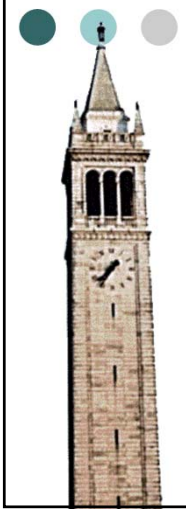
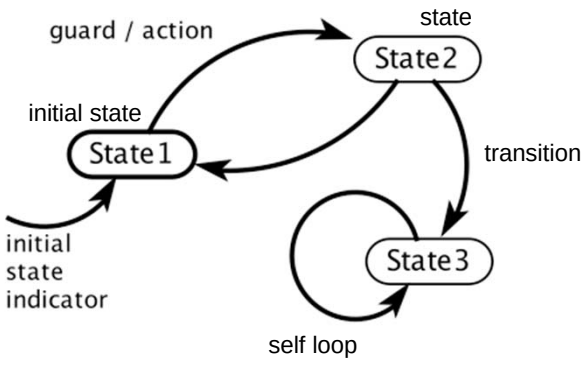


Introduction to Embedded Systems

Sanjit A. Seshia
UC Berkeley
EECS 149/249A
Fall 2015

Chapter 3, 4: Extended Finite State Machines, Timed Automata, Hybrid Automata

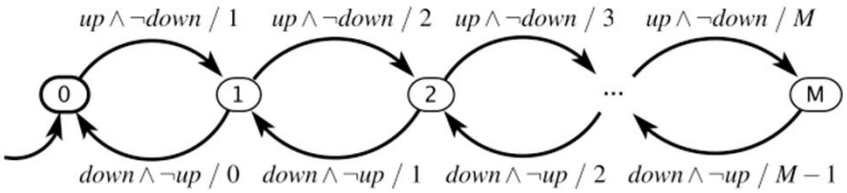
Recall FSM Notation



Garage Counter Example

Recall this example, which counts cars in a parking garage:

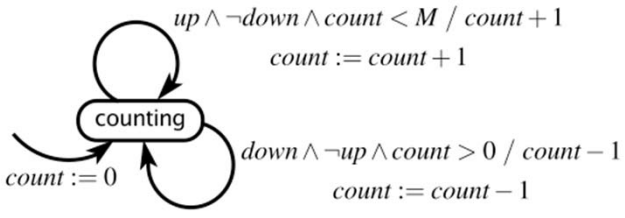
inputs: $up, down \in \{present, absent\}$
output $\in \{0, \cdots, M\}$



Extended State Machines

Extended state machines augment the FSM model with *variables* that may be read or written. E.g.:

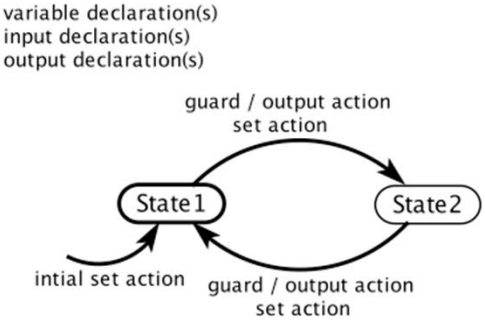
variable: $count \in \{0, \cdots, M\}$
inputs: $up, down \in \{present, absent\}$
output $\in \{0, \cdots, M\}$



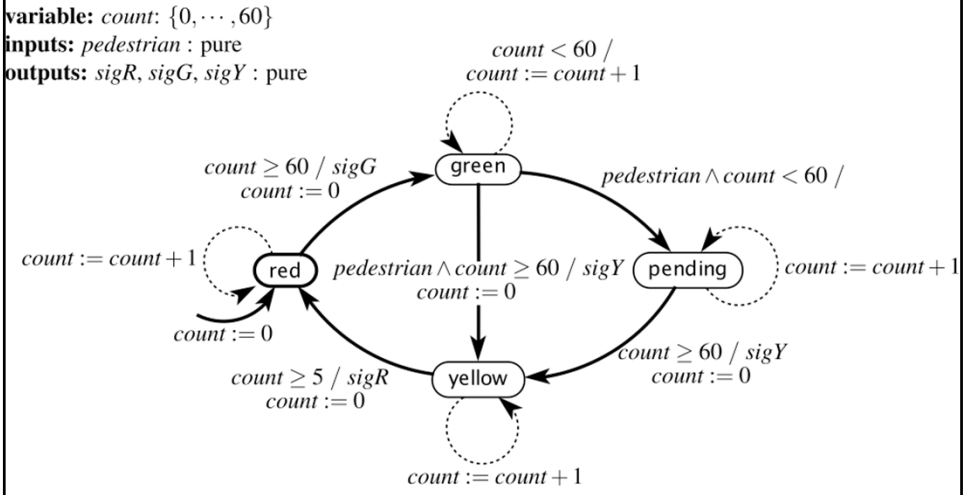
Question: What is the size of the state space?

