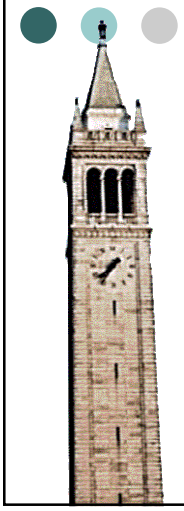


Introduction to Embedded Systems

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

Lecture 12: Temporal Logic

Specification, Verification, and Control

Specification
A mathematical statement of the goal to be achieved

Verification
Does the system achieve its goal, as designed?

Controller Synthesis
Given an incomplete design, synthesize a strategy to complete the system so that it achieves its goal

Specification, Verification, and Control

Specification TEMPORAL LOGIC

A mathematical statement of the goal to be achieved

Verification REACHABILITY ANALYSIS

Does the system achieve its goal, as designed?

Controller Synthesis

Given an incomplete design, synthesize a strategy to complete the system so that it achieves its goal

Temporal Logic

- A mathematical way to express properties of a system over time
  - E.g., Behavior of an FSM or Hybrid System
- Many flavors of temporal logic
  - Propositional temporal logic
  - Real-time temporal logic
- Amir Pnueli won ACM Turing Award, in part, for the idea of using temporal logic for specification

Example: Specification of the *SpaceWire* Protocol (European Space Agency standard)

8.5.2.2 ErrorReset

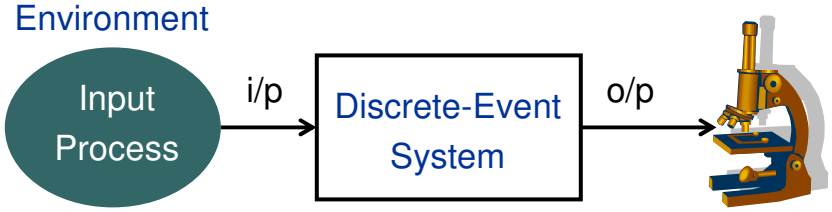
a. The *ErrorReset* state shall be entered after a system reset, after link operation is terminated for any reason or if there is an error during link initialization.

b. In the *ErrorReset* state the Transmitter and Receiver shall all be reset.

c. When the reset signal is de-asserted the *ErrorReset* state shall be left unconditionally after a delay of 6,4 µs (nominal) and the state machine shall move to the *ErrorWait* state.

d. Whenever the reset signal is asserted the state machine shall move immediately to the *ErrorReset* state and remain there until the reset signal is de-asserted.

Recap: Simulating a Discrete-Event System



2. How to generate random input?

1. How to simulate the system?

3. How to check Output?

Propositional Temporal Logic

Every send(1, 2) is eventually followed by a recv(2, 1)

G { send(1,2) ⇒ **F** recv(2, 1) }

At any point in time

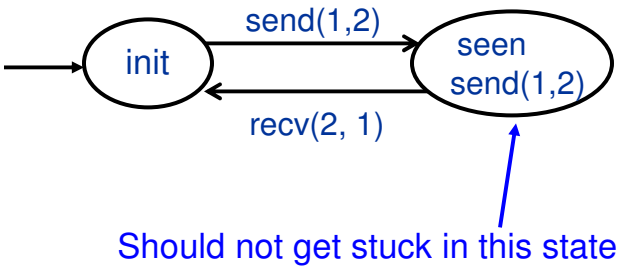
If a send(1, 2) occurs

It is *eventually* followed by a recv(2, 1)

Propositional Temporal Logic

Every send(1, 2) is eventually followed by a recv(2, 1)

