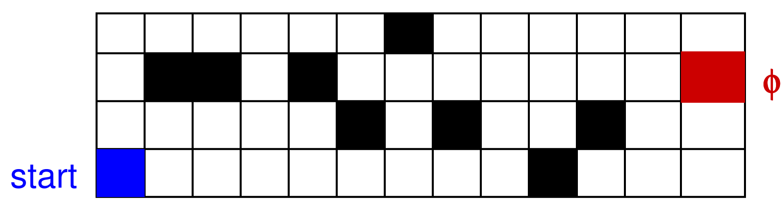


Introduction to Embedded Systems

Edward A. Lee & Sanjit A. Seshia
UC Berkeley
EECS 124
Spring 2008

Lecture 14: Reachability Analysis

A Robot delivery service, with moving obstacles



ϕ = destination for robot

At any time step:

Robot can move Left, Right, Up, Down, Stay Put

Environment can move one obstacle Up or Down or Stay Put

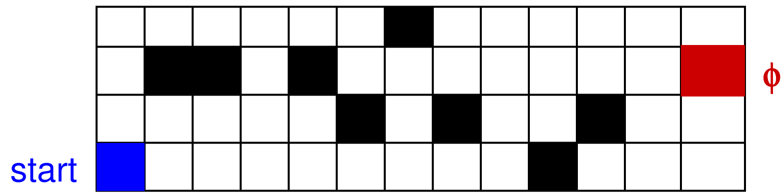
→ But only 5 times total

Can model Robot and Env as FSMs

→ Robot state = its position,

→ Env state = positions of obstacles and counts

A Robot delivery service, with moving obstacles



ϕ = robot delivers item to destination

Goal to be achieved can be stated in temporal logic

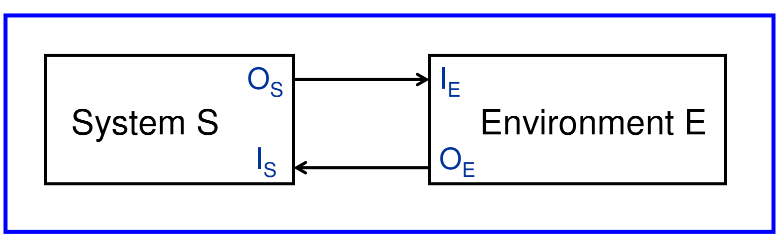
$\mathbf{F}\ \phi$

How can we find a path for the robot from starting point to the destination?

→ This is an example of a "reachability problem"

Solving the Reachability Problem

- Construct FSMs for Robot and Environment
- Compose FSMs to form a new FSM
- Check whether the goal state is reachable from the start state

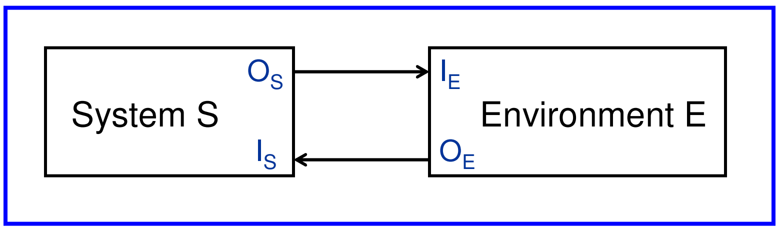


Open vs. Closed Systems

A closed system is one with no inputs and no outputs

Typically, the system we analyze is the composition of the system with its environment

- ➢ this composed system is closed!
- ➢ In general, could be non-deterministic (why?)



Open vs. Closed Systems

A closed system is one with no inputs and no outputs

Typically, the system we analyze is the composition of the system with its environment

- ➢ this composed system is closed!
- ➢ In general, could be non-deterministic (env non-det.)

Recall: a ND FSM is a 5-tuple

(States, Inputs, Outputs, possibleUpdates, initialStates)

For a closed system, Inputs = Outputs = $\emptyset$

Denote:

States – Q, possibleUpdates – δ, initialStates – Q_0

Reachability Analysis for FSMs

The reachability problem:

Given an FSM $M = (Q, \delta, Q_0)$, and a state *s*,
is *s* reachable from some $q_0 \in Q_0$ by following δ ?