General Notation for Extended State Machines

We make explicit declarations of variables, inputs, and outputs to help distinguish the three.



Extended state machine model of a traffic light controller at a pedestrian crossing:

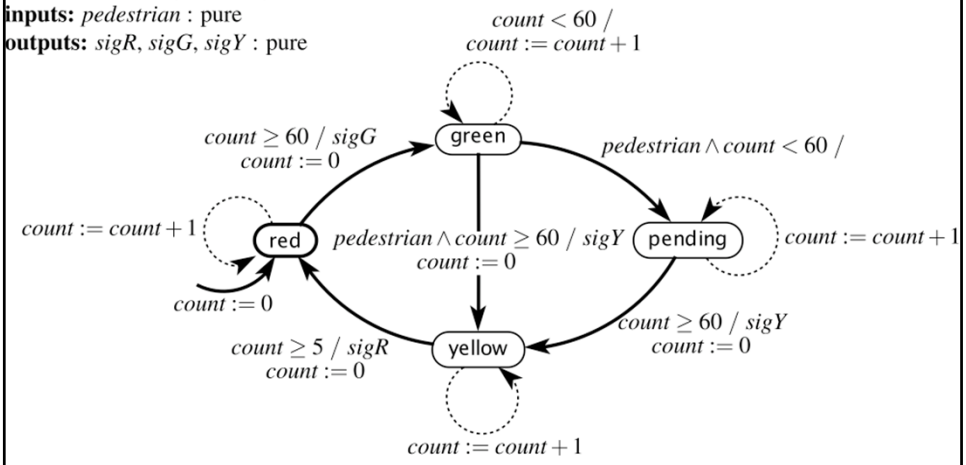


This model assumes one reaction per second

(a *time-triggered* model)

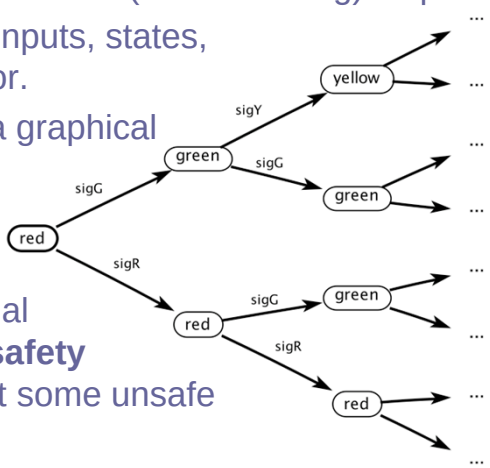
Quiz: What is the Size of the State Space for the Traffic Light Controller?

variable: *count*: $\{0, \cdots, 60\}$
inputs: *pedestrian* : pure
outputs: *sigR*, *sigG*, *sigY* : pure

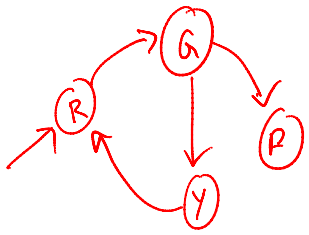


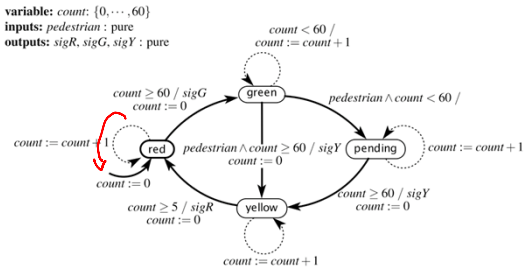
Behaviors and Traces

- FSM **behavior** is a sequence of (non-stuttering) steps.
- A **trace** is the record of inputs, states, and outputs in a behavior.
- A **computation tree** is a graphical representation of all possible traces.



FSMs are suitable for formal analysis. For example, **safety** analysis might show that some unsafe state is not reachable.

