Week 1- Introduction to model checking

B. Srivathsan

Chennai Mathematical Institute

NPTEL-course

July - November 2015

Course overview

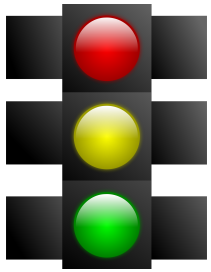
What are we **interested** in?

What are we **interested** in?

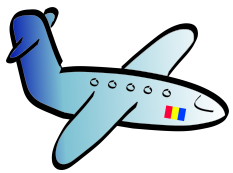
Software Controllers

Code that controls the working of an

Information and Communication (ICT) device



Traffic lights controller

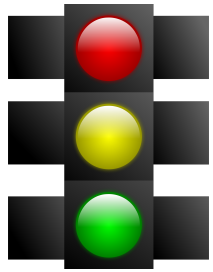


Flight control

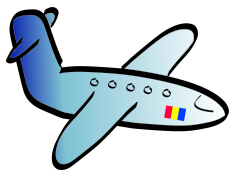
Automatic gear control

ATM

Pacemaker



Traffic lights controller



Flight control

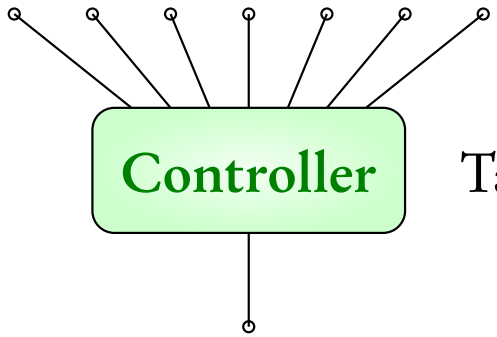
Automatic gear control

ATM

Pacemaker

Lifts, Automatic doors, Hardware circuits, Netbanking ... and many more!

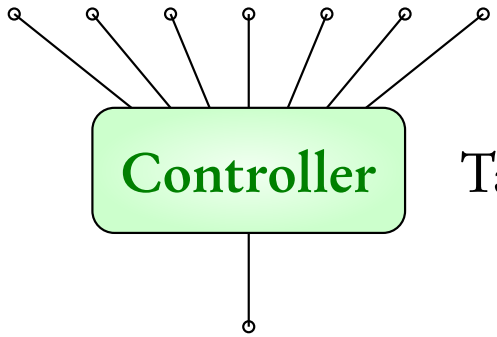
Listens to **various inputs**



Takes certain **decisions**

Gives **output action**

Listens to **various inputs**



Takes certain **decisions**

Gives **output action**

Many **safety-critical** systems controlled by code

How **reliable** is the controlling code?

- **decision making** should be correct
- **all possible scenarios** should be considered

Bugs are costly

- **Intel's Pentium II processor:**

  Error in floating point division code (1994)

  - Loss of 475 million US dollars

- **Ariane 5 rocket:**

  Error in the control software (1996)

  - Crashed 36 seconds after launch

- **Therac-25 radiation therapy machine:**

  Error in control software (1985 - 1987)

  - Death of 6 patients due to radiation overdose

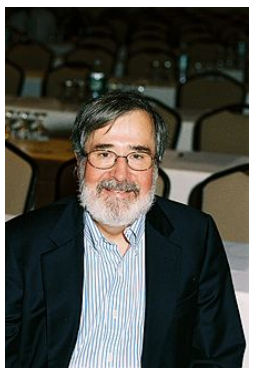
Goal: Make **low-defect** software controllers

Traditional testing **insufficient** for safety-critical systems

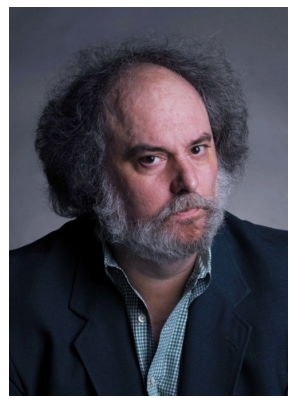
Goal: Make **low-defect** software controllers