Reachability Analysis for FSMs

The reachability problem:

Given an FSM $M = (Q, \delta, Q_0)$, and a state *s*,
is *s* reachable from some $q_0 \in Q_0$ by following δ ?

Note: Although we write Q as part of M, typically we don't have the set of states Q

- it's too large!!!

Reachability Analysis for FSMs

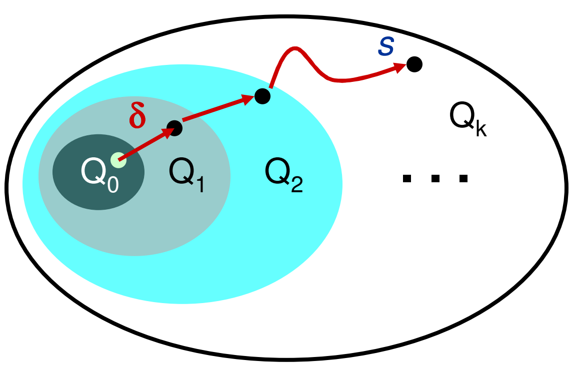
The reachability problem:

Given an FSM $M = (Q, \delta, Q_0)$, and a state *s*,
is *s* reachable from some $q_0 \in Q_0$ by following δ ?

How can we express the property
"s is reachable from a start state"
in Temporal Logic?

Outline of Approach

- Generate the state graph by repeated application of δ
- If the goal state reached, stop & report success. Else, continue until all states are seen.



The Reachability Algorithm

Input: Description of M: (Q_0, δ), s

Output: Is s reachable from Q_0?

Init: $S := S_{new} := Q_0$;
while ($S_{new} \mathrel{!=} \emptyset$) {
  if ($s \in S_{new}$)
    return YES;
  $S' := \{ q \mid \exists p \in S \text{ s.t. } q \in \delta(p) \} \cup S$
  $S_{new} := S' \setminus S$;
}

Suppose we have a Robot that must pick up multiple things, in any order

ϕ_i = robot picks up item i, $1 \leq i \leq n$

How would you state this goal in temporal logic?

Suppose we have a Robot that must pick up multiple things, in any order

ϕ_i = robot picks up item i, $1 \leq i \leq n$

Goal to be achieved is:

$$\mathbf{F}\,\phi_1 \wedge \mathbf{F}\,\phi_2 \wedge \ldots \wedge \mathbf{F}\,\phi_n$$

Suppose we have a Robot that must pick up multiple things, in any order

ϕ_i = robot picks up item i, $1 \leq i \leq n$

Goal to be achieved is:

$$\mathbf{F}\,\phi_1 \wedge \mathbf{F}\,\phi_2 \wedge \ldots \wedge \mathbf{F}\,\phi_n$$

How can we find a strategy to achieve this goal?

Suppose we have a Robot that must pick up multiple things, in any order

ϕ_i = robot picks up item i, $1 \leq i \leq n$

Goal to be achieved is:

$$\mathbf{F}\ \phi_1 \wedge \mathbf{F}\ \phi_2 \wedge \ldots \wedge \mathbf{F}\ \phi_n$$

How can we find a strategy to achieve this goal?

→ Do repeated reachability, first from Q_0 to reach ϕ_1, then from ϕ_1 to reach ϕ_2, then ϕ_2 to reach ϕ_3, …

Student question: Suppose we have a Robot that must pick up multiple things, ***in a specified order***

ϕ_i = robot picks up item i, $1 \leq i \leq n$

Goal to be achieved is:

$$\mathbf{F(}\ \phi_1 \wedge \mathbf{F\ (}\ \phi_2 \wedge \ldots \wedge \mathbf{F}\ \phi_n\ \mathbf{))}$$

Exercise

Can we do reachability analysis backwards?

I.e.: start with s instead of Q_0, and then follow the update function δ backwards…