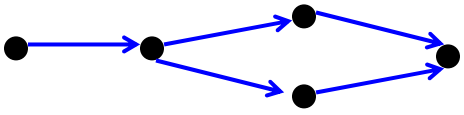




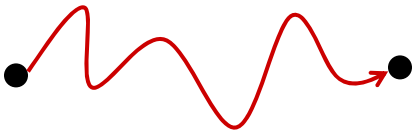
$(R,0) \to (R,1) \to \cdots \to (R,60) \xrightarrow{sigG} (G,0) \xrightarrow{tick} (P,0) \to (P,1)$

$\to \cdots (P,60) \xrightarrow{sigY} (Y,0) \to \cdots$

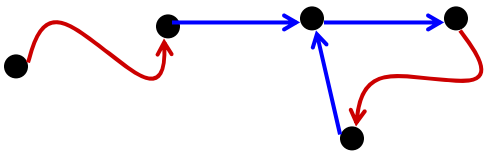
Discrete System (FSM)

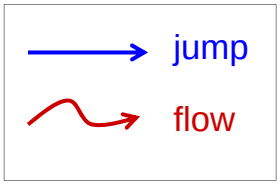


Continuous System



Hybrid System

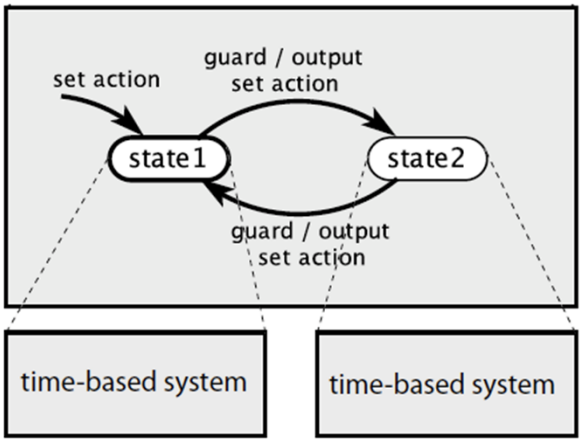




Where do Hybrid Systems arise?

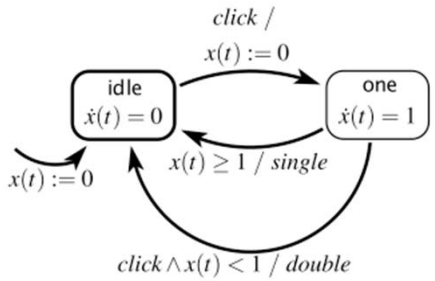
- Digital controller of physical "plant"
  - thermostat
  - intelligent cruise/powertrain control in cars
  - aircraft auto pilot
- Phased operation of natural phenomena
  - bouncing ball
  - biological cell growth
- Multi-agent systems
  - ground and air transportation systems
  - interacting robots

An alternative to FSMs that is explicit about the passage of time: ***Timed automata***, a special case of hybrid systems.



Example: Mouse Double Click Detector

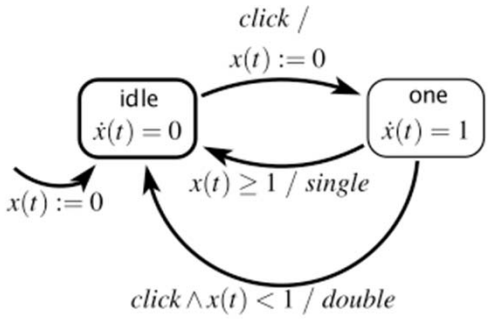
continuous variable: $x(t) \in \mathbb{R}$
inputs: $click \in \{present, absent\}$
outputs: $single, double \in \{present, absent\}$



This simple form of hybrid system is called a timed automaton, where the dynamics is just passage of time.

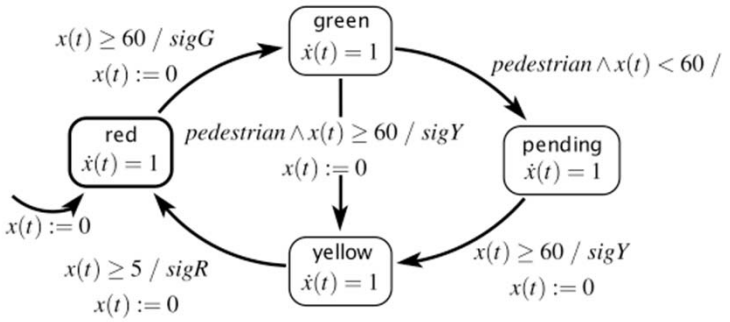
Quiz: How many states does this automaton have?

continuous variable: $x(t) \in \mathbb{R}$
inputs: $click \in \{present, absent\}$
outputs: $single, double \in \{present, absent\}$