Traditional testing **insufficient** for safety-critical systems

→ A new **verification technology** called **Model-checking**



Edmund Clarke

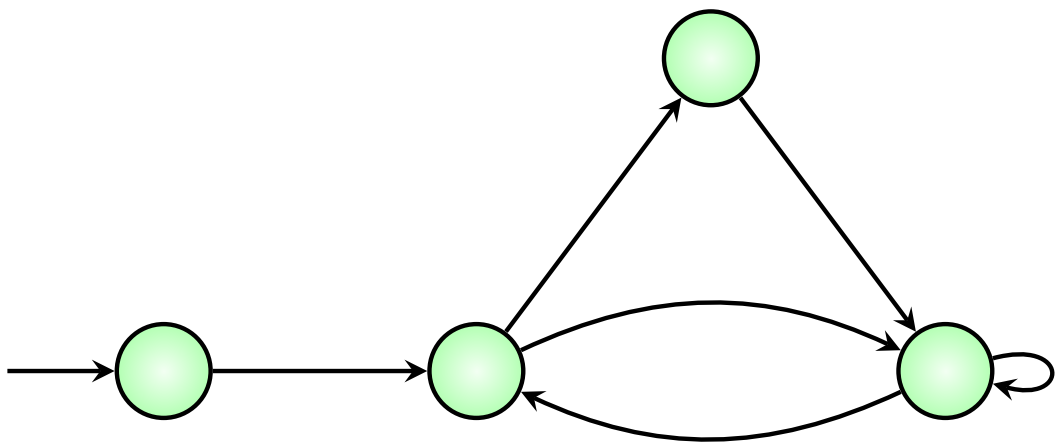


Allen Emerson

Joseph Sifakis

Model Checking

Uses **finite state machines** to model and **verify** controllers



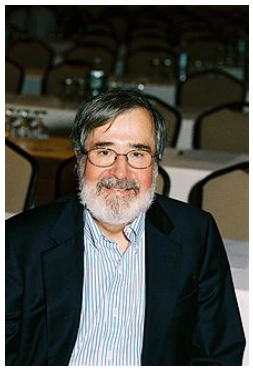
Some places where **Model Checking** technology is **used**

- *Hardware:* Intel, IBM, Synopsys
- *Avionics:* Rockwell Collins, Honeywell
- *Automobiles:* Toyota
- *Space:* NASA, European Space Agency
- *Others:* Microsoft Research, Tata, Mathworks

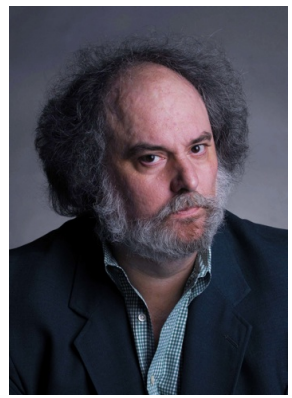
Some places where **Model Checking** technology is **used**

- *Hardware:* Intel, IBM, Synopsys
- *Avionics:* Rockwell Collins, Honeywell
- *Automobiles:* Toyota
- *Space:* NASA, European Space Agency
- *Others:* Microsoft Research, Tata, Mathworks

Backed by many **university groups** from all over the world!



Edmund Clarke



Allen Emerson

Joseph Sifakis

Turing Award'07 for their work on Model-checking

Why do this course?

- Various **industries adopting** model-checking into their design cycle
- Need engineers **qualified** in model-checking technology
- Scope for **higher studies**

In this course

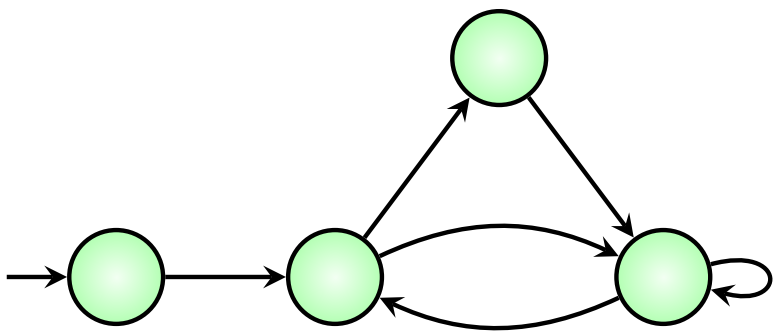
Introduction to **techniques and tools** used in Model-Checking

Book: Principles of Model Checking,
Christel Baier and Joost-Pieter Katoen, MIT Press (2008)

In this course

Introduction to **techniques and tools** used in Model-Checking

Book: Principles of Model Checking,
Christel Baier and Joost-Pieter Katoen, MIT Press (2008)



$$(\{q_1, q_2, q_3, q_4\}, \delta)$$

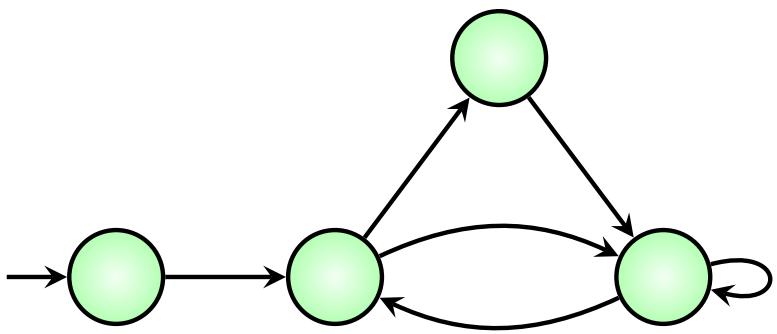
$$\delta(q_1) = q_2, \delta(q_2) = \{q_3, q_4\}$$

$$\delta(q_3) = q_4, \delta(q_4) = \{q_2, q_4\}$$

In this course

Introduction to **techniques and tools** used in Model-Checking

Book: Principles of Model Checking,
Christel Baier and Joost-Pieter Katoen, MIT Press (2008)



$$(\{q_1, q_2, q_3, q_4\}, \delta)$$

$$\delta(q_1) = q_2, \delta(q_2) = \{q_3, q_4\}$$

$$\delta(q_3) = q_4, \delta(q_4) = \{q_2, q_4\}$$

Bachelors/Masters in CS/IT/EEE/ECE **welcome!**

Hope you'll **enjoy** the course!