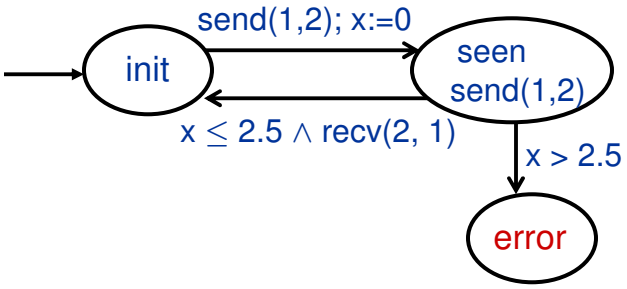
G { send(1,2) ⇒ **F** recv(2, 1) }



Real-Time Temporal Logic

Every send(1, 2) is followed by a recv(2, 1) within 2.5 ms

$$\mathbf{G}\ \{\ \text{send}(1,2)\ \Rightarrow\ \mathbf{F}_{\leq 2.5}\ \text{recv}(2,1)\ \}$$



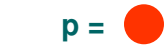
Property on a Single State

A Boolean expression over system state or input/output symbols
- send(1,2): packet sent from node 1 to node 2
- x > 2.5: clock variable x exceeds 2.5

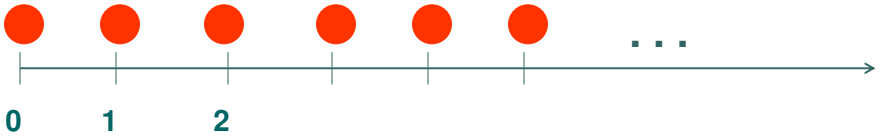
We will visualize each such Boolean expression by
- a distinct color
- using a name such as p, q, …

Globally p: G p

G p is true in a state if p holds at all points of time (along the path) starting from that state

p = 

G p holds in the initial state iff

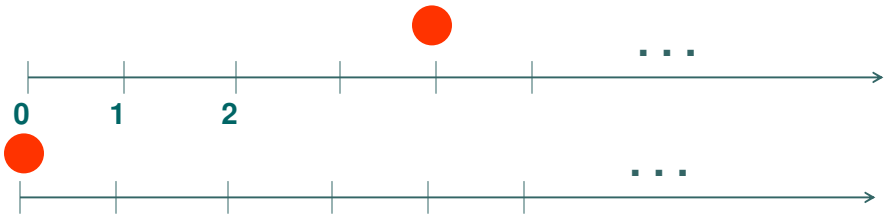


Eventually p: F p

F p is true in a state if p holds at some point in the future, starting from that state

p = 

If F p holds in the initial state, we could have the scenario:

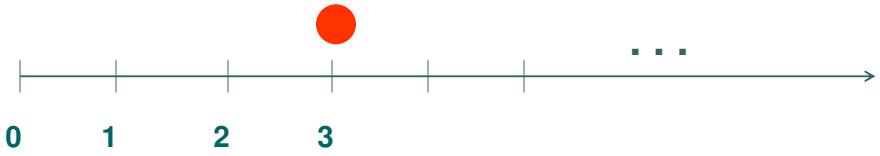


Next p: X p

X p is true along a path starting in a state if p holds in the next state

p = 

Suppose X p holds in state at t = 2



Nesting of Formulas

p need not be just a Boolean formula.

It can be a temporal logic formula itself!

p = 

"X p holds in all states, starting from initial state"

How can we write this in temporal logic?

How do we draw this?

Alternate Notation

Sometimes you'll see alternative notation in the literature:

G	□
F	◊
X	○

Examples: What do they mean?

- G F p
- F G p
- G(p → F q)
- F(p → (X X q))

Remember:

Gp p holds in all states
Fp p holds eventually
Xp p holds in the next state

p Until q: p U q

p U q is true in a state if

- q is true in some state reachable from s
- p is true in all states from s until q holds

Temporal Operators & Relationships

G, F, X, U: All express properties along system traces

- Can you express G p purely in terms of F, p, and Boolean operators ?
- How about F in terms of U?
- What about X in terms of G, F, or U?

Examples: Write in Temporal Logic

1. "Whenever the iRobot is at the ramp-edge (cliff), eventually it moves 5 cm away from the cliff."
   - p – iRobot is at the cliff
   - q – iRobot is 5 cm away from the cliff

2. "Whenever the distance between cars is less than 2m, cruise control is deactivated"
   - p – distance between cars is less than 2 m
   - q – cruise control is active

Ex. write the SpaceWire specs. in Temporal Logic