Timed automaton model of a traffic light controller

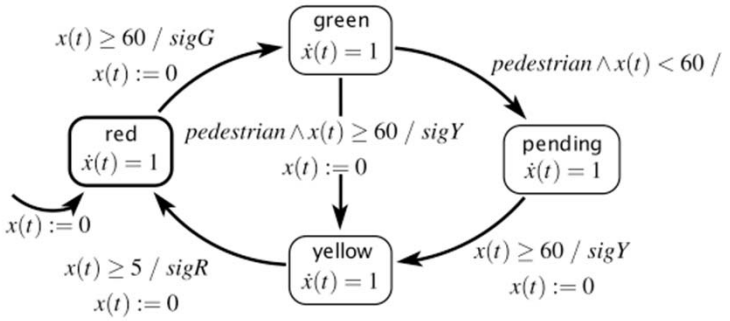
continuous variable: $x(t)$: $\mathbb{R}$
inputs: *pedestrian*: pure
outputs: *sigR*, *sigG*, *sigY*: pure



This light remains green at least 60 seconds, and then turns yellow if a pedestrian has requested a crossing. It then remains red for 60 seconds.

When do reactions occur in a hybrid automaton?

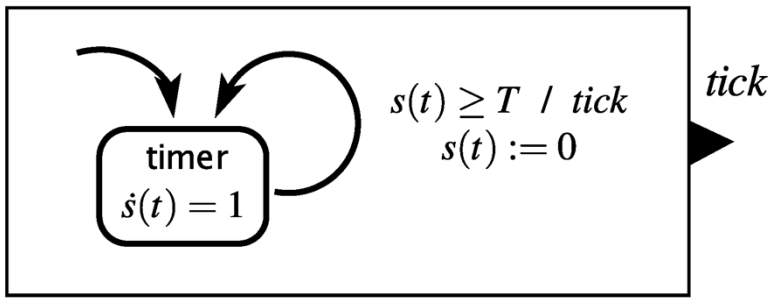
continuous variable: $x(t)$: $\mathbb{R}$
inputs: *pedestrian*: pure
outputs: *sigR*, *sigG*, *sigY*: pure



Reactions are occurring continually, with the continuous state variable *x* being continually updated.

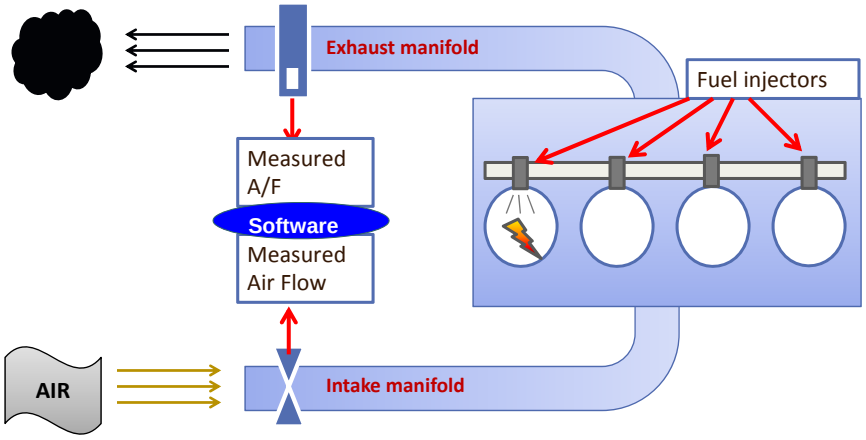
Example: "Tick" Generator (Timer)

How would you model a timer that generates a 'tick' each time T time units elapses?



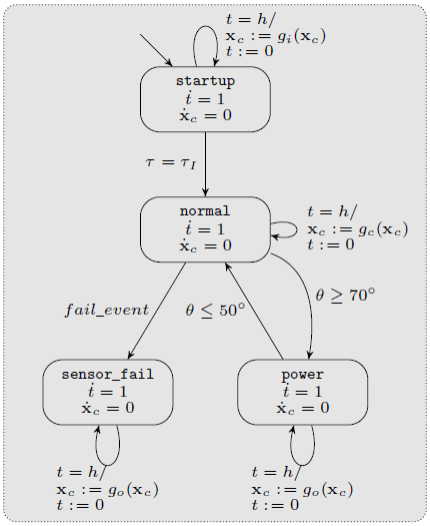
A similar timed automaton can model a generator of a timer interrupt.

Hybrid Automaton Model of Toyota Powertrain Control Example



[Slide due to J. Deshmukh, Toyota]

Hybrid Automaton Model of Toyota Powertrain Control Example



"Powertrain Control Verification Benchmark", Jin et al., HSCC 2014

Four Operating Modes:

1. Startup: Wait for O2 sensors to start giving accurate readings (temp dependent), employ open-loop control
2. Normal: Use combination of feedback PI control and feedforward control to regulate A/F ratio
3. Power: Driver depresses gas pedal more (higher throttle angle) – switch to feedforward
4. Sensor Failure: switch to feedforward control